ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 18045— 2008

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Методология оценки безопасности информационных технологий

ISO/IEC 18045:2005
Information technology — Security techniques — Methodology for IT security evaluation
(IDT)

Издание официальное

БЗ 12—2007/465

Москва
Стандартинформ
2009

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0 — 2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным государственным учреждением «4 Центральный научно-исследовательский институт Министерства обороны России» (ФГУ «4 ЦНИИ Минобороны России»), Федеральным государственным унитарным предприятием «Научно-технический и сертификационный центр по комплексной защите информации» (ФГУП Центр «Атомзащитаинформ»), Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт управления, экономики и информации Росатома» (ФГУП «ЦНИИАТОМИНФОРМ») при участии экспертов Международной рабочей группы по Общим критериям на основе собственного аутентичного перевода стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 522-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 18045:2005 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» (ISO/IEC 18045:2005 «Information technology — Security techniques — Methodology for IT security evaluation»).

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

5 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 1
4 Обозначения и сокращения . . . 2
5 Краткий обзор . . . 3
5.1 Структура стандарта . . . 3
6 Принятые соглашения . . . 3
6.1 Терминология . . . 3
6.2 Применение глаголов . . . 3
6.3 Общие указания по оценке . . . 3
6.4 Взаимосвязь между структурами ИСО/МЭК 15408 и настоящего стандарта . . . 4
6.5 Вердикты оценщика . . . 4
7 Общие задачи оценки . . . 5
7.1 Введение . . . 5
7.2 Задача получения исходных данных для оценки . . . 5
7.2.1 Цели . . . 5
7.2.2 Замечания по применению . . . 5
7.2.3 Подзадача управления свидетельством оценки . . . 6
7.3 Задача оформления результатов оценки . . . 7
7.3.1 Цели . . . 7
7.3.2 Замечания по применению . . . 7
7.3.3 Подзадача подготовки СП . . . 7
7.3.4 Подзадача подготовки ТОО . . . 7
7.3.5 Подвиды деятельности по оценке . . . 12
8 Оценка профиля защиты . . . 12
8.1 Введение . . . 12
8.2 Организация оценки ПЗ . . . 12
8.3 Вид деятельности «Оценка профиля защиты» . . . 13
8.3.1 Оценка раздела «Описание ОО» (APE_DES.1) . . . 13
8.3.2 Оценка раздела «Среда безопасности ОО» (APE_ENV.1) . . . 14
8.3.3 Оценка раздела «Введение ПЗ» (APE_INT.1) . . . 16
8.3.4 Оценка раздела «Цели безопасности» (APE_OBJ.1) . . . 16
8.3.5 Оценка раздела «Требования безопасности ИТ» (APE_REQ.1) . . . 19
8.3.6 Оценка требований безопасности ИТ, сформулированных в явном виде (APE_SRE.1) . . . 27
9 Оценка задания по безопасности . . . 29
9.1 Введение . . . 29
9.2 Организация оценки ЗБ . . . 29
9.3 Вид деятельности «Оценка задания по безопасности» . . . 30
9.3.1 Оценка раздела «Описание ОО» (ASE_DES.1) . . . 30
9.3.2 Оценка раздела «Среда безопасности ОО» (ASE_ENV.1) . . . 31
9.3.3 Оценка раздела «Введение ЗБ» (ASE_INT.1) . . . 33
9.3.4 Оценка целей безопасности (ASE_OBJ.1) . . . 34
9.3.5 Оценка раздела «Утверждение о соответствии ПЗ» (ASE_PPC.1) . . . 37
9.3.6 Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1) . . . 38
9.3.7 Оценка требований безопасности ИТ, сформулированных в явном виде (ASE_SRE.1) . . . 46
9.3.8 Оценка раздела «Краткая спецификация ОО» (ASE_TSS.1) . . . 48
10 Оценка по ОУД1 . . . 51
10.1 Введение . . . 51
10.2 Цели . . . 51
10.3 Организация оценки по ОУД1 . . . 51
10.4 Вид деятельности «Управление конфигурацией» . . . 51
10.4.1 Оценка возможностей УК (ACM_CAP.1) . . . 52

10.5 Вид деятельности «Поставка и эксплуатация» . . . 52
10.5.1 Оценка установки, генерации и запуска (ADO_IGS.1) . . . 52
10.6 Вид деятельности «Разработка» . . . 53
10.6.1 Замечания по применению . . . 53
10.6.2 Оценка функциональной спецификации (ADV_FSP.1) . . . 54
10.6.3 Оценка соответствия представлений (ADV_RCR.1) . . . 57
10.7 Вид деятельности «Руководства» . . . 57
10.7.1 Замечания по применению . . . 58
10.7.2 Оценка руководства администратора (AGD_ADM.1) . . . 58
10.7.3 Оценка руководства пользователя (AGD_USR.1) . . . 60
10.8 Вид деятельности «Тестирование» . . . 62
10.8.1 Замечания по применению . . . 62
10.8.2 Оценка путем независимого тестирования (ATE_IND.1) . . . 62
11 Оценка по ОУД2 . . . 65
11.1 Введение . . . 65
11.2 Цели . . . 65
11.3 Организация оценки по ОУД2 . . . 65
11.4 Вид деятельности «Управление конфигурацией» . . . 66
11.4.1 Оценка возможностей УК (ACM_CAP.2) . . . 66
11.5 Вид деятельности «Поставка и эксплуатация» . . . 68
11.5.1 Оценка поставки (ADO_DEL.1) . . . 68
11.5.2 Оценка установки, генерации и запуска (ADO_IGS.1) . . . 69
11.6 Вид деятельности «Разработка» . . . 70
11.6.1 Замечания по применению . . . 70
11.6.2 Оценка функциональной спецификации (ADV_FSP.1) . . . 70
11.6.3 Оценка проекта верхнего уровня (ADV_HLD.1) . . . 74
11.6.4 Оценка соответствия представлений (ADV_RCR.1) . . . 76
11.7 Вид деятельности «Руководства» . . . 77
11.7.1 Замечания по применению . . . 77
11.7.2 Оценка руководства администратора (AGD_ADM.1) . . . 77
11.7.3 Оценка руководства пользователя (AGD_USR.1) . . . 79
11.8 Вид деятельности «Тестирование» . . . 81
11.8.1 Замечания по применению . . . 81
11.8.2 Оценка покрытия (ATE_COV.1) . . . 81
11.8.3 Оценка функциональных тестов (ATE_FUN.1) . . . 83
11.8.4 Оценка путем независимого тестирования (ATE_IND.2) . . . 86
11.9 Вид деятельности «Оценка уязвимостей» . . . 90
11.9.1 Оценка стойкости функций безопасности ОО (AVA_SOF.1) . . . 90
11.9.2 Оценка анализа уязвимостей (AVA_VLA.1) . . . 93
12 Оценка по ОУД3 . . . 97
12.1 Введение . . . 97
12.2 Цели . . . 97
12.3 Организация оценки по ОУД3 . . . 97
12.4 Вид деятельности «Управление конфигурацией» . . . 98
12.4.1 Оценка возможностей УК (ACM_CAP.3) . . . 98
12.4.2 Оценка области УК (ACM_SCP.1) . . . 101
12.5 Вид деятельности «Поставка и эксплуатация» . . . 101
12.5.1 Оценка поставки (ADO_DEL.1) . . . 101
12.5.2 Оценка установки, генерации и запуска (ADO_IGS.1) . . . 102
12.6 Вид деятельности «Разработка» . . . 103
12.6.1 Замечания по применению . . . 103
12.6.2 Оценка функциональной спецификации (ADV_FSP.1) . . . 104
12.6.3 Оценка проекта верхнего уровня (ADV_HLD.2) . . . 107
12.6.4 Оценка соответствия представлений (ADV_RCR.1) . . . 110

12.7 Вид деятельности «Руководства» . . . 111
12.7.1 Замечания по применению . . . 111
12.7.2 Оценка руководства администратора (AGD_ADM.1) . . . 111
12.7.3 Оценка руководства пользователя (AGD_USR.1) . . . 113
12.8 Вид деятельности «Поддержка жизненного цикла» . . . 115
12.8.1 Оценка безопасности разработки (ALC_DVS.1) . . . 115
12.9 Вид деятельности «Тестирование» . . . 117
12.9.1 Замечания по применению . . . 117
12.9.2 Оценка покрытия (ATE_COV.2) . . . 119
12.9.3 Оценка глубины (ATE_DPT.1) . . . 120
12.9.4 Оценка функциональных тестов (ATE_FUN.1) . . . 122
12.9.5 Оценка путем независимого тестирования (ATE_IND.2) . . . 126
12.10 Вид деятельности «Оценка уязвимостей» . . . 130
12.10.1 Оценка неправильного применения (AVA_MSU.1) . . . 130
12.10.2 Оценка стойкости функций безопасности ОО (AVA_SOF.1) . . . 132
12.10.3 Оценка анализа уязвимостей (AVA_VLA.1) . . . 134
13 Оценка по ОУД4 . . . 139
13.1 Введение . . . 139
13.2 Цели . . . 139
13.3 Организация оценки по ОУД4 . . . 139
13.4 Вид деятельности «Управление конфигурацией» . . . 139
13.4.1 Оценка автоматизации УК (ACM_AUT.1) . . . 140
13.4.2 Оценка возможностей УК (ACM_CAP.4) . . . 141
13.4.3 Оценка области УК (ACM_SCP.2) . . . 145
13.5 Вид деятельности «Поставка и эксплуатация» . . . 145
13.5.1 Оценка поставки (ADO_DEL.2) . . . 145
13.5.2 Оценка установки, генерации и запуска (ADO_IGS.1) . . . 147
13.6 Вид деятельности «Разработка» . . . 148
13.6.1 Замечания по применению . . . 148
13.6.2 Оценка функциональной спецификации (ADV_FSP.2) . . . 149
13.6.3 Оценка проекта верхнего уровня (ADV_HLD.2) . . . 152
13.6.4 Оценка представления реализации (ADV_IMP.1) . . . 155
13.6.5 Оценка проекта нижнего уровня (ADV_LLD.1) . . . 157
13.6.6 Оценка соответствия представлений (ADV_RCR.1) . . . 160
13.6.7 Оценка моделирования политики безопасности ОО (ADV_SPM.1) . . . 161
13.7 Вид деятельности «Руководства» . . . 164
13.7.1 Замечания по применению . . . 164
13.7.2 Оценка руководства администратора (AGD_ADM.1) . . . 165
13.7.3 Оценка руководства пользователя (AGD_USR.1) . . . 167
13.8 Вид деятельности «Поддержка жизненного цикла» . . . 169
13.8.1 Оценка безопасности разработки (ALC_DVS.1) . . . 169
13.8.2 Оценка определения жизненного цикла (ALC_LCD.1) . . . 171
13.8.3 Оценка инструментальных средств и методов (ALC_TAT.1) . . . 172
13.9 Вид деятельности «Тестирование» . . . 173
13.9.1.Замечания по применению . . . 173
13.9.2 Оценка покрытия (ATE_COV.2) . . . 175
13.9.3 Оценка глубины (ATE_DPT.1) . . . 176
13.9.4 Оценка функциональных тестов (ATE_FUN.1) . . . 178
13.9.5 Оценка путем независимого тестирования (ATE_IND.2) . . . 181
13.10 Вид деятельности «Оценка уязвимостей» . . . 186
13.10.1 Оценка неправильного применения (AVA_MSU.2) . . . 186
13.10.2 Оценка стойкости функций безопасности ОО (AVA_SOF.1) . . . 189
13.10.3 Оценка анализа уязвимостей (AVA_VLA.2) . . . 191

14 Подвид деятельности «Устранение недостатков» . . . 201
14.1 Оценка устранения недостатков (ALC_FLR.1) . . . 201
14.1.1 Цели . . . 201
14.1.2 Исходные данные . . . 201
14.1.3 Действие ALC_FLR.1.1E . . . 201
14.2 Оценка устранения недостатков (ALC_FLR.2) . . . 203
14.2.1 Цели . . . 203
14.2.2 Исходные данные . . . 203
14.2.3 Действие ALC_FLR.2.1E . . . 203
14.3 Оценка устранения недостатков (ALC_FLR.3) . . . 206
14.3.1 Цели . . . 206
14.3.2 Исходные данные . . . 206
14.3.3 Действие ALC_FLR.3.1E . . . 206
Приложение А(обязательное) Общие указания по оценке . . . 211
А.1 Цели . . . 211
А.2 Выборка . . . 211
А.3 Анализ непротиворечивости . . . 212
А.4 Зависимости . . . 213
А.4.1 Зависимости между видами деятельности . . . 213
А.4.2 Зависимости между подвидами деятельности . . . 214
А.4.3 Зависимости между действиями . . . 214
А.5 Посещение объектов . . . 214
А.6 Границы объекта оценки . . . 215
А.6.1 Продукт и система . . . 215
А.6.2 Объект оценки . . . 215
А.6.3 Функции безопасности объекта оценки . . . 215
А.6.4 Оценка . . . 215
А.6.5 Сертификация . . . 216
А.7 Угрозы и требования класса FPT . . . 216
А.7.1 Объекты оценки, для которых не обязательны требования класса FPT . . . 216
А.7.1.1 Объект оценки с ограниченным интерфейсом пользователя . . . 216
А.7.1.2 Объект оценки, не осуществляющий соответствующую политику безопасности . . . 217
А.7.1.3 Защита обеспечивается средой . . . 217
А.7.2 Воздействие на семейства доверия . . . 217
А.7.2.1 ADV . . . 217
А.7.2.2 AVA_VLA . . . 217
А.7.2.3 ATE_IND . . . 217
А.8 Стойкость функций безопасности и анализ уязвимостей . . . 217
А.8.1 Потенциал нападения . . . 218
А.8.1.1 Применение потенциала нападения . . . 218
А.8.1.2 Трактовка мотивации . . . 218
А.8.2 Вычисление потенциала нападения . . . 219
А.8.2.1 Идентификация и использование . . . 219
А.8.2.2 Учитываемые факторы . . . 219
А.8.2.3 Подход к вычислению . . . 220
А.8.3 Пример анализа стойкости функции . . . 222
А.9 Сфера ответственности системы оценки . . . 223
Приложение В (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 224

Введение

Международный стандарт ИСО/МЭК 18045:2005 подготовлен Совместным техническим комитетом ИСО/МЭК СТК 1 «Информационные технологии», Подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ». Идентичный ИСО/МЭК 18045:2005 текст опубликован организациями — спонсорами проекта «Общие критерии» как «Общая методология оценки безопасности информационных технологий», версия 2.3 (ОМО, версия 2.3).

Методология оценки безопасности информационных технологий (ИТ), представленная в настоящем стандарте, идентичном ИСО/МЭК 18045:2005, ограничена оценками для оценочных уровней доверия (ОУД) ОУД1 — ОУД4, определенных в ИСО/МЭК 15408:2005. Это не обеспечивает руководство для оценки по ОУД 5-7, а также для оценок, использующих другие пакеты доверия.

Потенциальные пользователи настоящего стандарта — прежде всего оценщики, применяющие ИСО/МЭК 15408, и органы по сертификации, подтверждающие действия оценщика, заявители оценки, разработчики, авторы профилей защиты (ПЗ) и заданий по безопасности (ЗБ) и другие стороны, заинтересованные в безопасности ИТ.

Настоящим стандартом признано, что не на все вопросы оценки безопасности ИТ можно найти в нем ответы и что дальнейшие интерпретации будут необходимы. В конкретных системах оценки должно быть решено, как обращаться с такими интерпретациями, хотя они могут быть подчинены соглашениям о взаимном признании. Список связанных с методологией вопросов, которые могут быть определены в конкретной системе оценки, приведен в приложении А.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Методология оценки безопасности информационных технологий

Information technology. Security techniques. Methodology for IT security evaluation

Дата введения — 2009 — 10 — 01

1 Область применения

Настоящий стандарт — нормативный документ, применяемый совместно с ИСО/МЭК 15408. Настоящий стандарт описывает минимум действий, выполняемых оценщиком при проведении оценки безопасности информационных технологий (ИТ) по ИСО/МЭК 15408 с использованием критериев и свидетельств оценки, определенных в ИСО/МЭК 15408.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты:

ИСО/МЭК 15408-1:2005 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель

ИСО/МЭК 15408-2:2005 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности

ИСО/МЭК 15408-3:2005 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты

ИСО 9000:2000 Системы менеджмента качества. Основные положения и словарь

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

Примечание – Для терминов, выделенных в тексте определений полужирным шрифтом, в настоящем разделе даны собственные определения.

3.1 **действие** (action): Элемент действий оценщика по ИСО/МЭК 15408-3. Эти действия или сформулированы в явном виде как действия оценщика, или неявно следуют из действий разработчика (подразумеваемые действия оценщика) в рамках компонентов доверия ИСО/МЭК 15408-3.

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

3.3 **проверить** (check): Вынести **вердикт** посредством простого сравнения, при этом специальные знания и опыт оценщика не требуются. В формулировке, в которой используется этот глагол, должно быть описано то, что подлежит сравнению.

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

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

Издание официальное

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

3.7 **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 должны быть подвергнуты анализу.

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

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

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

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

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

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

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

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

3.16 **подвид деятельности** (sub-activity): Применение компонента доверия ИСО/МЭК 15408-3. Семейства доверия прямо не рассматриваются в настоящем стандарте, поскольку при проведении оценки всегда используется только один компонент доверия из применяемого семейства.

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

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

3.19 **шаг оценивания** (work unit): Наименьшая структурная единица работ по оценке. Каждое действие в методологии оценки включает в себя один или несколько шагов оценивания, которые сгруппированы в пределах действия методологии оценки применительно к элементам содержания и представления свидетельств или элементам действий разработчика ИСО/МЭК 15408-3. Шаги оценивания представлены в настоящем стандарте в том же порядке, что и элементы ИСО/МЭК 15408-3, из которых они следуют. Шаги оценивания идентифицированы условным обозначением типа 4:ALC_TAT.1-2. В этом обозначении первая цифра *(4)* указывает на оценочный уровень доверия (ОУД), последовательность символов ALC_TAT.1 указывает на компонент ИСО/МЭК 15408-3 (т.е. на подвид деятельности из настоящего стандарта), а завершающая цифра *(2)* указывает, что это второй шаг оценивания в подвиде деятельности ALC_TAT.1.

4 Обозначения и сокращения

В настоящем стандарте применены следующие сокращения:

ЗБ (ST) — задание по безопасности;
ИТ (IT) — информационная технология;
ИФБО (TSFI) — интерфейс функции безопасности объекта оценки;
ОДФ (TSC) — область действия функции безопасности объекта оценки;
ОО (TOE) — объект оценки;
ОУД (EAL) — оценочный уровень доверия;
ПБО (TSP) — политика безопасности объекта оценки;
ПЗ (PP) — профиль защиты;

ПФБ (SFP) — политика функции безопасности;
СФБ (SOF) — стойкость функции безопасности;
СП (OR) — сообщение о проблеме;
ТОО (ETR) — технический отчет об оценке;
УК (CM) — управление конфигурацией;
ФБ (SF) — функция безопасности;
ФБО (TSF) — функции безопасности объекта оценки.

5 Краткий обзор

5.1 Структура стандарта

Раздел 6 определяет соглашения, используемые в настоящем стандарте.

В разделе 7 описаны общие задачи оценки без определения вердиктов, связанных с ними, поскольку эти задачи не отображаются на элементы действий оценщика из ИСО/МЭК 15408-3.

Раздел 8 определяет оценку профиля защиты.

Раздел 9 определяет оценку задания по безопасности.

В разделах 10—13 определены минимальные усилия по оценке, необходимые для успешного выполнения оценки по ОУД1—ОУД4, и предоставлено руководство по способам и средствам выполнения оценки.

Раздел 14 определяет виды деятельности по оценке устранения недостатков.

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

6 Принятые соглашения

6.1 Терминология

В отличие от ИСО/МЭК 15408, где каждый соответствующий элемент во всех компонентах одного семейства доверия имеет один и тот же номер, указанный последней цифрой его условного обозначения, настоящий стандарт может вводить новые шаги оценивания при изменении элемента действий оценщика из ИСО/МЭК 15408 в зависимости от подвида деятельности; в результате, последняя цифра условного обозначения последующих шагов оценивания изменится, хотя шаг оценивания останется тем же самым. Например, если для ОУД4 добавлен новый шаг оценивания, помеченный 4:ADV_FSP.2-7, то номера последующих шагов оценивания подвида деятельности FSP увеличиваются на единицу. Тогда шагу оценивания 3:ADV_FSP.1-8 соответствует шаг оценивания 4:ADV_FSP.2-9, хотя каждый из указанных шагов содержит одно и то же требование, их нумерация внутри своего подвида деятельности более не совпадает.

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

6.2 Применение глаголов

Любому основному глаголу описания шага оценивания или подзадачи предшествует вспомогательный глагол «должен». Вспомогательный глагол «должен» используют при обязательности содержащего его текста и, следовательно, только в рамках шага оценивания или подзадачи. Шаги оценивания и подзадачи содержат обязательные действия, которые оценщик должен выполнить, чтобы вынести вердикт.

Текст, сопровождающий шаги оценивания и подзадачи, содержит дальнейшие разъяснения использования формулировок ИСО/МЭК 15408 при оценке.

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

6.3 Общие указания по оценке

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

6.4 Взаимосвязь между структурами ИСО/МЭК 15408 и настоящего стандарта

Имеется прямая взаимосвязь между структурой ИСО/МЭК 15408 (класс-семейство-компонент-элемент) и структурой настоящего стандарта. Рисунок 1 иллюстрирует соответствие между такими конструкциями ИСО/МЭК 15408, как классы, компоненты и элементы действий оценщика, и рассматриваемыми в методологии оценки видами деятельности, подвидами деятельности и действиями. Некоторые шаги оценивания из методологии оценки могут следовать из требований ИСО/МЭК 15408, содержащихся в элементах действий разработчика или элементах содержания и представления свидетельств.

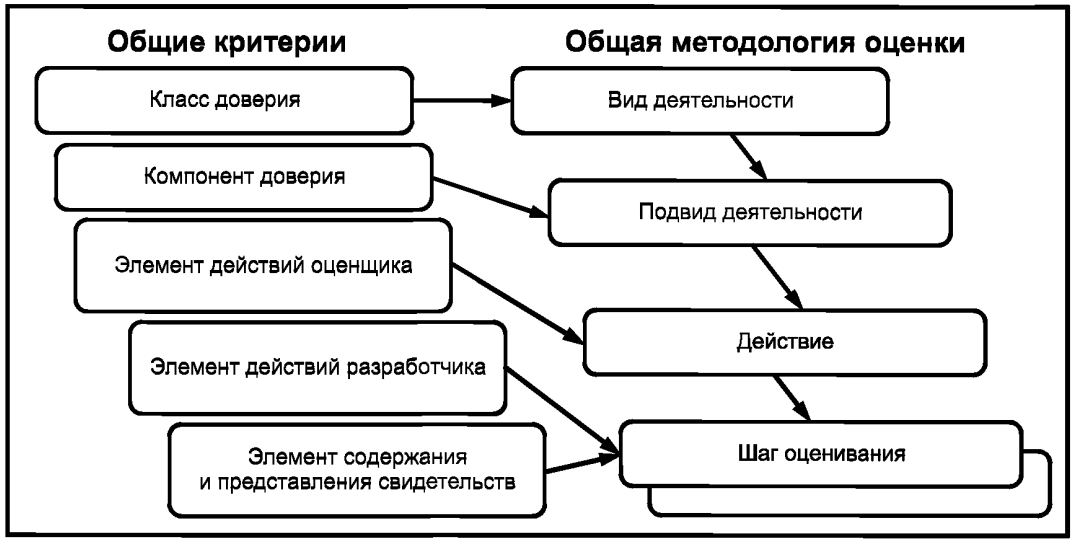


Рисунок 1 — Соотношение структур ИСО/МЭК 15408 и настоящего стандарта

6.5 Вердикты оценщика

Оценщик выносит вердикт относительно выполнения требований ИСО/МЭК 15408, а не требований настоящего стандарта. Наименьшая структурная единица ИСО/МЭК 15408, по которой выносят вердикт, — элемент действий оценщика (явный или подразумеваемый). Вердикт по выполняемому элементу действий оценщика из ИСО/МЭК 15408 выносят как результат выполнения соответствующего действия из методологии оценки и составляющих его шагов оценивания. В итоге результат оценки формируют в соответствии с ИСО/МЭК 15408-1 (подраздел 6.3).

В настоящем стандарте различают три взаимоисключающих вида вердикта:

a) условиями положительного вердикта являются завершение оценщиком элемента действий оценщика по ИСО/МЭК 15408 и определение, что при оценке требования к ПЗ, ЗБ или ОО выполнены. Для элемента действий оценщика условием положительного вердикта является успешное завершение всех шагов оценивания, составляющих соответствующее действие из методологии оценки;

b) условием неокончательного вердикта является незавершение оценщиком одного или нескольких шагов оценивания из действия, изложенного в методологии оценки, связанного с элементом действий оценщика по ИСО/МЭК 15408;

c) условиями отрицательного вердикта являются завершение оценщиком элемента действий оценщика из ИСО/МЭК 15408 и определение, что при оценке требования к ПЗ, ЗБ или ОО не выполнены.

Все вердикты сначала неокончательные и остаются такими до вынесения положительного или отрицательного вердикта.

Общий вердикт положительный тогда и только тогда, когда все составляющие вердикта положительные. В примере, показанном на рисунке 2, вердикт для одного из элементов действий оценщика отрицательный, поэтому вердикты для соответствующего компонента доверия, класса доверия и общий вердикт также отрицательные.

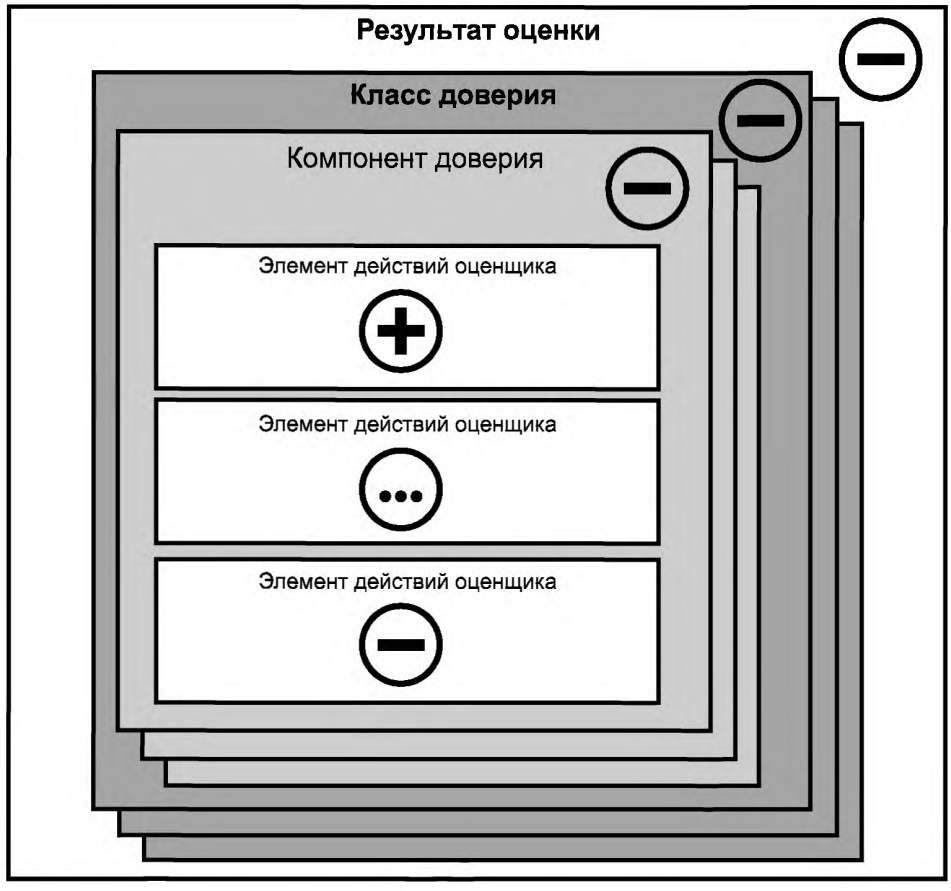


Рисунок 2 — Пример правила вынесения вердикта

7 Общие задачи оценки

7.1 Введение

Каждый тип оценки — оценка ПЗ или оценка ОО (в том числе оценка ЗБ), включает в себя две общие задачи для оценщика: задачу получения исходных данных для оценки и задачу оформления результатов оценки. Эти две задачи, которые относятся к управлению свидетельствами оценки и созданию отчетов, описаны в настоящем разделе. Каждая из задач включает в себя связанные с ней подзадачи, которые применяются и являются нормативными для всех типов оценок по ИСО/МЭК 15408 (оценка ПЗ или оценка ОО).

Несмотря на то, что ИСО/МЭК 15408 не предъявляет каких-либо конкретных требований к этим задачам оценки, такие требования там, где это необходимо, устанавливает настоящий стандарт. В отличие от видов деятельности, описанных в других местах настоящего стандарта, эти задачи не предполагают вынесения по ним каких-либо вердиктов, поскольку они не отображаются на элементы действий оценщика, изложенные в ИСО/МЭК 15408; их выполняют, чтобы обеспечить соответствие настоящему стандарту.

7.2 Задача получения исходных данных для оценки

7.2.1 Цели

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

7.2.2 Замечания по применению

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

заявителя. Поскольку требования доверия относятся к ОО в целом, то необходимо, чтобы оценщику были доступны свидетельства оценки, относящиеся ко всем продуктам, которые являются частями ОО. Область применения и требуемое содержание такого свидетельства оценки независимы от уровня контроля разработчиком каждого из продуктов, составляющих ОО. Например, если требуется проект верхнего уровня, то требования семейства ADV_HLD «Проект верхнего уровня» относятся ко всем подсистемам, осуществляющим ФБО. Кроме того, требования доверия, согласно которым необходимо выполнение определенных процедур (например, из семейств ACM_CAP «Возможности УК» и ADO_DEL «Поставка»), также относятся к ОО в целом (включая любой продукт другого разработчика).

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

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

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

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

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

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

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

7.2.3 Подзадача управления свидетельством оценки

7.2.3.1 Контроль конфигурации

Оценщик должен осуществлять контроль конфигурации свидетельства оценки.

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

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

7.2.3.2 Изъятие из использования

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

a) возврата свидетельств оценки;

b) архивирования свидетельств оценки;

c) уничтожения свидетельств оценки.

7.2.3.3 Конфиденциальность

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

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

7.3 Задача оформления результатов оценки

7.3.1 Цели

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

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

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

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

b) подготовку ТОО.

7.3.2 Замечания по применению

В настоящем стандарте требования обеспечения оценщика свидетельствами для поддержки переоценки и повторного использования в явном виде не сформулированы. Пока еще не определена информация, являющаяся результатом работы оценщика и способствующая проведению переоценки или повторного использования. Когда заявителю потребуется информация для переоценки или повторного использования, следует проконсультироваться в системе оценки, в которой была проведена оценка.

7.3.3 Подзадача подготовки СП

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

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

В любом СП оценщик должен привести следующее:

a) идентификатор оцениваемого ПЗ или ОО;

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

c) суть проблемы;

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

e) наименование организации, ответственной за решение вопроса;

f) рекомендуемые сроки решения;

g) влияние на оценку отрицательного результата решения проблемы.

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

7.3.4 Подзадача подготовки ТОО

7.3.4.1 Цели

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

ТОО может содержать информацию, являющуюся собственностью разработчика или заявителя.

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

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

ТОО помогает органу оценки вынести свой вердикт, но, предположительно, может не содержать всей необходимой для этого информации, а задокументированные результаты оценки могут не содержать необходимых в данной системе оценки свидетельств для подтверждения правильности выполненной оценки.

Этот фактор находится за рамками области действия настоящего стандарта и должен быть учтен посредством использования других методов надзора.

7.3.4.2 ТОО при оценке ПЗ

В настоящем подпункте приведено минимально необходимое содержание информации, включаемой в ТОО при оценке ПЗ. Содержание ТОО показано на рисунке 3; этот рисунок может быть использован как образец при построении структурной схемы ТОО.



Рисунок 3 — Содержание ТОО при оценке ПЗ

7.3.4.2.1 Введение

Оценщик должен привести в отчете идентификаторы системы оценки.

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

Оценщик должен привести в отчете идентификаторы контроля конфигурации ТОО.

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

Оценщик должен привести в отчете идентификаторы контроля конфигурации ПЗ.

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

Оценщик должен привести в отчете идентификатор разработчика.

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

Оценщик должен привести в отчете идентификатор заявителя.

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

Оценщик должен привести в отчете идентификатор оценщика.

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

7.3.4.2.2 Оценка

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

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

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

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

7.3.4.2.3 Результаты оценки

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

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

7.3.4.2.4 Выводы и рекомендации

Оценщик должен привести в отчете выводы по результатам оценки, в частности общий вердикт в соответствии с ИСО/МЭК 15408-1 (подраздел 6.3) и процедурой вынесения вердикта, описанной в 6.5 настоящего стандарта.

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

7.3.4.2.5 Перечень свидетельств оценки

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

- наименование составителя (например, разработчика, заявителя);
- наименование свидетельства оценки;
- уникальную ссылку (например, дату составления и номер версии).

7.3.4.2.6 Перечень сокращений/глоссарий терминов

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

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

7.3.4.2.7 Сообщения о проблемах

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

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

7.3.4.3 ТОО при оценке ОО

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



Рисунок 4 — Содержание ТОО при оценке ОО

7.3.4.3.1 Введение

Оценщик должен привести в отчете идентификаторы системы оценки.

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

Оценщик должен привести в отчете идентификаторы контроля конфигурации ТОО.

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

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

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

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

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

Оценщик должен привести в отчете идентификатор разработчика.

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

Оценщик должен привести в отчете идентификатор заявителя.

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

Оценщик должен привести в отчете идентификатор оценщика.

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

7.3.4.3.2 Описание архитектуры ОО

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

Назначение этого раздела состоит в указании степени архитектурного разделения главных компонентов. Если в ЗБ отсутствуют требования из семейства ADV_HLD «Проект верхнего уровня», этот раздел не применяют.

7.3.4.3.3 Оценка

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

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

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

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

7.3.4.3.4 Результаты оценки

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

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

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

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

Для видов деятельности «Оценка уязвимостей» и «Тестирование» указывают шаги оценивания, которые определяют информацию, включаемую в ТОО.

7.3.4.3.5 Выводы и рекомендации

Оценщик должен привести в отчете выводы по результатам оценки об удовлетворении ОО требованиям своего ЗБ, в частности общий вердикт в соответствии с ИСО/МЭК 15408-1 (подраздел 6.3) и процедурой вынесения вердикта, описанной в 6.5 настоящего стандарта.

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

7.3.4.3.6 Перечень свидетельств оценки

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

- наименование составителя (например, разработчика, заявителя);
- наименование свидетельства оценки;
- уникальную ссылку (например, дату составления и номер версии).

7.3.4.3.7 Перечень сокращений/глоссарий терминов

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

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

7.3.4.3.8 Сообщения о проблемах

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

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

7.3.5 Подвиды деятельности по оценке

Рисунок 5 представляет краткий обзор работы, которая будет выполнена для оценки.

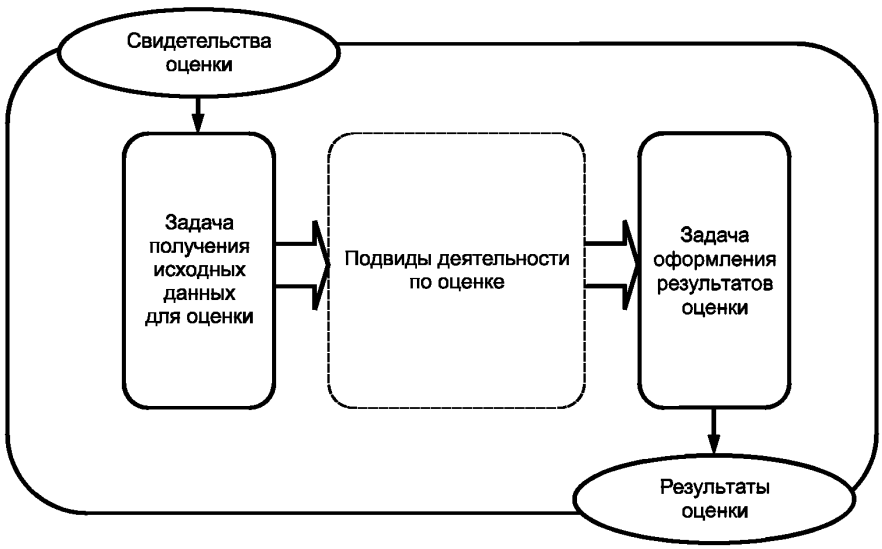


Рисунок 5 — Общая модель оценки

Свидетельства оценки могут варьироваться в зависимости от типа оценки (для оценки ПЗ требуется только ПЗ, в то время как для оценки ОО требуются предусмотренные для ОО свидетельства). Результаты оценки приводят в ТОО и, возможно, в сообщениях о проблемах (СП). Подвиды деятельности по оценке варьируются и, в случае с оценкой ОО, зависят от требований доверия по ИСО/МЭК 15408-3.

Разделы 8—13 организованы единообразно, основываясь на работах, требуемых при оценке. В разделе 8 рассмотрены работы, необходимые для достижения результатов оценки ПЗ. Раздел 9 связан с работами, необходимыми для оценки ЗБ, хотя для этих работ не предусмотрен отдельный результат оценки. Разделы 10—13 относятся к работам, необходимым для достижения результатов оценки по ОУД1 — ОУД4 (в сочетании с оценкой ЗБ). Каждый из этих разделов предусмотрен как автономный раздел и, следовательно, может содержать повторения текста, содержащегося в других разделах.

8 Оценка профиля защиты

8.1 Введение

Настоящий раздел описывает оценку ПЗ. Требования и методология оценки ПЗ идентичны для каждой оценки ПЗ независимо от ОУД (или другой совокупности критериев доверия), заявленного в ПЗ. В то время как последующие разделы настоящего стандарта ориентированы на проведение оценки по конкретным ОУД, настоящий раздел применим к любому оцениваемому ПЗ.

Методология оценки в настоящем разделе основана на требованиях к ПЗ, определенных в ИСО/МЭК 15408-1, приложение А и классе APE «Оценка профиля защиты» ИСО/МЭК 15408-3.

8.2 Организация оценки ПЗ

Виды деятельности по проведению полной оценки ПЗ охватывают следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) вид деятельности по оценке ПЗ, включающий в себя следующие подвиды деятельности:

1) оценку раздела «Описание ОО» (8.3.1);

2) оценку раздела «Среда безопасности ОО» (8.3.2);

3) оценку раздела «Введение ПЗ» (8.3.3);

4) оценку раздела «Цели безопасности» (8.3.4);

5) оценку раздела «Требования безопасности ИТ» (8.3.5);

7) оценку сформулированных в явном виде требований безопасности ИТ (8.3.6);

c) задачу оформления результатов оценки (раздел 7).

Задачи получения исходных данных для оценки и оформления результатов оценки описаны в разделе 7. Подвиды деятельности по оценке вытекают из требований доверия класса APE, содержащихся в ИСО/МЭК 15408-3.

В настоящем разделе описаны подвиды деятельности, включенные в оценку ПЗ. Хотя подвиды деятельности могут начинаться более или менее случайно, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком. Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

Подвид деятельности по оценке сформулированных в явном виде требований безопасности ИТ выполняют только тогда, когда в состав требований безопасности ИТ включены требования безопасности, взятые не из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3.

8.3 Вид деятельности «Оценка профиля защиты»

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

8.3.1.1 Цели

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

8.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.1.3 Действие APE_DES.1.1E

8.3.1.3.1 Шаг оценивания APE_DES.1-1

ИСО/МЭК 15408-3 APE_DES.1.1C: *Описание ОО должно включать в себя тип продукта и общие свойства ИТ, присущие ОО.*

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

Оценщик делает заключение, достаточно ли «Описание ОО» для общего понимания предполагаемого использования продукта или системы и обеспечивает ли, таким образом, контекст оценки. Примерами некоторых типов продуктов и систем являются: межсетевой экран, смарт-карта, криптомодем, веб-сервер, интрасеть.

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 рассмотрено в разделе «Описание ОО». Примером этого является ОО типа «межсетевой экран», в «Описании ОО» которого изложено, что он не может быть подключен к сетям.

8.3.1.3.2 Шаг оценивания APE_DES.1-2

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

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 этих характеристик.

8.3.1.4 Действие APE_DES.1.2E

8.3.1.4.1 Шаг оценивания APE_DES.1-3

Оценщик должен исследовать ПЗ, чтобы сделать заключение, является ли «Описание ОО» логически упорядоченным.

Изложение раздела «Описание ОО» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. разработчикам, оценщикам и потребителям).

8.3.1.4.2 Шаг оценивания APE_DES.1-4

Оценщик должен исследовать ПЗ, чтобы сделать заключение, является ли «Описание ОО» внутренне непротиворечивым.

Оценщику необходимо иметь в виду, что данный раздел ПЗ предназначен только для того, чтобы определить общее назначение ОО.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

8.3.1.5 Действие APE_DES.1.3E

8.3.1.5.1 Шаг оценивания APE_DES.1-5

Оценщик должен исследовать ПЗ, чтобы сделать заключение, согласовано ли «Описание ОО» с другими частями ПЗ.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

8.3.2.1 Цели

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

8.3.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.2.3 Действие APE_ENV.1.1E

8.3.2.3.1 Шаг оценивания APE_ENV.1-1

ИСО/МЭК 15408-3 APE_ENV.1.1C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждое предположение о предполагаемом применении ОО и среде использования ОО.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо предположения.

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

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

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

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

a) Физические аспекты включают в себя предположения, которые необходимо сделать относительно физического расположения ОО или подключенных периферийных устройств для того, чтобы ОО функционировал безопасным образом. Несколько примеров:

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

b) Аспекты, имеющие отношение к персоналу, включают в себя 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:

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

c) Аспекты внешних связей включают в себя 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:

- предполагают, что для хранения файлов регистрации, генерируемых ОО, доступным является, по крайней мере, 100 Мб внешнего дискового пространства;

- предполагают, что ОО является единственным приложением, не относящимся к операционной системе, выполняемым на отдельной рабочей станции;

- предполагают, что дисковод ОО для накопителей на гибком магнитном диске отключен;

- предполагают, что ОО не будет подключен к недоверенной сети.

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 четкими и понятными, то это может, в конечном счете, привести к тому, что ОО будет использован в среде, в которой он не будет функционировать безопасным образом.

8.3.2.3.2 Шаг оценивания APE_ENV.1-2

ИСО/МЭК 15408-3 APE_ENV.1.2C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждую известную или предполагаемую угрозу активам, от которой будет требоваться защита посредством ОО или его среды.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо угрозы.

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 таком случае данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

8.3.2.3.3 Шаг оценивания APE_ENV.1-3

ИСО/МЭК 15408-3 APE_ENV.1.3C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо политики безопасности организации.

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 таком случае данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Оценщик делает заключение, изложена ли политика безопасности организации в виде правил, практических приемов или руководств, установленных организацией, контролирующей среду использования ОО, которым должен следовать ОО или его среда. Примером политики безопасности организации является требование генерации и шифрования паролей в соответствии с национальным стандартом.

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

8.3.2.4 Действие APE_ENV.1.2E

8.3.2.4.1 Шаг оценивания APE_ENV.1-4

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

Изложение раздела «Среда безопасности ОО» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

8.3.2.4.2 Шаг оценивания APE_ENV.1-5

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

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

a) изложение раздела «Среда безопасности ОО», которое содержит угрозу, метод нападения для которой не может быть реализован источником угрозы;

b) изложение раздела «Среда безопасности ОО», которое содержит правило политики безопасности организации «ОО не должен быть подключен к Интернету» и угрозу, источником которой является злоумышленник из Интернета.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

8.3.3.1 Цели

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

8.3.3.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.3.3 Действие APE_INT.1.1E

8.3.3.3.1 Шаг оценивания APE_INT.1-1

ИСО/МЭК 15408-3 APE_INT.1.1C: *Введение ПЗ должно содержать данные идентификации ПЗ, которые предоставляют маркировку и описательную информацию, необходимые для идентификации, каталогизации, регистрации ПЗ и ссылок на него.*

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

Оценщик делает заключение, включает ли в себя идентификационная информация ПЗ:

a) информацию, необходимую для контроля и уникальной идентификации ПЗ (например, наименование ПЗ, номер версии, дату публикации, авторов, организацию-заявителя);

b) указание версии ИСО/МЭК 15408, использованной при разработке ПЗ;

c) регистрационную информацию, если перед оценкой ПЗ был зарегистрирован;

d) перекрестные ссылки, если ПЗ сопоставляется с другим (другими) ПЗ;

e) дополнительную информацию в соответствии с требованиями системы оценки.

8.3.3.3.2 Шаг оценивания APE_INT.1-2

ИСО/МЭК 15408-3 APE_INT.1.2C: *Введение ПЗ должно содержать аннотацию ПЗ с общей характеристикой ПЗ в описательной форме.*

Оценщик должен проверить, представлена ли в разделе «Введение ПЗ» «Аннотация ПЗ» в повествовательной форме.

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

8.3.3.4 Действие APE_INT.1.2E

8.3.3.4.1 Шаг оценивания APE_INT.1-3

Оценщик должен исследовать «Введение ПЗ», чтобы сделать заключение, является ли оно логически упорядоченным.

«Введение ПЗ» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. разработчикам, оценщикам и потребителям).

8.3.3.4.2 Шаг оценивания APE_INT.1-4

Оценщик должен исследовать «Введение ПЗ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

8.3.3.5 Действие APE_INT.1.3E

8.3.3.5.1 Шаг оценивания APE_INT.1-5

Оценщик должен исследовать ПЗ, чтобы сделать заключение, согласовано ли «Введение ПЗ» с другими частями ПЗ.

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 предполагается ли в нем наличие характеристик безопасности, которые выходят за рамки оценки.

Оценщик также делает заключение, согласовано ли «Утверждение о соответствии ИСО/МЭК 15408» с другими частями ПЗ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

8.3.4 Оценка раздела «Цели безопасности» (APE_OBJ.1)

8.3.4.1 Цели

Цель данного подвида деятельности — сделать заключение, полностью ли и согласованно описаны цели безопасности, направлены ли цели безопасности на противостояние идентифицированным угрозам,

на достижение идентифицированной политики безопасности организации и согласованы ли они с приведенными предположениями.

8.3.4.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.4.3 Действие APE_OBJ.1.1E

8.3.4.3.1 Шаг оценивания APE_OBJ.1-1

ИСО/МЭК 15408-3 APE_OBJ.1.1C: *Изложение целей безопасности должно определить цели безопасности для ОО и его среды.*

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

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

8.3.4.3.2 Шаг оценивания APE_OBJ.1-2

ИСО/МЭК 15408-3 APE_OBJ.1.2C: *Цели безопасности для ОО должны быть сопоставлены с теми аспектами идентифицированных угроз, которым будет противостоять ОО, и/или с политикой безопасности организации, которая будет выполняться ОО.*

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

Оценщик делает заключение, прослежена ли каждая цель безопасности для ОО, по крайней мере, к одной угрозе или политике безопасности организации.

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.

Поэтому угрозе полностью может соответствовать одна или более цель для среды. Крайний случай — это когда отсутствуют цели безопасности для ОО. Хотя и в этом случае использование конструкции ПЗ/ЗБ остается правомерным, определение ОО, для которого все угрозы и политики безопасности организации учитываются средой, вряд ли бы имело какой-то практический смысл, так как для такого ОО не было бы никаких функциональных требований безопасности. Решение о сертификации подобных ОО является прерогативой системы оценки.

8.3.4.3.3 Шаг оценивания APE_OBJ.1-3

ИСО/МЭК 15408-3 APE_OBJ.1.3C: *Цели безопасности для среды должны быть сопоставлены с теми аспектами идентифицированных угроз, которым ОО противостоит не полностью, и/или с политикой безопасности организации или предположениями, не полностью выполняемыми ОО.*

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, прослежены ли цели безопасности для среды к тем 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.

Оценщик делает заключение, прослежена ли каждая цель безопасности для среды, по крайней мере, к одному предположению, угрозе или политике безопасности организации.

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.

8.3.4.3.4 Шаг оценивания APE_OBJ.1-4

ИСО/МЭК 15408-3 APE_OBJ.1.4C: *Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.*

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

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

Оценщик делает заключение, демонстрирует ли логическое 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.

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.

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).

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.

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.

Несмотря на то, что прослеживание целей безопасности к угрозам в обосновании целей безопасности может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является только заявлением, отражающим намерение предотвратить реализацию конкретной угрозы, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

8.3.4.3.5 Шаг оценивания APE_OBJ.1-5

ИСО/МЭК 15408-3 APE_OBJ.1.5C: *Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.*

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого аспекта политики безопасности организации приемлемое логическое обоснование того, что цели безопасности покрывают данный аспект политики безопасности организации.

Если ни одна цель безопасности не прослежена к политике безопасности организации, то результат данного шага оценивания отрицательный.

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

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

Несмотря на то, что прослеживание целей безопасности к политике безопасности организации в обосновании целей безопасности может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является только заявлением, отражающим намерение реализовать конкретную политику безопасности, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

8.3.4.3.6 Шаг оценивания APE_OBJ.1-6

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

Если ни одна цель безопасности для среды не прослежена к приведенному предположению, то результат данного шага оценивания отрицательный.

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

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

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.

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

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.

Несмотря на то, что прослеживание целей безопасности для среды к предположениям относительно среды использования ОО в подразделе «Обоснование целей безопасности» может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности представляет собой перефразированное предположение, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

8.3.4.4 Действие APE_OBJ.1.2E

8.3.4.4.1 Шаг оценивания APE_OBJ.1-7

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно логически упорядоченным.

Изложение раздела «Цели безопасности» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

8.3.4.4.2 Шаг оценивания APE_OBJ.1-8

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно полным.

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 быть выполнен совместно с шагами оценивания APE_OBJ.1-4, APE_OBJ.1-5 и APE_OBJ.1-6.

8.3.4.4.3 Шаг оценивания APE_OBJ.1-9

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

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».

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

8.3.5.1 Цели

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.

8.3.5.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.5.3 Действие APE_REQ.1.1E

8.3.5.3.1 Шаг оценивания APE_REQ.1-1

ИСО/МЭК 15408-3 APE_REQ.1.1C: *Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований ИСО/МЭК 15408-2.*

Оценщик должен проверить изложение функциональных требований безопасности ОО, чтобы сделать заключение, идентифицированы ли в нем функциональные требования безопасности ОО, составленные из компонентов функциональных требований по ИСО/МЭК 15408-2.

Оценщик делает заключение, что все компоненты функциональных требований безопасности ОО, взятые из ИСО/МЭК 15408-2, идентифицированы либо путем ссылки на отдельные компоненты по ИСО/МЭК 15408-2, либо путем воспроизведения их в ПЗ.

8.3.5.3.2 Шаг оценивания APE_REQ.1-2

Оценщик должен проверить, что каждая ссылка на компонент функциональных требований безопасности ОО является правильной.

Для каждой ссылки на компонент функционального требования безопасности ОО по ИСО/МЭК 15408-2 оценщик делает заключение, существует ли упомянутый компонент в ИСО/МЭК 15408-2.

8.3.5.3.3 Шаг оценивания APE_REQ.1-3

Оценщик должен проверить, что каждый компонент функциональных требований безопасности ОО, взятый из ИСО/МЭК 15408-2 и воспроизведенный в ПЗ, воспроизведен правильно.

Оценщик делает заключение, правильно ли воспроизведены требования в подразделе «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.

8.3.5.3.4 Шаг оценивания APE_REQ.1-4

ИСО/МЭК 15408-3 APE_REQ.1.2C: *Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия ИСО/МЭК 15408-3.*

Оценщик должен проверить изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, идентифицированы ли в нем требования доверия к безопасности ОО, составленные из компонентов требований доверия ИСО/МЭК 15408-3.

Оценщик делает заключение, все ли компоненты требований доверия к безопасности ОО, взятые из ИСО/МЭК 15408-3, идентифицированы либо путем ссылки на некоторый ОУД, либо на отдельные компоненты из ИСО/МЭК 15408-3, либо путем их воспроизведения в ПЗ.

8.3.5.3.5 Шаг оценивания APE_REQ.1-5

Оценщик должен проверить, что каждая ссылка на компоненты требований доверия к безопасности ОО является правильной.

Для каждой ссылки на компонент требований доверия к безопасности ОО по ИСО/МЭК 15408-3 оценщик делает заключение, существует ли упомянутый компонент в ИСО/МЭК 15408-3.

8.3.5.3.6 Шаг оценивания APE_REQ.1-6

Оценщик должен проверить, что каждый компонент требований доверия к безопасности ОО, взятый из ИСО/МЭК 15408-3 и воспроизведенный в ПЗ, воспроизведен правильно.

Оценщик делает заключение, правильно ли воспроизведены требования в подразделе «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.

8.3.5.3.7 Шаг оценивания APE_REQ.1-7

ИСО/МЭК 15408-3 APE_REQ.1.3C: *В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в ИСО/МЭК 15408-3.*

Оценщик должен исследовать изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, содержит ли оно ОУД, определенный в ИСО/МЭК 15408-3, либо в нем логически обосновано отсутствие ОУД.

Если никакой из ОУД не включен, то оценщик делает заключение, указана ли в логическом обосновании причина невключения ОУД в подраздел «Требования доверия к безопасности ОО». Это логическое 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 «Возможности УК», ADO_IGS «Установка, генерация и запуск», ADV_FSP «Функциональная спецификация», ADV_RCR «Соответствие представлений», AGD_ADM «Руководство администратора», AGD_USR «Руководство пользователя» и ATE_IND «Независимое тестирование»).

8.3.5.3.8 Шаг оценивания APE_REQ.1-8

ИСО/МЭК 15408-3 APE_REQ.1.4C: *Свидетельство должно содержать логическое обоснование, что изложение требований доверия к ОО является соответствующим.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, достаточно ли логично в нем обосновано то, что изложение требований доверия к безопасности ОО является приемлемым.

Если требования доверия содержат какой-либо ОУД, то в логическом 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 логическое обоснование каждого такого усиления. Если подраздел «Требования доверия к безопасности ОО» содержит требования доверия, сформулированные в явном виде, оценщик делает заключение, приведено ли логическое обоснование использования каждого сформулированного в явном виде требования доверия.

Оценщик делает заключение, дано ли в подразделе «Обоснование требований безопасности» достаточно логичное 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 «Анализ уязвимостей разработчиком», который является несвойственным для обнаружения недостатков безопасности, не являющихся очевидными.

Логическое обоснование может также включать в себя основания, подобные следующим:

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

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

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

d) требования потребителей.

Краткий обзор назначения и целей для каждого ОУД приведен в ИСО/МЭК 15408-3, подраздел 10.2.

Оценщику необходимо иметь в виду, что заключение о том, являются ли требования доверия приемлемыми, может быть субъективным, а значит, анализ достаточности логического обоснования не следует проводить слишком строго.

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.

8.3.5.3.9 Шаг оценивания APE_REQ.1-9

ИСО/МЭК 15408-3 APE_REQ.1.5C: *ПЗ должен, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.*

Оценщик должен проверить, что в ПЗ, при необходимости, идентифицированы требования безопасности для среды ИТ.

Если ПЗ не содержит требований безопасности для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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 «Аудит безопасности» и FIA «Идентификация и аутентификация».

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

Пример зависимости от среды ИТ — программный криптомодуль, который периодически проверяет свой код и, в случае обнаружения несанкционированной модификации, самоотключается. Для обеспечения возможности восстановления предусмотрено требование FPT_RCV.2 «Автоматическое восстановление». Поскольку криптомодуль не может самостоятельно восстановить свой код после самоотключения, то требование по восстановлению становится требованием к среде ИТ. Одной из зависимостей компонента FPT_RCV.2 «Автоматическое восстановление» является компонент AGD_ADM.1 «Руководство администратора». Следовательно, это требование доверия становится требованием доверия для среды ИТ.

Оценщику необходимо иметь в виду, что ссылка требований безопасности для среды ИТ на ФБО относится к функциям безопасности среды, а не к функциям безопасности ОО.

8.3.5.3.10 Шаг оценивания APE_REQ.1-10

ИСО/МЭК 15408-3 APE_REQ.1.6C: *Все завершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.*

Оценщик должен проверить, что все завершенные операции над требованиями безопасности ИТ идентифицированы.

Допустимо, чтобы ПЗ содержал элементы с незавершенными операциями, т.е. ПЗ может содержать формулировки функциональных требований безопасности, которые включают в себя незавершенные операции «назначение» или «выбор». Данные операции должны быть впоследствии завершены в ЗБ, отобра-

жающем этот ПЗ, что позволяет разработчику ЗБ проявлять большую гибкость при разработке ОО и соответствующего ЗБ, в котором утверждается о соответствии конкретному ПЗ.

Разрешенными операциями для компонентов по ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 являются «назначение», «итерация», «выбор» и «уточнение». Операции «назначение» и «выбор» разрешены только в специально обозначенных местах компонента. Операции «итерация» и «уточнение» разрешены для всех компонентов.

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.

8.3.5.3.11 Шаг оценивания APE_REQ.1-11

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, корректно ли выполнены операции.

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

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

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

b) 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 необходим 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);

c) для операции «уточнение» — уточнен ли компонент таким образом, что ОО, удовлетворяющий уточненному требованию, также удовлетворяет и неуточненному требованию. Если уточненное требование выходит за эти рамки, то его считают расширенным требованием.

Пример: ADV_SPM.1.2C — Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, 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, что моделировать следует только управление доступом, то это уточнение не является правомерным.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, а именно переформулирование предложения в соответствии с правилами 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 необходимо иметь в виду, что редакционные уточнения должны быть четко идентифицированы (см. шаг оценивания APE_REQ.1-10);

d) 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.

8.3.5.3.12 Шаг оценивания APE_REQ.1-12

ИСО/МЭК 15408-3 APE_REQ.1.7C: *Любые незавершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.*

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

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.

8.3.5.3.13 Шаг оценивания APE_REQ.1-13

ИСО/МЭК 15408-3 APE_REQ.1.8C: *Зависимости между требованиями безопасности ИТ, включенными в ПЗ, следует удовлетворить.*

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, удовлетворены ли зависимости, требуемые компонентами, используемыми при изложении раздела «Требования безопасности ИТ».

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

Хотя ИСО/МЭК 15408 поддерживает проведение анализа зависимостей путем их включения в описание компонентов требований, сам по себе данный факт не является логическим обоснованием того, что никакие другие зависимости не существуют. 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 перечислены данные объекты или субъекты.

Зависимости требований безопасности для среды ИТ следует излагать и удовлетворять в ПЗ.

Оценщику необходимо иметь в виду, что в соответствии с ИСО/МЭК 15408 не требуется, чтобы все зависимости были удовлетворены: см. следующий шаг оценивания.

8.3.5.3.14 Шаг оценивания APE_REQ.1-14

ИСО/МЭК 15408-3 APE_REQ.1.9C: *Свидетельство должно содержать логическое обоснование каждого неудовлетворения зависимостей.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое логическое обоснование для каждого случая, когда зависимости требований безопасности не удовлетворены.

Оценщик с учетом идентифицированных целей безопасности делает заключение, объяснено ли в логическом обосновании, почему удовлетворение зависимости не требуется.

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

Пример приемлемого логического 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 логическое 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 не способны 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».

8.3.5.3.15 Шаг оценивания APE_REQ.1-15

ИСО/МЭК 15408-3 APE_REQ.1.10C: *ПЗ должен включать в себя изложение приемлемого минимального уровня стойкости функций безопасности (СФБ) для функциональных требований безопасности ОО: базовой, средней или высокой СФБ.*

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.

Если требования доверия к безопасности ОО не включают в себя компонент AVA_SOF.1 «Оценка стойкости функции безопасности ОО», то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Стойкость криптографических алгоритмов находится вне области действия ИСО/МЭК 15408. Стойкость функции безопасности применяют 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 ИСО/МЭК 15408. Когда такие криптографические механизмы входят в состав ОО, то оценщик делает заключение, представлено ли в ПЗ четкое изложение того, что оценка стойкости криптографических алгоритмов не является частью оценки.

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.

Примером этого является распределенная терминальная система, включающая в себя 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, соответствующих 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.

8.3.5.3.16 Шаг оценивания APE_REQ.1-16

ИСО/МЭК 15408-3 APE_REQ.1.11C: *При изложении требований безопасности должны быть идентифицированы все функциональные требования безопасности, для которых требуется явное заявление стойкости функции, с явным заявлением стойкости функции для каждого такого функционального требования безопасности.*

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.

Если подраздел «Требования доверия к безопасности ОО» не содержит компонент AVA_SOF.1 «Оценка стойкости функции безопасности ОО», то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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. Данный шаг оценивания относится к тому случаю, когда автор ПЗ требует определить конкретные требования СФБ (т.е. выше, чем общее требование к СФБ в ПЗ) или — конкретную метрику СФБ. Конкретные требования к СФБ для функциональных требований безопасности ОО могут быть определены автором ПЗ. При отсутствии каких-либо конкретных требований к СФБ общее требование к СФБ в ПЗ применяют ко всем функциональным требованиям безопасности ОО, изложенным в ПЗ. Оценщику следует удостовериться, что наличие или отсутствие требований к СФБ, сформулированных в явном виде, согласовано с другими частями данного ПЗ.

Потенциально в ПЗ определения требований к СФБ могут варьироваться. В ПЗ может иметься общее требование к СФБ, кроме того, в рамках ПЗ для конкретных функциональных требований безопасности ОО могут иметься требования к СФБ, определенные специально для этих функциональных требований.

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

8.3.5.3.17 Шаг оценивания APE_REQ.1-17

ИСО/МЭК 15408-3 APE_REQ.1.12C: *Обоснование требований безопасности должно демонстрировать, что минимальный уровень стойкости функции в ПЗ, как и каждое явное указание стойкости функции, согласуются с целями безопасности ОО.*

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.

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

Оценщик делает заключение, учтены ли в подразделе «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.

Оценщик также делает заключение, учтены ли в подразделе «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 в себя соответствующее утверждение о стойкости связанных с этими требованиями функций безопасности.

8.3.5.3.18 Шаг оценивания APE_REQ.1-18

ИСО/МЭК 15408-3 APE_REQ.1.13C: *Обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.*

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности ОО к целям безопасности для ОО.

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

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

Допустимо также, но необязательно, прослеживание отдельных или всех требований доверия к безопасности ОО к целям безопасности для ОО.

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 «Номера версий», и поэтому разработчик ПЗ прослеживает данный компонент к рассматриваемой цели безопасности для ОО.

8.3.5.3.19 Шаг оценивания APE_REQ.1-19

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности для среды ИТ к целям безопасности для среды.

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

Неудача при попытке 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.

Допустимо также, но необязательно, для некоторых или всех требований доверия к безопасности для среды ИТ прослеживание к целям безопасности для среды.

8.3.5.3.20 Шаг оценивания APE_REQ.1-20

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

Если никакие требования безопасности ОО не прослежены к конкретной цели безопасности для ОО, то результат данного шага оценивания отрицательный.

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

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

Несмотря на то, что прослеживание от требований безопасности ОО к целям безопасности для ОО, представленное в подразделе «Обоснование требований безопасности», может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

8.3.5.3.21 Шаг оценивания APE_REQ.1-21

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, содержит ли он для каждой цели безопасности для среды ИТ приемлемое логическое обосно-

вание, что требования безопасности для среды ИТ пригодны для удовлетворения данной цели безопасности для среды ИТ.

Если никакие требования безопасности для среды ИТ не прослежены к конкретной цели безопасности для среды ИТ, то результат данного шага оценивания отрицательный.

Оценщик делает заключение, демонстрирует ли логическое 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.

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.

Несмотря на то, что прослеживание требований безопасности для среды ИТ к целям безопасности для среды ИТ, представленное в подразделе «Обоснование требований безопасности», может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

8.3.5.3.22 Шаг оценивания APE_REQ.1-22

ИСО/МЭК 15408-3 APE_REQ.1.14C: *Обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.*

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он внутреннюю непротиворечивость совокупности требований безопасности ИТ.

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, приведено приемлемое логическое обоснование отсутствия таких противоречий.

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. Сюда может входить 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.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

8.3.5.3.23 Шаг оценивания APE_REQ.1-23

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

Данный шаг оценивания основан 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.

Данный шаг оценивания основан также на анализе зависимостей, выполняемом на предыдущих шагах оценивания, поскольку если функциональное требование А имеет зависимость от функционального требования В, то В поддерживает А по определению.

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

a) на предотвращение обхода механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_RVM.1 «Невозможность обхода ПБО»;

b) на предотвращение вмешательства в работу механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_SEP «Разделение домена»;

c) на предотвращение деактивации механизмов, реализующих другие функциональные требования безопасности, такие, например, как FMT_MOF.1 «Управление режимом выполнения функций безопасности»;

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

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

8.3.5.4 Действие APE_REQ.1.2E

8.3.5.4.1 Шаг оценивания APE_REQ.1-24

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно логически упорядоченным.

Изложение требований безопасности ИТ является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

8.3.5.4.2 Шаг оценивания APE_REQ.1-25

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно полным.

При выполнении данного шага оценивания используют 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».

Изложение раздела «Требования безопасности ИТ» является полным, если оценщик считает требования безопасности достаточными для того, чтобы удостовериться, что все цели безопасности для ОО удовлетворены.

8.3.5.4.3 Шаг оценивания APE_REQ.1-26

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

При выполнении данного шага оценивания используют 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».

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.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

8.3.6.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли функциональные требования и/или требования доверия к безопасности, сформулированные без ссылки на ИСО/МЭК 15408, приемлемыми и адекватными.

8.3.6.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ПЗ.

8.3.6.3 Замечания по применению

Этот пункт применяют только в случае, если в ПЗ содержатся требования безопасности, сформулированные в явном виде без ссылки на ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. В противном случае все шаги оценивания, описанные в данном пункте, не применяют и поэтому считают удовлетворенными.

Требования семейства APE_SRE «Требования безопасности ИТ, сформулированные в явном виде» не заменяют требования семейства APE_REQ «Требования безопасности ИТ», а являются дополнительными к ним. Это означает, что требования безопасности, сформулированные в явном виде без ссылки на ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, должны быть оценены на соответствие критериям семейства APE_SRE, а также в сочетании со всеми остальными требованиями безопасности – на соответствие критериям семейства APE_REQ.

8.3.6.4 Действие APE_SRE.1.1E

8.3.6.4.1 Шаг оценивания APE_SRE.1-1

ИСО/МЭК 15408-3 APE_SRE.1.1C: *Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.*

Оценщик должен проверить, что в изложении раздела «Требования безопасности ИТ» идентифицированы все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408.

Необходимо, чтобы все функциональные требования безопасности ОО, которые не специфицированы на основе функциональных компонентов из ИСО/МЭК 15408-2, были четко идентифицированы как таковые. Аналогично необходимо, чтобы все требования доверия к безопасности ОО, которые не специфицированы на основе компонентов доверия из ИСО/МЭК 15408-3, были четко идентифицированы как таковые.

8.3.6.4.2 Шаг оценивания APE_SRE.1-2

ИСО/МЭК 15408-3 APE_SRE.1.2C: *Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.*

Оценщик должен проверить, что в изложении раздела «Требования безопасности ИТ» идентифицированы все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408.

Необходимо, чтобы все функциональные требования безопасности для среды ИТ, которые не специфицированы на основе функциональных компонентов из ИСО/МЭК 15408-2, были четко идентифицированы как таковые. Аналогично необходимо, чтобы все требования доверия к среде ИТ, которые не специфицированы на основе компонентов доверия по ИСО/МЭК 15408-3, были четко идентифицированы как таковые.

8.3.6.4.3 Шаг оценивания APE_SRE.1-3

ИСО/МЭК 15408-3 APE_SRE.1.3C: *Свидетельство должно содержать логическое обоснование, почему требования безопасности должны быть сформулированы в явном виде.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое логическое обоснование, почему каждое из сформулированных в явном виде требований безопасности пришлось сформулировать в явном виде.

Оценщик для каждого сформулированного в явном виде требования безопасности ИТ делает заключение, объяснено ли в логическом обосновании, почему существующие функциональные компоненты или компоненты доверия (из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 соответственно) не могли быть использованы для выражения требований безопасности, сформулированных в явном виде. При вынесении заключения оценщик принимает во внимание возможность выполнения операций (т.е. назначение, итерация, выбор и уточнение) над этими существующими компонентами.

8.3.6.4.4 Шаг оценивания APE_SRE.1-4

ИСО/МЭК 15408-3 APE_SRE.1.4C: *Сформулированные в явном виде требования безопасности ИТ должны использовать компоненты, семейства и классы требований ИСО/МЭК 15408 как образец для представления.*

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 по ИСО/МЭК 15408.

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 ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. Оценщик также делает заключение, разделены ли функциональные требования на отдельные функциональные элементы и определяют ли требования доверия элементы действий разработчика, содержания и представления свидетельств, а также действий оценщика.

8.3.6.4.5 Шаг оценивания APE_SRE.1-5

ИСО/МЭК 15408-3 APE_SRE.1.5C: *Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать объективные требования оценки, такие, чтобы соответствие или несоответствие им ОО могло быть определено и последовательно продемонстрировано.*

Оценщик должен исследовать каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, измеримо ли оно и устанавливает ли объективные требования оценки такие, что соответствие или несоответствие им ОО может быть определено и продемонстрировано систематическим методом.

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 необходимости вынесения о них субъективного суждения со стороны оценщика.

Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны быть использованы как образец.

8.3.6.4.6 Шаг оценивания APE_SRE.1-6

ИСО/МЭК 15408-3 APE_SRE.1.6C: *Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.*

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

Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны быть использованы как образец.

8.3.6.4.7 Шаг оценивания APE_SRE.1-7

ИСО/МЭК 15408-3 APE_SRE.1.7C: *Обоснование требований безопасности должно демонстрировать, что требования доверия применимы и пригодны для поддержки каждого из сформулированных в явном виде функциональных требований безопасности ОО.*

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.

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).

8.3.6.5 Действие APE_SRE.1.2E

8.3.6.5.1 Шаг оценивания APE_SRE.1-8

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

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

Примеры возможных зависимостей: компоненты класса FAU «Аудит безопасности», если в сформулированном в явном виде функциональном требовании упоминается аудит; компоненты семейства ADV_IMP «Представление реализации», если в сформулированном в явном виде требовании доверия упоминается исходный код или представление реализации ОО.

9 Оценка задания по безопасности

9.1 Введение

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

Требования и методология оценки ЗБ идентичны для каждой оценки ЗБ независимо от ОУД (или другой совокупности критериев доверия), заявленного в ЗБ. В то время как последующие разделы настоящего стандарта ориентированы на проведение оценки по конкретным ОУД, настоящий раздел применим к любому ЗБ, подвергаемому оценке.

Методология оценки в настоящем разделе основана на требованиях к ЗБ, определенных в ИСО/МЭК 15408-1, приложение В и классе ASE «Оценка задания по безопасности» ИСО/МЭК 15408-3.

9.2 Организация оценки ЗБ

Виды деятельности по проведению полной оценки ЗБ охватывают следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) вид деятельности по оценке ЗБ, включающий в себя следующие подвиды деятельности:

1) оценку раздела «Описание ОО» (9.3.1);

2) оценку раздела «Среда безопасности ОО» (9.3.2);

3) оценку раздела «Введение ЗБ» (9.3.3);

4) оценку раздела «Цели безопасности» (9.3.4);

5) оценку раздела «Утверждения о соответствии ПЗ» (9.3.5);

6) оценку раздела «Требования безопасности ИТ» (9.3.6);

7) оценку сформулированных в явном виде требований безопасности ИТ (9.3.7);

8) оценку раздела «Краткая спецификация ОО» (9.3.8);

c) задачу оформления результатов оценки (раздел 7).

Задачи получения исходных данных для оценки и оформления результатов оценки описаны в разделе 7. Подвиды деятельности по оценке вытекают из требований доверия класса ASE, содержащихся в ИСО/МЭК 15408-3.

В настоящем разделе описаны подвиды деятельности, включенные в оценку ЗБ. Хотя подвиды деятельности могут начинаться более или менее случайно, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком. Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

Необходимость выполнения подвидов деятельности по оценке утверждений о соответствии ПЗ и по оценке сформулированных в явном виде требований безопасности ИТ не является постоянной: подвид деятельности по оценке утверждений о соответствии ПЗ выполняют только тогда, когда имеет место утверждение о соответствии ПЗ, а подвид деятельности по оценке сформулированных в явном виде требований безопасности ИТ выполняют только тогда, когда в изложение требований безопасности ИТ включены требования безопасности, взятые не из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3.

Некоторая информация, подлежащая включению в ЗБ, может быть представлена соответствующей ссылкой. Например, если в ЗБ утверждают о соответствии некоторому ПЗ, то такую информацию из ПЗ, как описание среды и угроз, можно рассматривать как часть ЗБ и предполагать, что она соответствует критериям для ЗБ.

Если в ЗБ утверждают 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 возможно при оценке изложения среды безопасности, целей безопасности и требований безопасности ИТ. В ЗБ допускается утверждение о соответствии нескольким ПЗ.

9.3 Вид деятельности «Оценка задания по безопасности»

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

9.3.1.1 Цели

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

9.3.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.1.3 Замечания по применению

Между ОО и продуктом, который может приобрести потребитель, могут существовать некоторые отличия. Материалы по данному вопросу представлены в А.6 «Границы ОО» (приложение А).

9.3.1.4 Действие ASE_DES.1.1E

9.3.1.4.1 Шаг оценивания ASE_DES.1-1

ИСО/МЭК 15408-3 ASE_DES.1.1C: *Описание ОО должно включать в себя тип продукта или системы, область применения ОО, а также физические и логические границы ОО.*

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

Оценщик делает заключение, достаточно ли «Описание ОО» для общего понимания предполагаемого использования продукта или системы и обеспечивает ли, таким образом, контекст оценки. Примерами некоторых типов продуктов и систем являются: межсетевой экран, смарт-карта, криптомодем, веб-сервер, интрасеть.

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 рассмотрено в разделе «Описание ОО». Примером этого является ОО типа «межсетевой экран», в «Описании ОО» которого изложено, что он не может быть подключен к сетям.

9.3.1.4.2 Шаг оценивания 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.

Оценщик делает заключение, рассмотрены 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 этих компонентов и/или модулей.

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

9.3.1.4.3 Шаг оценивания 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.

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 этих характеристик.

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

9.3.1.5 Действие ASE_DES.1.2E

9.3.1.5.1 Шаг оценивания ASE_DES.1-4

Оценщик должен исследовать ЗБ, чтобы сделать заключение, является ли «Описание ОО» логически упорядоченным.

Изложение раздела «Описание ОО» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

9.3.1.5.2 Шаг оценивания ASE_DES.1-5

Оценщик должен исследовать ЗБ, чтобы сделать заключение, является ли «Описание ОО» внутренне непротиворечивым.

Оценщику необходимо иметь в виду, что данный раздел ЗБ предназначен только для того, чтобы определить общее назначение ОО.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

9.3.1.6 Действие ASE_DES.1.3E

9.3.1.6.1 Шаг оценивания ASE_DES.1-6

Оценщик должен исследовать ЗБ, чтобы сделать заключение, согласовано ли «Описание ОО» с другими частям ЗБ.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

9.3.2.1 Цели

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

9.3.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.2.3 Действие ASE_ENV.1.1E

9.3.2.3.1 Шаг оценивания ASE_ENV.1-1

ИСО/МЭК 15408-3 ASE_ENV.1.1C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждое предположение о предполагаемом применении ОО и среде использования ОО.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо предположения.

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

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

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

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

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

- предполагают, что консоли администраторов находятся в некоторой зоне, доступ в которую ограничен только персоналом, являющимся администраторами;

- предполагают, что хранение всех файлов для ОО осуществляется на той рабочей станции, на которой функционирует ОО.

b) Аспекты, имеющие отношение к персоналу, включают в себя 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:

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

c) Аспекты внешних связей включают в себя 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:

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

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 четкими и понятными, то это может, в конечном счете, привести к тому, что ОО будет использован в среде, в которой он не будет функционировать безопасным образом.

9.3.2.3.2 Шаг оценивания ASE_ENV.1-2

ИСО/МЭК 15408-3 ASE_ENV.1.2C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждую известную или предполагаемую угрозу активам, от которой будет требоваться защита посредством ОО или его среды.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо угрозы.

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 таком случае данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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.

9.3.2.3.3 Шаг оценивания ASE_ENV.1-3

ИСО/МЭК 15408-3 ASE_ENV.1.3C: *Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.*

Оценщик должен исследовать изложение раздела «Среда безопасности ОО», чтобы сделать заключение, идентифицированы и разъяснены ли в нем какие-либо политики безопасности организации.

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 таком случае данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Оценщик делает заключение, изложена ли политика безопасности организации в виде правил, практических приемов или руководств, установленных организацией, контролирующей среду использования ОО, которым должен следовать ОО или его среда. Примером политики безопасности организации является требование генерации и шифрования паролей в соответствии с национальным стандартом.

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

9.3.2.4 Действие ASE_ENV.1.2E

9.3.2.4.1 Шаг оценивания ASE_ENV.1-4

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

Изложение раздела «Среда безопасности ОО» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

9.3.2.4.2 Шаг оценивания ASE_ENV.1-5

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

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

- изложение раздела «Среда безопасности ОО», которое содержит угрозу, метод нападения для которой не может быть реализован источником угрозы;
- изложение раздела «Среда безопасности ОО», которое содержит правило политики безопасности организации «ОО не должен быть подключен к Интернету» и угрозу, источником которой является злоумышленник из Интернета.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

9.3.3.1 Цели

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

9.3.3.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.3.3 Действие ASE_INT.1.1E

9.3.3.3.1 Шаг оценивания ASE_INT.1-1

ИСО/МЭК 15408-3 ASE_INT.1.1C: *Введение ЗБ должно содержать данные идентификации ЗБ, которые предоставляют маркировку и описательную информацию, необходимые для идентификации и применения ЗБ и ОО, к которому оно относится.*

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

Оценщик делает заключение, включает ли в себя идентификационная информация ЗБ:

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

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

c) указание версии ИСО/МЭК 15408, использованной при разработке ЗБ;

d) дополнительную информацию в соответствии с требованиями системы оценки.

9.3.3.3.2 Шаг оценивания ASE_INT.1-2

ИСО/МЭК 15408-3 ASE_INT.1.2C: *Введение ЗБ должно содержать аннотацию ЗБ с общей характеристикой ЗБ в описательной форме.*

Оценщик должен проверить, представлена ли в разделе «Введение ЗБ» «Аннотация ЗБ» в повествовательной форме.

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

9.3.3.3.3 Шаг оценивания ASE_INT.1-3

ИСО/МЭК 15408-3 ASE_INT.1.3C: Введение ЗБ должно содержать утверждение о соответствии ИСО/МЭК 15408, излагающее все оцениваемые утверждения о соответствии ОО ИСО/МЭК 15408.

Оценщик должен проверить, содержит ли «Введение ЗБ» подраздел «Утверждение о соответствии ИСО/МЭК 15408», в котором изложено утверждение о соответствии ОО ИСО/МЭК 15408.

Оценщик делает заключение, соответствует ли «Утверждение о соответствии ИСО/МЭК 15408» подразделу 6.4 ИСО/МЭК 15408-1.

Оценщик делает заключение, что «Утверждение о соответствии ИСО/МЭК 15408» содержит утверждение о соответствии либо ИСО/МЭК 15408-2, либо ИСО/МЭК 15408-2, расширенному другими компонентами функциональных требований.

Оценщик делает заключение, что «Утверждение о соответствии ИСО/МЭК 15408» содержит утверждение о соответствии либо ИСО/МЭК 15408-3, либо ИСО/МЭК 15408-3, расширенному другими компонентами требований доверия.

Если утверждается о расширении ИСО/МЭК 15408-3 и пакет требований доверия включает в себя требования доверия из ИСО/МЭК 15408-3, оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ИСО/МЭК 15408», какие требования доверия из ИСО/МЭК 15408-3 заявлены.

Если утверждается о соответствии именованному пакету, оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ИСО/МЭК 15408», какой пакет заявлен.

Если утверждается об усилении именованного пакета, оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ИСО/МЭК 15408», какой пакет заявлен и какое усиление к этому пакету заявлено.

Если утверждается о соответствии ПЗ, то оценщик делает заключение, сформулировано ли в подразделе «Утверждение о соответствии ИСО/МЭК 15408», по отношению к какому профилю защиты или профилям защиты сделано утверждение о соответствии.

Оценщику необходимо иметь в виду, что если утверждается о соответствии ПЗ, то применяются критерии оценки утверждений о соответствии ПЗ (ASE_PPC.1), а если утверждается о расширении ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, то применяются критерии оценки требований безопасности, сформулированных в явном виде (ASE_SRE.1).

9.3.3.4 Действие ASE_INT.1.2E

9.3.3.4.1 Шаг оценивания ASE_INT.1-4

Оценщик должен исследовать «Введение ЗБ», чтобы сделать заключение, является ли оно логически упорядоченным.

«Введение ЗБ» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

9.3.3.4.2 Шаг оценивания ASE_INT.1-5

Оценщик должен исследовать «Введение ЗБ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

9.3.3.5 Действие ASE_INT.1.3E

9.3.3.5.1 Шаг оценивания ASE_INT.1-6

Оценщик должен исследовать ЗБ, чтобы сделать заключение, согласовано ли «Введение ЗБ» с другими частями ЗБ.

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 предполагается ли в нем наличие характеристик безопасности, которые выходят за рамки оценки.

Оценщик также делает заключение, согласовано ли «Утверждение о соответствии ИСО/МЭК 15408» с другими частями ЗБ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

9.3.4 Оценка целей безопасности (ASE_OBJ.1)

9.3.4.1 Цели

Цель данного подвида деятельности — сделать заключение, полностью ли и согласованно описаны цели безопасности, направлены ли цели безопасности на противостояние идентифицированным угрозам, на достижение идентифицированной политики безопасности организации и согласованы ли они с приведенными предположениями.

9.3.4.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.4.3 Действие ASE_OBJ.1.1E

9.3.4.3.1 Шаг оценивания ASE_OBJ.1-1

ИСО/МЭК 15408-3 ASE_OBJ.1.1C: *Изложение целей безопасности должно определить цели безопасности для ОО и его среды.*

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

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

9.3.4.3.2 Шаг оценивания ASE_OBJ.1-2

ИСО/МЭК 15408-3 ASE_OBJ.1.2C: *Цели безопасности для ОО должны быть сопоставлены с теми аспектами идентифицированных угроз, которым будет противостоять ОО, и/или с политикой безопасности организации, которая будет выполняться ОО.*

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

Оценщик делает заключение, прослежена ли каждая цель безопасности для ОО, по крайней мере, к одной угрозе или политике безопасности организации.

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.

9.3.4.3.3 Шаг оценивания ASE_OBJ.1-3

ИСО/МЭК 15408-3 ASE_OBJ.1.3C: *Цели безопасности для среды должны быть сопоставлены с теми аспектами идентифицированных угроз, которым ОО противостоит не полностью, и/или с политикой безопасности организации или предположениями, не полностью выполняемыми ОО.*

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.

Оценщик делает заключение, прослежена ли каждая цель безопасности для среды, по крайней мере, к одному предположению, угрозе или политике безопасности организации.

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.

Поэтому угрозе полностью может соответствовать одна или более цель для среды. Крайний случай — это когда отсутствуют цели безопасности для ОО. В этом случае использование конструкции ПЗ/ЗБ остается правомерным, определение ОО, для которого все угрозы и политики безопасности организации учитываются средой, вряд ли бы имело какой-то практический смысл, так как для такого ОО не было бы никаких функциональных требований безопасности. Решение о сертификации подобных ОО является прерогативой системы оценки.

9.3.4.3.4 Шаг оценивания ASE_OBJ.1-4

ИСО/МЭК 15408-3 ASE_OBJ.1.4C: *Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.*

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

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

Оценщик делает заключение, демонстрирует ли логическое 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.

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.

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).

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.

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.

Несмотря на то, что прослеживание целей безопасности к угрозам в обосновании целей безопасности может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является только заявлением, отражающим намерение предотвратить реализацию конкретной угрозы, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

9.3.4.3.5 Шаг оценивания ASE_OBJ.1-5

ИСО/МЭК 15408-3 ASE_OBJ.1.5C: *Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.*

Оценщик должен исследовать «Обоснование целей безопасности», чтобы сделать заключение, содержится ли в нем для каждого аспекта политики безопасности организации приемлемое логическое обоснование того, что цели безопасности покрывают данный аспект политики безопасности организации.

Если ни одна цель безопасности не прослежена к политике безопасности организации, то результат данного шага оценивания отрицательный.

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

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

Несмотря на то, что прослеживание целей безопасности к политике безопасности организации в обосновании целей безопасности может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности является только заявлением, отражающим намерение реализовать конкретную политику безопасности, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

9.3.4.3.6 Шаг оценивания ASE_OBJ.1-6

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

Если ни одна цель безопасности для среды не прослежена к приведенному предположению, то результат данного шага оценивания отрицательный.

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

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

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.

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

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.

Несмотря на то, что прослеживание целей безопасности для среды к предположениям относительно среды использования ОО в подразделе «Обоснование целей безопасности» может быть частью логического обоснования, само по себе оно не является логическим обоснованием. Даже в том случае, когда цель безопасности представляет собой перефразированное предположение, все равно требуется логическое обоснование, хотя в данном случае оно может быть минимальным.

9.3.4.4 Действие ASE_OBJ.1.2E

9.3.4.4.1 Шаг оценивания ASE_OBJ.1-7

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно логически упорядоченным.

Изложение раздела «Цели безопасности» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

9.3.4.4.2 Шаг оценивания ASE_OBJ.1-8

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно полным.

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 быть выполнен совместно с шагами оценивания ASE_OBJ.1-4, ASE_OBJ.1-5 и ASE_OBJ.1-6.

9.3.4.4.3 Шаг оценивания ASE_OBJ.1-9

Оценщик должен исследовать изложение раздела «Цели безопасности», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

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».

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

9.3.5.1 Цели

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

9.3.5.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

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

9.3.5.3 Замечания по применению

Данный пункт применим, только если в ЗБ утверждают о соответствии одному или нескольким ПЗ. Если в ЗБ не утверждают о соответствии одному или нескольким ПЗ, то все шаги оценивания из этого пункта не применяют и поэтому считают удовлетворенными.

9.3.5.4 Действие ASE_PPC.1.1E

9.3.5.4.1 Шаг оценивания ASE_PPC.1-1

ИСО/МЭК 15408-3 ASE_PPC.1.1C: *Каждое утверждение о соответствии ПЗ должно идентифицировать ПЗ, соответствие которому утверждается, включая необходимые уточнения, связанные с этим утверждением.*

Оценщик должен проверить, что в каждом утверждении о соответствии ПЗ в ЗБ идентифицирован ПЗ, о соответствии которому сделано утверждение.

Оценщик делает заключение, идентифицирован ли однозначно каждый ПЗ, о соответствии которому в ЗБ сделано утверждение (например, путем указания наименования и номера версии или использования идентификационной информации, включенной в раздел «Введение» данного ПЗ). Оценщику необходимо иметь в виду, что утверждения о частичном соответствии ПЗ не допускаются ИСО/МЭК 15408.

9.3.5.4.2 Шаг оценивания ASE_PPC.1-2

ИСО/МЭК 15408-3 ASE_PPC.1.2C: *Каждое утверждение о соответствии ПЗ должно идентифицировать формулировки требований безопасности ИТ, в которых завершены разрешенные операции или иначе выполнено дальнейшее уточнение требований ПЗ.*

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.

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.

9.3.5.4.3 Шаг оценивания ASE_PPC.1-3

ИСО/МЭК 15408-3 ASE_PPC.1.3C: *Каждое утверждение о соответствии ПЗ должно идентифицировать формулировки содержащихся в ЗБ целей безопасности и требований безопасности ИТ, которые дополняют имеющиеся в ПЗ.*

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.

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

9.3.5.5 Действие ASE_PPC.1.2E

9.3.5.5.1 Шаг оценивания 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.

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.

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

9.3.6.1 Цели

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.

9.3.6.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.6.3 Действие ASE_REQ.1.1E

9.3.6.3.1 Шаг оценивания ASE_REQ.1-1

ИСО/МЭК 15408-3 ASE_REQ.1.1C: *Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований из ИСО/МЭК 15408-2.*

Оценщик должен проверить изложение функциональных требований безопасности ОО, чтобы сделать заключение, идентифицированы ли в нем функциональные требования безопасности ОО, составленные из компонентов функциональных требований по ИСО/МЭК 15408-2.

Оценщик делает заключение, что все компоненты функциональных требований безопасности ОО, взятые из ИСО/МЭК 15408-2, идентифицированы либо путем ссылки на отдельные компоненты по ИСО/МЭК 15408-2, либо путем ссылки на отдельные компоненты из ПЗ, о соответствии которому утверждают в ЗБ, либо путем воспроизведения их в ЗБ.

9.3.6.3.2 Шаг оценивания ASE_REQ.1-2

Оценщик должен проверить, что каждая ссылка на компонент функциональных требований безопасности ОО является правильной.

Для каждой ссылки на компонент функционального требования безопасности ОО по ИСО/МЭК 15408-2 оценщик делает заключение, существует ли упомянутый компонент в ИСО/МЭК 15408-2.

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

9.3.6.3.3 Шаг оценивания ASE_REQ.1-3

Оценщик должен проверить, что каждый компонент функциональных требований безопасности ОО, взятый из ИСО/МЭК 15408-2 и воспроизведенный в ЗБ, воспроизведен правильно.

Оценщик делает заключение, правильно ли воспроизведены требования в подразделе «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.

9.3.6.3.4 Шаг оценивания ASE_REQ.1-4

ИСО/МЭК 15408-3 ASE_REQ.1.2C: *Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия ИСО/МЭК 15408-3.*

Оценщик должен проверить изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, идентифицированы ли в нем требования доверия к безопасности ОО, составленные из компонентов требований доверия ИСО/МЭК 15408-3.

Оценщик делает заключение, все ли компоненты требований доверия к безопасности ОО, взятые из ИСО/МЭК 15408-3, идентифицированы либо путем ссылки на некоторый ОУД, либо на отдельные компоненты из ИСО/МЭК 15408-3, либо путем ссылки на ПЗ, соответствие которому заявлено в ЗБ, либо путем их воспроизведения в ЗБ.

9.3.6.3.5 Шаг оценивания ASE_REQ.1-5

Оценщик должен проверить, что каждая ссылка на компоненты требований доверия к безопасности ОО является правильной.

Для каждой ссылки на компонент требований доверия к безопасности ОО по ИСО/МЭК 15408-3 оценщик делает заключение, существует ли упомянутый компонент в ИСО/МЭК 15408-3.

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

9.3.6.3.6 Шаг оценивания ASE_REQ.1-6

Оценщик должен проверить, что каждый компонент требований доверия к безопасности ОО, взятый из ИСО/МЭК 15408-3 и воспроизведенный в ЗБ, воспроизведен правильно.

Оценщик делает заключение, правильно ли воспроизведены требования в подразделе «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.

9.3.6.3.7 Шаг оценивания ASE_REQ.1-7

ИСО/МЭК 15408-3 ASE_REQ.1.3C: *В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в ИСО/МЭК 15408-3.*

Оценщик должен исследовать изложение подраздела «Требования доверия к безопасности ОО», чтобы сделать заключение, содержит ли оно ОУД, определенный в ИСО/МЭК 15408-3, либо в нем логически обосновано отсутствие ОУД.

Если никакой из ОУД не включен, то оценщик делает заключение, указана ли в логическом обосновании причина невключения ОУД в подраздел «Требования доверия к безопасности ОО». Это логическое обоснование может указывать либо на причину невозможности, нежелательности или нецелесообразности включения ОУД, либо на причину невозможности, нежелательности или нецелесообразности включения конкретных компонентов семейств, составляющих ОУД1 (ACM_CAP «Возможности УК», ADO_IGS «Установка, генерация и запуск», ADV_FSP «Функциональная спецификация», ADV_RCR «Соответствие представлений», AGD_ADM «Руководство администратора», AGD_USR «Руководство пользователя» и ATE_IND «Независимое тестирование»).

9.3.6.3.8 Шаг оценивания ASE_REQ.1-8

ИСО/МЭК 15408-3 ASE_REQ.1.4C: *Свидетельство должно содержать логическое обоснование, что изложение требований доверия к ОО является соответствующим.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, достаточно ли логично в нем обосновано то, что изложение требований доверия к безопасности ОО является приемлемым.

Если требования доверия содержат какой-либо ОУД, то в логическом 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 логическое обоснование каждого такого усиления. Если подраздел «Требования доверия к безопасности ОО» содержит требования доверия, сформулированные в явном виде, оценщик делает заключение, приведено ли логическое обоснование использования каждого сформулированного в явном виде требования доверия.

Оценщик делает заключение, дано ли в подразделе «Обоснование требований безопасности» достаточно логичное 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 «Анализ уязвимостей разработчиком», который является несвойственным для обнаружения недостатков безопасности, не являющихся очевидными.

Логическое обоснование может также включать в себя основания, подобные следующим:

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

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

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

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

e) требования потребителей.

Краткий обзор назначения и целей для каждого ОУД приведен в ИСО/МЭК 15408-3 (подраздел 10.2).

Оценщику необходимо иметь в виду, что заключение о том, являются ли требования доверия приемлемыми, может быть субъективным, а значит, анализ достаточности логического обоснования не следует проводить слишком строго.

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.

9.3.6.3.9 Шаг оценивания ASE_REQ.1-9

ИСО/МЭК 15408-3 ASE_REQ.1.5C: *ЗБ должно, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.*

Оценщик должен проверить, что в ЗБ, при необходимости, идентифицированы требования безопасности для среды ИТ.

Если ЗБ не содержит требований безопасности для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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 «Аудит безопасности» и FIA «Идентификация и аутентификация».

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

Пример зависимости от среды ИТ — программный криптомодуль, который периодически проверяет свой код и, в случае обнаружения несанкционированной модификации, самоотключается. Для обеспечения возможности восстановления предусмотрено требование FPT_RCV.2 «Автоматическое восстановление». Поскольку криптомодуль не может самостоятельно восстановить свой код после самоотключения, то требование по восстановлению становится требованием к среде ИТ. Одной из зависимостей компонента FPT_RCV.2 «Автоматическое восстановление» является компонент AGD_ADM.1 «Руководство администратора». Следовательно, это требование доверия становится требованием доверия для среды ИТ.

Оценщику необходимо иметь в виду, что ссылка требований безопасности для среды ИТ на ФБО относится к функциям безопасности среды, а не к функциям безопасности ОО.

9.3.6.3.10 Шаг оценивания ASE_REQ.1-10

ИСО/МЭК 15408-3 ASE_REQ.1.6C: *Операции, предусмотренные в требованиях безопасности ИТ, включенных в ЗБ, должны быть идентифицированы и выполнены.*

Оценщик должен проверить, что все операции над требованиями безопасности ИТ идентифицированы.

Разрешенными операциями для компонентов по ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 являются «назначение», «итерация», «выбор» и «уточнение». Операции «назначение» и «выбор» разрешены только в специально обозначенных местах компонента. Операции «итерация» и «уточнение» разрешены для всех компонентов.

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.

9.3.6.3.11 Шаг оценивания ASE_REQ.1-11

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, все ли операции «назначение» и «выбор» выполнены.

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

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 логическое обоснование для этого случая заключается в том, что конкретное значение будет выбрано из диапазона допустимых значений администратором в процессе инсталляции ОО.

9.3.6.3.12 Шаг оценивания ASE_REQ.1-12

Оценщик должен исследовать ЗБ, чтобы сделать заключение, все ли операции выполнены корректно.

Оценщик сравнивает каждую формулировку с элементом, из которого она получена, чтобы сделать заключение:

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

b) 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 необходим 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);

c) для операции «уточнение» — уточнен ли компонент таким образом, что ОО, удовлетворяющий уточненному требованию, также удовлетворяет и неуточненному требованию. Если уточненное требование выходит за эти рамки, то его считают расширенным требованием.

Пример: ADV_SPM.1.2C — Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, 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, что моделировать следует только управление доступом, то это уточнение не является правомерным.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, а именно переформулирование предложения в соответствии с правилами 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 необходимо иметь в виду, что редакционные уточнения должны быть четко идентифицированы (см. шаг оценивания ASE_REQ.1-10);

d) 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.

9.3.6.3.13 Шаг оценивания ASE_REQ.1-13

ИСО/МЭК 15408-3 ASE_REQ.1.7C: *Зависимости между требованиями безопасности ИТ, включенными в ЗБ, следует удовлетворить.*

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, удовлетворены ли зависимости, требуемые компонентами, используемыми при изложении раздела «Требования безопасности ИТ».

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

Хотя ИСО/МЭК 15408 поддерживает проведение анализа зависимостей путем их включения в описание компонентов требований, сам по себе данный факт не является логическим обоснованием того, что никакие другие зависимости не существуют. 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 перечислены данные объекты или субъекты.

Зависимости требований безопасности для среды ИТ следует излагать и удовлетворять в ЗБ.

Оценщику необходимо иметь в виду, что в ИСО/МЭК 15408 не требуется, чтобы все зависимости были удовлетворены: см. следующий шаг оценивания.

9.3.6.3.14 Шаг оценивания ASE_REQ.1-14

ИСО/МЭК 15408-3 ASE_REQ.1.8C: *Свидетельство должно содержать логическое обоснование каждого неудовлетворения зависимостей.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое логическое обоснование для каждого случая, когда зависимости требований безопасности не удовлетворены.

Оценщик с учетом идентифицированных целей безопасности делает заключение, объяснено ли в логическом обосновании, почему удовлетворение зависимости не требуется.

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

Пример приемлемого логического 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 логическое 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 не способны 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».

9.3.6.3.15 Шаг оценивания ASE_REQ.1-15

ИСО/МЭК 15408-3 ASE_REQ.1.9C: *ЗБ должно включать в себя изложение приемлемого минимального уровня стойкости функций безопасности (СФБ) для функциональных требований безопасности ОО: базовой, средней или высокой СФБ.*

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.

Если требования доверия к безопасности ОО не включают в себя компонент AVA_SOF.1 «Оценка стойкости функции безопасности ОО», то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Стойкость криптографических алгоритмов находится вне области действия ИСО/МЭК 15408. Стойкость функции безопасности применяют 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 ИСО/МЭК 15408. Когда такие криптографические механизмы входят в состав ОО, то оценщик делает заключение, представлено ли в ЗБ четкое изложение того, что оценка стойкости криптографических алгоритмов не является частью оценки.

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.

Примером этого является распределенная терминальная система, включающая в себя 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 безо-

пасности 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.

9.3.6.3.16 Шаг оценивания ASE_REQ.1-16

ИСО/МЭК 15408-3 ASE_REQ.1.10C: *При изложении требований безопасности должны быть идентифицированы все функциональные требования безопасности, для которых требуется явное заявление стойкости функции, с явным заявлением стойкости функции для каждого такого функционального требования безопасности.*

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.

Если подраздел «Требования доверия к безопасности ОО» не содержит компонент AVA_SOF.1 «Оценка стойкости функции безопасности ОО», то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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. Данный шаг оценивания относится к тому случаю, когда автору ЗБ требуется определить конкретные утверждения о СФБ (т.е. выше, чем общее утверждение о СФБ, заявленное в ЗБ) или — конкретную метрику СФБ. Конкретные утверждения о СФБ для функциональных требований безопасности ОО могут быть определены автором ПЗ. При отсутствии каких-либо конкретных утверждений о СФБ общее утверждение о СФБ в ЗБ применяют ко всем функциональным требованиям безопасности ОО, изложенным в ЗБ. Оценщику следует удостовериться, что наличие или отсутствие утверждений о СФБ, сформулированных в явном виде, согласовано с другими частями данного ЗБ.

Потенциально в ЗБ утверждения о СФБ могут варьироваться. В ЗБ может иметься общее утверждение о СФБ, кроме того, в рамках ЗБ для конкретных функциональных требований безопасности ОО могут иметься утверждения о СФБ, определенные специально для этих функциональных требований.

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

9.3.6.3.17 Шаг оценивания ASE_REQ.1-17

ИСО/МЭК 15408-3 ASE_REQ.1.11C: *Обоснование требований безопасности должно демонстрировать, что минимальный уровень стойкости функции в ЗБ, как и каждое явное указание стойкости функции согласуются с целями безопасности ОО.*

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.

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

Оценщик делает заключение, учтены ли в подразделе «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.

Оценщик также делает заключение, учтены ли в подразделе «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 в себя соответствующее утверждение о стойкости связанных с этими требованиями функций безопасности.

9.3.6.3.18 Шаг оценивания ASE_REQ.1-18

ИСО/МЭК 15408-3 ASE_REQ.1.12C: *Обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.*

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

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

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

Допустимо также, но необязательно, прослеживание отдельных или всех требований доверия к безопасности ОО к целям безопасности для ОО.

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 «Номера версий», и поэтому разработчик ЗБ прослеживает данный компонент к рассматриваемой цели безопасности для ОО.

9.3.6.3.19 Шаг оценивания ASE_REQ.1-19

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, прослежены ли требования безопасности для среды ИТ к целям безопасности для среды.

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

Неудача при попытке 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.

Допустимо также, но необязательно, для некоторых или всех требований доверия к безопасности для среды ИТ прослеживание к целям безопасности для среды.

9.3.6.3.20 Шаг оценивания ASE_REQ.1-20

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

Если никакие требования безопасности ОО не прослежены к конкретной цели безопасности для ОО, то результат данного шага оценивания отрицательный.

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

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

Несмотря на то, что прослеживание от требований безопасности ОО к целям безопасности для ОО, представленное в подразделе «Обоснование требований безопасности», может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

9.3.6.3.21 Шаг оценивания ASE_REQ.1-21

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, содержит ли он для каждой цели безопасности для среды ИТ приемлемое логическое обоснование, что требования безопасности для среды ИТ пригодны для удовлетворения данной цели безопасности для среды ИТ.

Если никакие требования безопасности для среды ИТ не прослежены к конкретной цели безопасности для среды ИТ, то результат данного шага оценивания отрицательный.

Оценщик делает заключение, демонстрирует ли логическое 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.

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.

Несмотря на то, что прослеживание требований безопасности для среды ИТ к целям безопасности для среды ИТ, представленное в подразделе «Обоснование требований безопасности», может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

9.3.6.3.22 Шаг оценивания ASE_REQ.1-22

ИСО/МЭК 15408-3 ASE_REQ.1.13C: *Обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.*

Оценщик должен исследовать подраздел «Обоснование требований безопасности», чтобы сделать заключение, демонстрирует ли он внутреннюю непротиворечивость совокупности требований безопасности ИТ.

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, приведено приемлемое логическое обоснование отсутствия таких противоречий.

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. Сюда может входить 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.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

9.3.6.3.23 Шаг оценивания ASE_REQ.1-23

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

Данный шаг оценивания основан 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.

Данный шаг оценивания основан также на анализе зависимостей, выполняемом на предыдущих шагах оценивания, поскольку если функциональное требование А имеет зависимость от функционального требования В, то В поддерживает А по определению.

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

a) на предотвращение обхода механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_RVM.1 «Невозможность обхода ПБО»;

b) на предотвращение вмешательства в работу механизмов, реализующих другие функциональные требования безопасности, такие, например, как FPT_SEP «Разделение домена»;

c) на предотвращение деактивации механизмов, реализующих другие функциональные требования безопасности, такие, например, как FMT_MOF.1 «Управление режимом выполнения функций безопасности»;

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

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

9.3.6.4 Действие ASE_REQ.1.2E

9.3.6.4.1 Шаг оценивания ASE_REQ.1-24

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно логически упорядоченным.

Изложение требований безопасности ИТ является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и потребителям).

9.3.6.4.2 Шаг оценивания ASE_REQ.1-25

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно полным.

При выполнении данного шага оценивания используют 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».

Изложение раздела «Требования безопасности ИТ» является полным, если все операции над требованиями завершены и оценщик считает требования безопасности достаточными для того, чтобы удостовериться, что все цели безопасности для ОО удовлетворены.

9.3.6.4.3 Шаг оценивания ASE_REQ.1-26

Оценщик должен исследовать изложение раздела «Требования безопасности ИТ», чтобы сделать заключение, является ли оно внутренне непротиворечивым.

При выполнении данного шага оценивания используют 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».

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.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

9.3.7.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли функциональные требования и/или требования доверия к безопасности, сформулированные без ссылки на ИСО/МЭК 15408, приемлемыми и адекватными.

9.3.7.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.7.3 Замечания по применению

Этот пункт применяют только в случае, если в ЗБ содержатся требования безопасности, сформулированные в явном виде без ссылки на ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. В противном случае все шаги оценивания, описанные в данном пункте, не применяют и поэтому считают удовлетворенными.

Требования семейства ASE_SRE «Требования безопасности ИТ, сформулированные в явном виде» не заменяют требования семейства ASE_REQ «Требования безопасности ИТ», а являются дополнительными к ним. Это означает, что требования безопасности, сформулированные в явном виде без ссылки на ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, должны быть оценены на соответствие критериям семейства ASE_SRE, а также в сочетании со всеми остальными требованиями безопасности — на соответствие критериям семейства ASE_REQ.

9.3.7.4 Действие ASE_SRE.1.1E

9.3.7.4.1 Шаг оценивания ASE_SRE.1-1

ИСО/МЭК 15408-3 ASE_SRE.1.1C: *Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.*

Оценщик должен проверить, что в изложении раздела «Требования безопасности ИТ» идентифицированы все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408.

Необходимо, чтобы все функциональные требования безопасности ОО, которые не специфицированы на основе функциональных компонентов из ИСО/МЭК 15408-2, были четко идентифицированы как таковые. Аналогично необходимо, чтобы все требования доверия к безопасности ОО, которые не специфицированы на основе компонентов доверия из ИСО/МЭК 15408-3, были четко идентифицированы как таковые.

9.3.7.4.2 Шаг оценивания ASE_SRE.1-2

ИСО/МЭК 15408-3 ASE_SRE.1.2C: *Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.*

Оценщик должен проверить, что в изложении раздела «Требования безопасности ИТ» идентифицированы все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408.

Требуется, чтобы все функциональные требования безопасности для среды ИТ, которые не специфицированы на основе функциональных компонентов из ИСО/МЭК 15408-2, были четко идентифицированы как таковые. Аналогично также требуется, чтобы все требования доверия к среде ИТ, которые не специфицированы на основе компонентов доверия из ИСО/МЭК 15408-3, были четко идентифицированы как таковые.

9.3.7.4.3 Шаг оценивания ASE_SRE.1-3

ИСО/МЭК 15408-3 ASE_SRE.1.3C: *Свидетельство должно содержать логическое обоснование, почему требования безопасности должны быть сформулированы в явном виде.*

Оценщик должен исследовать «Обоснование требований безопасности», чтобы сделать заключение, содержится ли в нем приемлемое логическое обоснование, почему каждое из сформулированных в явном виде требований безопасности пришлось сформулировать в явном виде.

Оценщик для каждого сформулированного в явном виде требования безопасности ИТ делает заключение, объяснено ли в логическом обосновании, почему существующие функциональные компоненты или компоненты доверия (из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 соответственно) не могли быть использованы для выражения требований безопасности, сформулированных в явном виде. При вынесении заключения оценщик принимает во внимание возможность выполнения операций (т.е. назначение, итерация, выбор и уточнение) над этими существующими компонентами.

9.3.7.4.4 Шаг оценивания ASE_SRE.1-4

ИСО/МЭК 15408-3 ASE_SRE.1.4C: *Сформулированные в явном виде требования безопасности ИТ должны использовать компоненты, семейства и классы требований ИСО/МЭК 15408 как образец для представления.*

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 ИСО/МЭК 15408.

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 ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. Оценщик также делает заключение, разделены ли функциональные требования на отдельные функциональные элементы и определяют ли требования доверия элементы действий разработчика, содержания и представления свидетельств, а также действий оценщика.

9.3.7.4.5 Шаг оценивания ASE_SRE.1-5

ИСО/МЭК 15408-3 ASE_SRE.1.5C: *Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать объективные требования оценки, такие, чтобы соответствие или несоответствие им ОО могло быть определено и последовательно продемонстрировано.*

Оценщик должен исследовать каждое сформулированное в явном виде требование безопасности ИТ, чтобы сделать заключение, измеримо ли оно и устанавливает ли объективные требования оценки такие, что соответствие или несоответствие им ОО может быть определено и продемонстрировано систематическим методом.

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 необходимости вынесения о них субъективного суждения со стороны оценщика.

Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны быть использованы как образец.

9.3.7.4.6 Шаг оценивания ASE_SRE.1-6

ИСО/МЭК 15408-3 ASE_SRE.1.6C: *Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.*

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

Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны быть использованы как образец.

9.3.7.4.7 Шаг оценивания ASE_SRE.1-7

ИСО/МЭК 15408-3 ASE_SRE.1.7C: *Обоснование требований безопасности должно демонстрировать, что требования доверия применимы и пригодны для поддержки каждого из сформулированных в явном виде функциональных требований безопасности ОО.*

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.

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).

9.3.7.5 Действие ASE_SRE.1.2E

9.3.7.5.1 Шаг оценивания ASE_SRE.1-8

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

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

Примеры возможных зависимостей: компоненты класса FAU «Аудит безопасности», если в сформулированном в явном виде функциональном требовании упоминается аудит; компоненты семейства ADV_IMP «Представление реализации», если в сформулированном в явном виде требовании доверия упоминается исходный код или представление реализации ОО.

9.3.8 Оценка раздела «Краткая спецификация ОО» (ASE_TSS.1)

9.3.8.1 Цели

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

9.3.8.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является ЗБ.

9.3.8.3 Действие ASE_TSS.1.1E

9.3.8.3.1 Шаг оценивания ASE_TSS.1-1

ИСО/МЭК 15408-3 ASE_TSS.1.1C: *Краткая спецификация ОО должна содержать описание функций безопасности ИТ и мер доверия к ОО.*

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

Оценщик делает заключение, представлено ли в разделе «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.

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).

9.3.8.3.2 Шаг оценивания ASE_TSS.1-2

ИСО/МЭК 15408-3 ASE_TSS.1.2C: *Краткая спецификация ОО должна сопоставить функции безопасности ИТ и функциональные требования безопасности ОО таким образом, чтобы можно было отметить, какие функции безопасности ИТ каким функциональным требованиям безопасности ОО удовлетворяют, и что каждая функция безопасности ИТ способствует удовлетворению, по меньшей мере, одного функционального требования безопасности ОО.*

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

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

9.3.8.3.3 Шаг оценивания ASE_TSS.1-3

ИСО/МЭК 15408-3 ASE_TSS.1.3C: *Функции безопасности ИТ должны быть определены в неформальном стиле на уровне детализации, необходимом для понимания их назначения.*

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

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».

Необходимо отметить, 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.

9.3.8.3.4 Шаг оценивания ASE_TSS.1-4

ИСО/МЭК 15408-3 ASE_TSS.1.4C: *Все ссылки на механизмы безопасности, включенные в ЗБ, должны быть сопоставлены с соответствующими функциями безопасности так, чтобы можно было отметить, какие механизмы безопасности использованы при реализации каждой функции.*

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

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 применяют и поэтому считают удовлетворенным.

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

Неудача при попытке такого прослеживания означает, что либо краткая спецификация ОО является неполной, либо механизм безопасности является бесполезным.

9.3.8.3.5 Шаг оценивания ASE_TSS.1-5

ИСО/МЭК 15408-3 ASE_TSS.1.5C: *Обоснование краткой спецификации ОО должно демонстрировать, что функции безопасности ИТ пригодны для удовлетворения функциональных требований безопасности ОО.*

Оценщик должен исследовать подраздел «Обоснование краткой спецификации ОО», чтобы сделать заключение, содержится ли в нем для каждого функционального требования безопасности ОО приемлемое логическое обоснование того, что функции безопасности ИТ пригодны для удовлетворения данного функционального требования безопасности ОО.

Если никакие функции безопасности ИТ не прослежены к конкретному требованию безопасности ОО, то результат данного шага оценивания отрицательный.

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

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.

Несмотря на то, что прослеживание функций безопасности ИТ к функциональным требованиям безопасности ОО, представленное в краткой спецификации ОО, может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

9.3.8.3.6 Шаг оценивания ASE_TSS.1-6

Оценщик должен исследовать подраздел «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.

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

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.

Обычно адекватность означает, что заявленная 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).

9.3.8.3.7 Шаг оценивания ASE_TSS.1-7

ИСО/МЭК 15408-3 ASE_TSS.1.6C: *Обоснование краткой спецификации ОО должно демонстрировать, что сочетание специфицированных функций безопасности ИТ в совокупности способно удовлетворить функциональные требования безопасности ОО.*

Оценщик должен исследовать подраздел «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.

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 устанавливает, не приводит ли включение данной информации к внесению потенциальных недостатков безопасности, таких, например, как возможность обхода, вмешательства в работу или деактивации механизмов, реализующих другие функции безопасности ИТ.

9.3.8.3.8 Шаг оценивания ASE_TSS.1-8

ИСО/МЭК 15408-3 ASE_TSS.1.7C: *Краткая спецификация ОО должна сопоставить меры и требования доверия так, чтобы можно было отметить, какие меры способствуют удовлетворению каких требований.*

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

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

9.3.8.3.9 Шаг оценивания ASE_TSS.1-9

ИСО/МЭК 15408-3 ASE_TSS.1.8C: *Обоснование краткой спецификации ОО должно демонстрировать, что меры доверия удовлетворяют все требования доверия к ОО.*

Оценщик должен исследовать подраздел «Обоснование краткой спецификации ОО», чтобы сделать заключение, содержится ли в нем для каждого требования доверия к безопасности ОО приемлемое логическое обоснование того, что конкретные меры доверия удовлетворяют данному требованию доверия к безопасности ОО.

Если ни одна мера доверия не прослежена к конкретному требованию доверия к безопасности ОО, то результат данного шага оценивания отрицательный.

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

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.

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

Несмотря на то, что прослеживание мер доверия к требованиям доверия к безопасности ОО, представленное в разделе «Краткая спецификация ОО», может быть частью логического обоснования, само по себе оно не является логическим обоснованием.

9.3.8.3.10 Шаг оценивания ASE_TSS.1-10

ИСО/МЭК 15408-3 ASE_TSS.1.9C: *Краткая спецификация ОО должна идентифицировать все функции безопасности ИТ, которые реализованы вероятностным или перестановочным механизмом соответственно.*

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

Если требования доверия к безопасности ОО не содержат компонент AVA_SOF.1, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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.

9.3.8.3.11 Шаг оценивания ASE_TSS.1-11

ИСО/МЭК 15408-3 ASE_TSS.1.10C: *Краткая спецификация ОО должна установить для каждой функции безопасности ИТ, для которой это необходимо, требование стойкости функции либо по специальной метрике, либо как базовую, среднюю или высокую СФБ.*

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.

Если требования доверия к безопасности ОО не включают в себя компонент AVA_SOF.1, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

9.3.8.4 Действие ASE_TSS.1.2E

9.3.8.4.1 Шаг оценивания ASE_TSS.1-12

Оценщик должен исследовать раздел «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел полным.

Раздел «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.

9.3.8.4.2 Шаг оценивания ASE_TSS.1-13

Оценщик должен исследовать раздел «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел логически упорядоченным.

Раздел «Краткая спецификация ОО» является логически упорядоченным, если его структура и содержание понятны целевой аудитории (т.е. оценщикам и разработчикам).

9.3.8.4.3 Шаг оценивания ASE_TSS.1-14

Оценщик должен исследовать раздел «Краткая спецификация ОО», чтобы сделать заключение, является ли данный раздел внутренне непротиворечивым.

Раздел «Краткая спецификация ОО» является внутренне непротиворечивым, 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.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

10 Оценка по ОУД1

10.1 Введение

ОУД1 обеспечивает базовый уровень доверия. Данный уровень доверия предусматривает анализ функций безопасности на предмет понимания режимов безопасности с использованием функциональной спецификации и документации руководств, а также выполнение независимого тестирования подмножества функций безопасности ОО.

10.2 Цели

Цель данного раздела заключается в определении минимальных усилий, необходимых для успешного выполнения оценки по ОУД1, и в предоставлении руководства по способам и средствам выполнения оценки.

10.3 Организация оценки по ОУД1

Оценка по ОУД1 предусматривает следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) виды деятельности по оценке по ОУД1, включающие в себя:

1) оценку ЗБ (раздел 9);

2) оценку управления конфигурацией (10.4);

3) оценку документов поставки и эксплуатации (10.5);

4) оценку документов разработки (10.6);

5) оценку руководств (10.7);

6) тестирование (10.8);

c) задачу оформления результатов оценки (раздел 7).

Виды деятельности по оценке следуют из требований доверия ОУД1, содержащихся в ИСО/МЭК 15408-3.

Оценка ЗБ начинается до выполнения любых подвидов деятельности по оценке ОО, так как ЗБ обеспечивает основание и контекст для выполнения этих подвидов деятельности.

В настоящем разделе приведено описание подвидов деятельности, выполняемых при оценке по ОУД1. Хотя выполнение подвидов деятельности может, в общем случае, начинаться более или менее случайным образом, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

10.4 Вид деятельности «Управление конфигурацией»

Цель вида деятельности «Управление конфигурацией» состоит в том, чтобы помочь потребителю в идентификации оцененного ОО.

10.4.1 Оценка возможностей УК (ACM_CAP.1)

10.4.1.1 Цели

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

10.4.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

10.4.1.3 Действие ACM_CAP.1.1E

10.4.1.3.1 Шаг оценивания 1:ACM_CAP.1-1

ИСО/МЭК 15408-3 ACM_CAP.1.1C: *Маркировка ОО должна быть уникальна для каждой версии ОО.*

Оценщик должен проверить, что версия ОО, представленная для оценки, уникально маркирована.

В этом компоненте доверия отсутствуют какие-либо другие требования к разработчику по использованию системы УК, кроме требования уникальной маркировки. В результате оценщик способен верифицировать уникальность версии ОО только путем проверки, что другие доступные для приобретения версии ОО не маркированы так же. При оценке, когда система УК представлена сверх требований ИСО/МЭК 15408, оценщик мог бы подтвердить уникальность маркировки путем проверки списка конфигурации. Свидетельство уникальной маркировки версии ОО, представленной для оценки, может оказаться неполным, если во время оценки была исследована только одна версия; поэтому оценщику необходимо выяснить систему маркирования, которая способна поддерживать уникальные маркировки (например, используя цифры, буквы или даты). Тем не менее, отсутствие какой-либо маркировки обычно будет приводить к отрицательному заключению по этому требованию, пока оценщик не будет уверен в возможности уникальной идентификации ОО.

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

10.4.1.3.2 Шаг оценивания 1:ACM_CAP.1-2

ИСО/МЭК 15408-3 ACM_CAP.1.2C: *ОО должен быть помечен маркировкой.*

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

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

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО может отображать свое наименование и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем физического нанесения на нем соответствующего номера.

10.4.1.3.3 Шаг оценивания 1:ACM_CAP.1-3

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, следует предусмотреть возможность связать любое помеченное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Таким образом обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей версией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ.

Оценщик также верифицирует, что маркировка ОО согласована с ЗБ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

10.5 Вид деятельности «Поставка и эксплуатация»

Вид деятельности «Поставка и эксплуатация» предназначен для определения достаточности документации по процедурам, используемым для обеспечения установки, генерации и запуска ОО способом, предусмотренным разработчиком.

10.5.1 Оценка установки, генерации и запуска (ADO_IGS.1)

10.5.1.1 Цели

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

10.5.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) руководство администратора;

b) процедуры безопасной установки, генерации и запуска;

c) ОО, пригодный для тестирования.

10.5.1.3 Замечания по применению

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

10.5.1.4 Действие ADO_IGS.1.1E

10.5.1.4.1 Шаг оценивания 1:ADO_IGS.1-1

ИСО/МЭК 15408-3 ADO_IGS.1.1C: *Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.*

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

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, если ОО поставлен в рабочем состоянии), то данный шаг оценивания (или отдельные его части) не применяют и поэтому считают удовлетворенным.

10.5.1.5 Действие ADO_IGS.1.2E

10.5.1.5.1 Шаг оценивания 1:ADO_IGS.1-2

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

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, если ОО поставлен в рабочем состоянии), то данный шаг оценивания (или отдельные его части) не применяют и поэтому считают удовлетворенным.

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

a) изменения задаваемых при инсталляции характеристик безопасности сущностей, находящихся под управлением ФБО;

b) обработки исключительных ситуаций и проблем;

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

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

10.6 Вид деятельности «Разработка»

Вид деятельности «Разработка» предназначен для оценки проектной документации на предмет ее достаточности для понимания того, каким образом ФБО предоставляют функции безопасности ОО. Это понимание достигается путем экспертизы функциональной спецификации (которая описывает внешние интерфейсы ОО) и описания соответствия представлений (которое отображает функциональную спецификацию на краткую спецификацию ОО, чтобы продемонстрировать их согласованность).

10.6.1 Замечания по применению

Требования ИСО/МЭК 15408 к проектной документации ранжированы по уровню формализации. В ИСО/МЭК 15408 рассмотрены следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ — это документ, который составлен на естественном языке. Методология не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки. Ниже дифференцировано содержание различных неформальных документов.

Неформальная функциональная спецификация включает в себя описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых интерфейсов ФБО. Например, если операционная система предоставляет пользователю средства идентифика-

ции пользователя, создания, модификации или удаления файлов, установления разрешения другим пользователям на доступ к файлам и взаимодействия с удаленными машинами, то ее функциональная спецификация, как правило, содержит описание каждой из этих функций. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание указанных функций аудита также обычно включают в состав функциональной спецификации; и хотя пользователь формально не обращается к этим функциям непосредственно через внешний интерфейс, на них определенно влияет все то, что происходит на уровне внешнего пользовательского интерфейса.

Необязательно, чтобы неформальная демонстрация соответствия представлений была в повествовательной форме; может быть достаточно простого двухмерного отображения (например, в виде таблицы).

10.6.2 Оценка функциональной спецификации (ADV_FSP.1)

10.6.2.1 Цели

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

10.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора.

10.6.2.3 Действие ADV_FSP.1.1E

10.6.2.3.1 Шаг оценивания 1:ADV_FSP.1-1

ИСО/МЭК 15408-3 ADV_FSP.1.1C: *Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.*

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

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

10.6.2.3.2 Шаг оценивания 1:ADV_FSP.1-2

ИСО/МЭК 15408-3 ADV_FSP.1.2C: *Функциональная спецификация должна быть внутренне непротиворечивой.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о ее внутренней непротиворечивости.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

10.6.2.3.3 Шаг оценивания 1:ADV_FSP.1-3

ИСО/МЭК 15408-3 ADV_FSP.1.3C: *Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

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

Термин «внешний» относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО — это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы возможен доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 6 показан ОО, включающий в себя ФБО-части (заштрихованы) и не-ФБО-части (не заштрихованы). Данный ОО имеет три внешних интерфейса: интерфейс **c** — непосредственный интерфейс ФБО; интерфейс **b** — косвенный интерфейс ФБО; интерфейс **a** — интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы **b** и **c** составляют ИФБО.

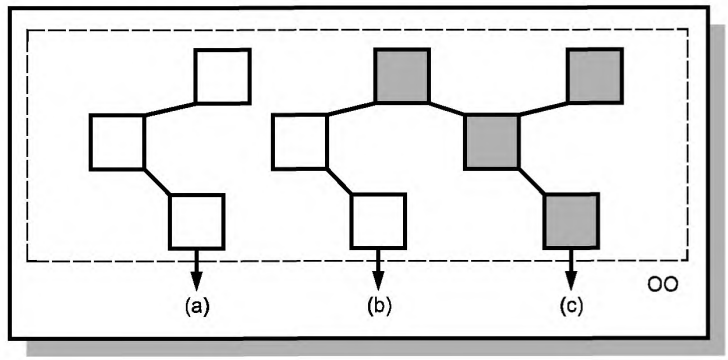


Рисунок 6 — Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях ИСО/МЭК 15408-2 (или в компонентах, дополнительных по отношению к ИСО/МЭК 15408-2), будут иметь своего рода внешне видимые проявления. И хотя необязательно все из них являются интерфейсами, через которые могут быть протестированы функции безопасности, все они до некоторой степени являются внешне видимыми и поэтому должны быть включены в функциональную спецификацию.

Руководство по определению границ ОО см. в А.6 «Границы ОО» (приложение А).

10.6.2.3.4 Шаг оценивания 1:ADV_FSP.1-4

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

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

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е. в его ЗБ включены компоненты требований из семейств FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена»), то в функциональной спецификации должны быть описаны все внешние интерфейсы, но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е. интерфейсы **b** и **c** на рисунке 6) должны быть описаны полностью, в то время как другие интерфейсы описывают только в объеме, достаточном для понимания того, что ФБО являются недоступными через рассматриваемый интерфейс (т.е. что интерфейс относится к типу **a**, а не типу **b** на рисунке 6). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс — это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, запрашиваются программой, у которой есть соответствующие привилегии. Все программы, выполняемые в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру и выполняемые в непривилегированном режиме, не способны влиять на ПБО (т.е. такие программы являются интерфейсами типа **a**, а не **b** на рисунке 6), а следовательно, могут не быть включены в функциональную спецификацию. Несмотря на то, что архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

10.6.2.3.5 Шаг оценивания 1:ADV_FSP.1-5

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

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

a) все ли относящиеся к безопасности, вводимые пользователем параметры (или характеристики этих параметров) определены. Для полноты необходимо, чтобы были определены параметры, которыми пользователь не управляет непосредственно, если они могут быть использованы администраторами;

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

c) все ли интерфейсы описаны для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса необходимо пояснение режимов его функционирования при наличии или отсутствии привилегии;

d) вся ли информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса непротиворечивы во всей документации.

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

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

10.6.2.3.6 Шаг оценивания 1:ADV_FSP.1-6

ИСО/МЭК 15408-3 ADV_FSP.1.4C: *Функциональная спецификация должна полностью представить ФБО.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни в одном из этих документов не должны быть описаны функции безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

10.6.2.4 Действие ADV_FSP.1.2E

10.6.2.4.1 Шаг оценивания 1:ADV_FSP.1-7

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением функциональных требований безопасности ОО.

С целью удостовериться, что все функциональные требования безопасности, определенные в ЗБ, охвачены функциональной спецификацией, оценщик может построить отображение краткой спецификации ОО на функциональную спецификацию. Такое отображение могло быть уже представлено самим разра-

ботчиком в качестве свидетельства для удовлетворения требований соответствия представлений (ADV_RCR.*); в этом случае оценщику необходимо только верифицировать полноту данного отображения, удостоверившись, что все функциональные требования безопасности отображены на соответствующие представления ИФБО в функциональной спецификации.

10.6.2.4.2 Шаг оценивания 1:ADV_FSP.1-8

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

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

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

10.6.3 Оценка соответствия представлений (ADV_RCR.1)

10.6.3.1 Цели

Цель данного подвида деятельности — сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ в функциональной спецификации.

10.6.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

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

10.6.3.3 Действие ADV_RCR.1.1E

10.6.3.3.1 Шаг оценивания 1:ADV_RCR.1-1

ИСО/МЭК 15408-3 ADV_RCR.1.1C: *Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.*

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

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

Оценщик анализирует соответствие между функциями безопасности ОО в краткой спецификации ОО и в функциональной спецификации. Оценщик проверяет непротиворечивость и точность данного соответствия. Там, где материалы анализа соответствия указывают на связь между описанием функции безопасности в краткой спецификации ОО и описанием интерфейса в функциональной спецификации, оценщик верифицирует, что описанные функциональные возможности безопасности являются одними и теми же. Если функции безопасности, описанные в краткой спецификации ОО, точно и полно представлены в описаниях соответствующих интерфейсов, рассматриваемый шаг оценивания считают выполненным.

Данный шаг оценивания может быть выполнен совместно с шагами оценивания ADV_FSP.1-7 и ADV_FSP.1-8.

10.7 Вид деятельности «Руководства»

Вид деятельности «Руководства» предназначен для определения достаточности документации, регламентирующей эксплуатацию ОО. Такая документация ориентирована как на доверенных администрато-

ров и не связанных с администрированием пользователей, чьи неправильные действия могли бы отрицательно повлиять на безопасность ОО, так и на недоверенных пользователей, чьи неправильные действия могли бы отрицательно повлиять на безопасность их собственных данных.

10.7.1 Замечания по применению

Вид деятельности «Руководства» применяют к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО должна быть описана в ЗБ.

10.7.2 Оценка руководства администратора (AGD_ADM.1)

10.7.2.1 Цели

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

10.7.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска.

10.7.2.3 Замечания по применению

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

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

10.7.2.4 Действие AGD_ADM.1.1E

10.7.2.4.1 Шаг оценивания 1:AGD_ADM.1-1

ИСО/МЭК 15408-3 AGD_ADM.1.1C: *Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описаны ли в нем относящиеся к администрированию функции безопасности и интерфейсы, доступные администратору ОО.

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

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

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

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

b) параметры, устанавливаемые администратором, их допустимые значения и значения по умолчанию;

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

10.7.2.4.2 Шаг оценивания 1:AGD_ADM.1-2

ИСО/МЭК 15408-3 AGD_ADM.1.2C: *Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описан ли в нем безопасный способ администрирования ОО.

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

10.7.2.4.3 Шаг оценивания 1:AGD_ADM.1-3

ИСО/МЭК 15408-3 AGD_ADM.1.3C: *Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, содержит ли оно предупреждения относительно функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

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

10.7.2.4.4 Шаг оценивания 1:AGD_ADM.1-4

ИСО/МЭК 15408-3 AGD_ADM.1.4C: *Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство администратора должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

10.7.2.4.5 Шаг оценивания 1:AGD_ADM.1-5

ИСО/МЭК 15408-3 AGD_ADM.1.5C: *Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.*

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

Для каждого параметра безопасности в руководстве администратора должны быть описаны предназначение параметра, допустимые значения параметра и его значение по умолчанию, а также безопасные и небезопасные настройки этих параметров как по отдельности, так и в сочетании.

10.7.2.4.6 Шаг оценивания 1:AGD_ADM.1-6

ИСО/МЭК 15408-3 AGD_ADM.1.6C: *Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.*

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

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

10.7.2.4.7 Шаг оценивания 1:AGD_ADM.1-7

ИСО/МЭК 15408-3 AGD_ADM.1.7C: *Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

10.7.2.4.8 Шаг оценивания 1:AGD_ADM.1-8

ИСО/МЭК 15408-3 AGD_ADM.1.8C: *Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

10.7.3 Оценка руководства пользователя (AGD_USR.1)

10.7.3.1 Цели

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

10.7.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска.

10.7.3.3 Замечания по применению

В ЗБ могут быть определены несколько различных ролей или групп пользователей, опознаваемых объектом оценки и взаимодействующих с ФБО. Возможности этих ролей и связанные с ними привилегии описывают в ЗБ в классе FMT «Управление безопасностью». Различные роли и группы пользователей должны быть рассмотрены в руководстве пользователя.

10.7.3.4 Действие AGD_USR.1.1E

10.7.3.4.1 Шаг оценивания 1:AGD_USR.1-1

ИСО/МЭК 15408-3 AGD_USR.1.1C: *Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.*

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

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

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

10.7.3.4.2 Шаг оценивания 1:AGD_USR.1-2

ИСО/МЭК 15408-3 AGD_USR.1.2C: *Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.*

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

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

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

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

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

b) параметры, устанавливаемые пользователем, их допустимые значения и значения по умолчанию;

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

10.7.3.4.3 Шаг оценивания 1:AGD_USR.1-3

ИСО/МЭК 15408-3 AGD_USR.1.3C: *Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство пользователя, чтобы сделать заключение, содержит ли оно предупреждения относительно доступных пользователю функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

В руководстве пользователя должны быть идентифицированы функции и привилегии, которые могут быть применены, требуемые для них типы команд и объяснения таких команд. В руководстве пользователя должны быть приведены предупреждающие сообщения относительно использования функций и привилегий, подлежащих контролю. Предупреждающие сообщения должны быть связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

10.7.3.4.4 Шаг оценивания 1:AGD_USR.1-4

ИСО/МЭК 15408-3 AGD_USR.1.4C: *Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство пользователя должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

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

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

10.7.3.4.5 Шаг оценивания 1:AGD_USR.1-5

ИСО/МЭК 15408-3 AGD_USR.1.5C: *Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

10.7.3.4.6 Шаг оценивания 1:AGD_USR.1-6

ИСО/МЭК 15408-3 AGD_USR.1.6C: *Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

10.8 Вид деятельности «Тестирование»

Цель данного вида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО установить, ведет ли себя ОО как предписано в проектной документации и в соответствии с функциональными требованиями безопасности ОО, определенными в ЗБ.

10.8.1 Замечания по применению

Объем и состав подмножества тестов оценщика зависят от нескольких факторов, рассматриваемых в подвиде деятельности «Независимое тестирование» (ATE_IND.1 «Независимое тестирование на соответствие»). Один из таких факторов, оказывающих влияние на состав подмножества тестов, — это известные из общедоступных источников слабые места, к информации о которых оценщику необходимо получить доступ (например, в рамках системы оценки).

Для разработки тестов оценщик должен понять ожидаемый режим выполнения функций безопасности применительно к требованиям, которым они должны удовлетворять. Оценщик может предпочесть анализировать функции безопасности ФБО поочередно, рассматривая конкретное требование ЗБ, а также — соответствующие части функциональной спецификации и документации руководств для понимания ожидаемого режима функционирования ОО.

10.8.2 Оценка путем независимого тестирования (ATE_IND.1)

10.8.2.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО определить, функционирует ли ОО в соответствии с тем, как определено в спецификациях.

10.8.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска;

f) ОО, пригодный для тестирования.

10.8.2.3 Действие ATE_IND.1.1E

10.8.2.3.1 Шаг оценивания 1:ATE_IND.1-1

ИСО/МЭК 15408-3 ATE_IND.1.1C: *ОО должен быть пригоден для тестирования.*

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.1 «Номера версий».

В ЗБ может быть определено более одной подлежащей оценке конфигурации. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут относиться к среде тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

При использовании любых средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

10.8.2.3.2 Шаг оценивания 1:ATE_IND.1-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности ADO_IGS.1 «Процедуры установки,

генерации и запуска» позволит считать выполненным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания ADO_IGS.1-2.

10.8.2.4 Действие ATE_IND.1.2E

10.8.2.4.1 Шаг оценивания 1:ATE_IND.1-3

Оценщик должен определить тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, приемлемую для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества ФБО, содержащего как можно большее число функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое число функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, стратегия тестирования, принятая оценщиком, должна находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику необходимо рассмотреть следующие факторы:

a) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

b) поддержание некоторого баланса между видами деятельности по оценке. Тестирование, как правило, занимает 20 % — 30 % усилий оценщика в течение оценки.

Оценщик выбирает определенные функции безопасности для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества ФБО:

a) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места неизвестны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функций безопасности;

b) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, должны быть включены в тестируемое подмножество;

c) сложность функции безопасности. Для сложных функций безопасности может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, которые, в свою очередь, не будут способствовать экономичным оценкам. С другой стороны, сложные функции безопасности – это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

d) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы могут обеспечивать несколько функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

e) типы интерфейсов ОО (например, программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть возможность включения тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

f) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

Выше сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

10.8.2.4.2 Шаг оценивания 1:ATE_IND.1-4

Оценщик должен разработать тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Установив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

a) подход, который будет использован, например, будет ли функция безопасности протестирована через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет применен альтернативный тестированию подход (например, в исключительных обстоятельствах — экспертиза кода);

b) интерфейс(ы) функции безопасности, который(е) будет(ут) использован(ы) для инициирования выполнения функции безопасности и наблюдения ее реакции;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности (например, генераторы пакетов), либо для наблюдения за функцией безопасности (например, сетевые анализаторы).

Оценщик может посчитать практичным тестировать каждую функцию безопасности с помощью ряда наборов тестов, где каждый набор тестов будет использован для тестирования конкретного режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

10.8.2.4.3 Шаг оценивания 1:ATE_IND.1-5

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для тестирования ОО, но это не мешает ему выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты должны быть внесены в тестовую документацию.

10.8.2.4.4 Шаг оценивания 1:ATE_IND.1-6

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестов:

a) идентификационную информацию тестируемого режима выполнения функции безопасности;

b) инструкции по подключению и настройке всего необходимого оборудования для тестирования, как это требуется для выполнения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения функции безопасности;

f) описание всех ожидаемых результатов и необходимого анализа, проводимого по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО;

h) фактические результаты тестирования.

Уровень детализации должен быть таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут различаться (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, приведенную на этом шаге оценивания (например, фактические результаты тестирования могут не требовать какого-либо анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

10.8.2.4.5 Шаг оценивания 1:ATE_IND.1-7

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая документация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

10.8.2.4.6 Шаг оценивания 1:ATE_IND.1-8

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию, объема выполненного тестирования, тестируемых конфигураций ОО и общих результатов вида деятельности по тестированию.

Информация об усилиях оценщика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, подвергнутые тестированию;

b) выбранный размер подмножества. Число протестированных в течение оценки функций безопасности и логическое обоснование этого размера;

c) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

d) протестированные функции безопасности. Краткий перечень функций безопасности, обоснованно включенных в подмножество;

e) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Приведенный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует представить в ТОО.

11 Оценка по ОУД2

11.1 Введение

ОУД2 обеспечивает независимо подтверждаемый уровень доверия к безопасности в диапазоне от невысокого до умеренного. Для обеспечения понимания режимов безопасного функционирования ОО функции безопасности анализируют с использованием функциональной спецификации, документации руководств и проекта верхнего уровня ОО. Данный анализ должен быть поддержан независимым тестированием подмножества функций безопасности ОО, свидетельством тестирования разработчиком, основанным на функциональной спецификации, выборочным подтверждением результатов тестирования разработчиком, анализом стойкости функций безопасности и свидетельством поиска разработчиком явных уязвимостей. Дополнительно доверие достигают применением списка конфигурации для ОО и свидетельства безопасных процедур поставки.

11.2 Цели

Цель данного раздела заключается в определении минимальных усилий, необходимых для успешного выполнения оценки по ОУД2, и в предоставлении руководства по способам и средствам выполнения оценки.

11.3 Организация оценки по ОУД2

Оценка по ОУД2 предусматривает следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) виды деятельности по оценке по ОУД2, включающие в себя:

1) оценку ЗБ (раздел 9);

2) оценку управления конфигурацией (11.4);

3) оценку документов поставки и эксплуатации (11.5);

4) оценку документов разработки (11.6);

5) оценку руководств (11.7);

6) оценку тестов (11.8);

7) тестирование (11.8);

8) оценку оценки уязвимостей (11.9);

c) задачу оформления результатов оценки (раздел 7).

Виды деятельности по оценке следуют из требований доверия ОУД2, содержащихся в ИСО/МЭК 15408-3.

Оценка ЗБ начинается до выполнения любых подвидов деятельности по оценке ОО, так как ЗБ обеспечивает основание и контекст для выполнения этих подвидов деятельности.

В настоящем разделе приведено описание подвидов деятельности, выполняемых при оценке по ОУД2. Хотя выполнение подвидов деятельности может, в общем случае, начинаться более или менее случайным образом, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

11.4 Вид деятельности «Управление конфигурацией»

Цель вида деятельности «Управление конфигурацией» состоит в том, чтобы помочь потребителю в идентификации оцененного ОО и удостовериться, что элементы конфигурации уникально идентифицированы.

11.4.1 Оценка возможностей УК (ACM_CAP.2)

11.4.1.1 Цели

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

11.4.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация управления конфигурацией.

11.4.1.3 Замечания по применению

Этот компонент содержит неявное действие оценщика, чтобы установить, что система УК используется. Поскольку требования данного компонента ограничены идентификацией ОО и условием наличия списка конфигурации, это действие уже охвачено и ограничивается приведенными ниже шагами оценивания. Требования, изложенные в компоненте ACM_CAP.3 «Средства контроля авторизации», выходят за рамки этих двух составляющих, и поэтому будет необходимо более явное свидетельство использования системы УК.

11.4.1.4 Действие ACM_CAP.2.1E

11.4.1.4.1 Шаг оценивания 2:ACM_CAP.2-1

ИСО/МЭК 15408-3 ACM_CAP.2.1C: *Маркировка ОО должна быть уникальна для каждой версии ОО.*

Оценщик должен проверить, что версия ОО, представленная для оценки, уникально маркирована.

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

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

11.4.1.4.2 Шаг оценивания 2:ACM_CAP.2-2

ИСО/МЭК 15408-3 ACM_CAP.2.2C: *ОО должен быть помечен маркировкой.*

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

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

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО может отображать свое наименование и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем физического нанесения на нем соответствующего номера.

11.4.1.4.3 Шаг оценивания 2:ACM_CAP.2-3

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, должна быть возможность связать любое помеченное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Таким образом обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей версией руководства, необходимой для эксплуатации данного ОО в соответствии с его ЗБ. Оценщик может использовать список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласована с ЗБ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.4.1.4.4 Шаг оценивания 2:ACM_CAP.2-4

ИСО/МЭК 15408-3 ACM_CAP.2.3C: *Документация УК должна включать в себя список конфигурации.*

Оценщик должен проверить, что представленная документация УК включает в себя список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

11.4.1.4.5 Шаг оценивания 2:ACM_CAP.2-5

ИСО/МЭК 15408-3 ACM_CAP.2.4C: *Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен проверить, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

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

11.4.1.4.6 Шаг оценивания 2:ACM_CAP.2-6

ИСО/МЭК 15408-3 ACM_CAP.2.5C: *Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.*

Оценщик должен исследовать список конфигурации, чтобы сделать заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP «Область УК». Если компоненты из семейства ACM_SCP «Область УК» не используются, оценщику следует оценить адекватность списка конфигурации на основе подхода, принятого разработчиком к УК, ориентируясь в качестве максимальных требований на требования компонента ACM_SCP.1 «Охват УК объекта оценки» (так как было бы необоснованно ожидать большего, чем требуется в данном компоненте). Например, в случае внесения изменения в ОО или в какой-либо элемент документации оценщик может определить или выяснить, на каком уровне детализации перевыпущен данный элемент. Эта степень детализации должна соответствовать элементам конфигурации, которые находятся в списке конфигурации.

11.4.1.4.7 Шаг оценивания 2:ACM_CAP.2-7

ИСО/МЭК 15408-3 ACM_CAP.2.6C: *Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.*

Оценщик должен исследовать способ идентификации элементов конфигурации, чтобы сделать заключение, что он описывает, каким образом элементы конфигурации идентифицируют уникально.

11.4.1.4.8 Шаг оценивания 2:ACM_CAP.2-8

ИСО/МЭК 15408-3 ACM_CAP.2.7C: *Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен исследовать элементы конфигурации с целью сделать заключение, что способ их идентификации соответствует документации УК.

Доверие к тому, что система УК однозначно идентифицирует все элементы конфигурации, должно быть достигнуто путем изучения идентификаторов элементов конфигурации. Как для элементов конфигурации, которые составляют ОО, так и для проектов элементов конфигурации, которые представлены разработчиком в качестве свидетельств оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором в соответствии с методом уникальной идентификации, описанным в документации УК.

11.5 Вид деятельности «Поставка и эксплуатация»

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

11.5.1 Оценка поставки (ADO_DEL.1)

11.5.1.1 Цели

Цель данного подвида деятельности — сделать заключение, описаны ли в документации поставки все процедуры, применяемые для поддержания безопасности ОО при его распространении по объектам использования.

11.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация поставки.

11.5.1.3 Действие ADO_DEL.1.1E

11.5.1.3.1 Шаг оценивания 2:ADO_DEL.1-1

ИСО/МЭК 15408-3 ADO_DEL.1.1C: *Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.*

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

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

В документации поставки должны быть описаны надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки. В этих процедурах должно быть описано, какие части ОО должны быть охвачены подобными процедурами. В документации поставки должны быть приведены процедуры как для распространения физических копий, так и распространения в электронном виде (например, через Интернет), где это применимо. Процедуры поставки относятся к ОО в целом, включая применяемое программное обеспечение, аппаратные средства, программно-аппаратные средства и документацию.

Акцент в документации поставки, вероятно, будет сделан на мерах, связанных с целостностью, поскольку для поддержки целостности ОО в процессе его поставки требуется применение технических мер. Однако при поставке некоторых ОО должны быть обеспечены конфиденциальность и доступность; процедуры, относящиеся к этим аспектам безопасной поставки, должны также быть рассмотрены в документации.

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

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

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

11.5.1.4 Подразумеваемое действие оценщика

11.5.1.4.1 Шаг оценивания 2:ADO_DEL.1-2

ИСО/МЭК 15408-3 ADO_DEL.1.2D: *Разработчик должен использовать процедуры поставки.*

Оценщик должен исследовать процедуры процесса поставки, чтобы сделать заключение о применении этих процедур.

Подход, предпринятый оценщиком для проверки применения процедур поставки, будет зависеть от природы ОО и самого процесса поставки. В дополнение к исследованию собственно процедур оценщику необходимо получить и определенную уверенность в их действительном применении. Некоторые возможные подходы перечислены ниже.

a) Посещение объекта (объектов) распространения, где можно наблюдать практическое применение процедур.

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

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

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

Для только что разработанного ОО возможно, что процедуры поставки еще необходимо отработать. В подобных случаях оценщику придется удовлетвориться тем, что имеются соответствующие процедуры и средства выполнения предстоящих поставок и что весь привлекаемый персонал знает свои обязанности. Оценщик может запросить «пробный прогон» поставки, если это практически осуществимо. Если разработчик производит другие подобные продукты, то для приобретения доверия может быть полезно исследование процедур при их применении.

11.5.2 Оценка установки, генерации и запуска (ADO_IGS.1)

11.5.2.1 Цели

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

11.5.2.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) руководство администратора;

b) процедуры безопасной установки, генерации и запуска;

c) ОО, пригодный для тестирования.

11.5.2.3 Замечания по применению

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

11.5.2.4 Действие ADO_IGS.1.1E

11.5.2.4.1 Шаг оценивания 2:ADO_IGS.1-1

ИСО/МЭК 15408-3 ADO_IGS.1.1C: *Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.*

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

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, если ОО поставлен в рабочем состоянии), то данный шаг оценивания (или отдельные его части) не применяют и поэтому считают удовлетворенным.

11.5.2.5 Действие ADO_IGS.1.2E

11.5.2.5.1 Шаг оценивания 2:ADO_IGS.1-2

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

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

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

a) изменения задаваемых при инсталляции характеристик безопасности сущностей, находящихся под управлением ФБО;

b) обработки исключительных ситуаций и проблем;

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

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

11.6 Вид деятельности «Разработка»

Вид деятельности «Разработка» предназначен для оценки проектной документации на предмет ее достаточности для понимания того, каким образом ФБО предоставляют функции безопасности ОО. Это понимание должно быть достигнуто путем экспертизы все более уточненных описаний в проектной документации ФБО. Проектная документация состоит из функциональной спецификации (которая описывает внешние интерфейсы ОО) и проекта верхнего уровня (который описывает архитектуру ОО в терминах внутренних подсистем). Имеется также описание соответствия представлений (которое отображает представления ОО друг на друга, чтобы продемонстрировать их согласованность).

11.6.1 Замечания по применению

Требования ИСО/МЭК 15408 к проектной документации ранжированы по уровню формализации. В ИСО/МЭК 15408 рассмотрены следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ — это документ, который составлен на естественном языке. Методология не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки. Ниже дифференцировано содержание различных неформальных документов.

Неформальная функциональная спецификация включает в себя описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых интерфейсов ФБО. Например, если операционная система предоставляет пользователю средства идентификации пользователя, создания, модификации или удаления файлов, установления разрешения другим пользователям на доступ к файлам и взаимодействия с удаленными машинами, то ее функциональная спецификация, как правило, содержит описание каждой из этих функций. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание указанных функций аудита также обычно включают в состав функциональной спецификации; и хотя пользователь формально не обращается к этим функциям непосредственно через внешний интерфейс, на них определенно влияет все то, что происходит на уровне внешнего пользовательского интерфейса.

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

Необязательно, чтобы неформальная демонстрация соответствия была в повествовательной форме; может быть достаточно простого двухмерного отображения (например, в виде таблицы).

11.6.2 Оценка функциональной спецификации (ADV_FSP.1)

11.6.2.1 Цели

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

11.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора.

11.6.2.3 Действие ADV_FSP.1.1E

11.6.2.3.1 Шаг оценивания 2:ADV_FSP.1-1

ИСО/МЭК 15408-3 ADV_FSP.1.1C: *Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.*

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

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

11.6.2.3.2 Шаг оценивания 2:ADV_FSP.1-2

ИСО/МЭК 15408-3 ADV_FSP.1.2C: *Функциональная спецификация должна быть внутренне непротиворечивой.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о ее внутренней непротиворечивости.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.6.2.3.3 Шаг оценивания 2:ADV_FSP.1-3

ИСО/МЭК 15408-3 ADV_FSP.1.3C: *Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

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

Термин «внешний» относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО — это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы возможен доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 7 показан ОО, включающий в себя ФБО-части (заштрихованы) и не-ФБО-части (не заштрихованы). Данный ОО имеет три внешних интерфейса: интерфейс **c** — непосредственный интерфейс ФБО; интерфейс **b** — косвенный интерфейс ФБО; интерфейс **a** — интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы **b** и **c** составляют ИФБО.

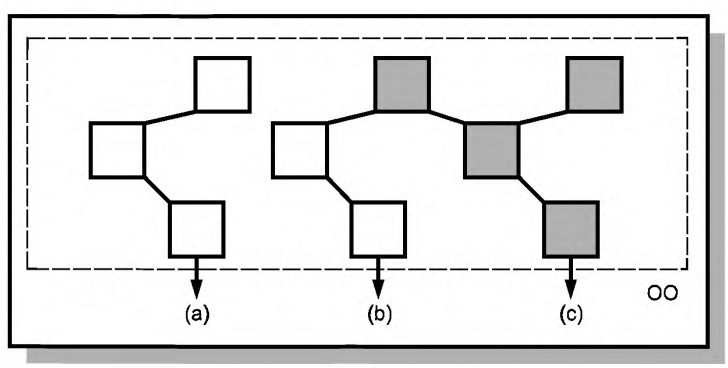


Рисунок 7 — Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях ИСО/МЭК 15408-2 (или в компонентах, дополнительных по отношению к ИСО/МЭК 15408-2), будут иметь своего рода внешне видимые проявления. И хотя не обязательно все из них являются интерфейсами, через которые могут быть протестированы функции безопасности, все они до некоторой степени являются внешне видимыми и поэтому должны быть включены в функциональную спецификацию.

Руководство по определению границ ОО см. в А.6 «Границы ОО» (приложение А).

11.6.2.3.4 Шаг оценивания 2:ADV_FSP.1-4

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

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

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е. в его ЗБ включены компоненты требований из семейств FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена»), то в функциональной спецификации должны быть описаны все внешние интерфейсы, но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е. интерфейсы **b** и **c** на рисунке 7) должны быть описаны полностью, в то время как другие интерфейсы описывают только в объеме, достаточном для понимания того, что ФБО являются недоступными через рассматриваемый интерфейс (т.е. что интерфейс относится к типу **a**, а не типу **b** на рисунке 7). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс — это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, запрашиваются программой, у которой есть соответствующие привилегии. Все программы, выполняемые в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру и выполняемые в непривилегированном режиме, не способны влиять на ПБО (т.е. такие программы являются интерфейсами типа **a**, а не **b** на рисунке 7), а следовательно, могут не быть включены в функциональную спецификацию. Несмотря на то, что архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

11.6.2.3.5 Шаг оценивания 2:ADV_FSP.1-5

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

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

a) все ли относящиеся к безопасности, вводимые пользователем параметры (или характеристики этих параметров) определены. Для полноты необходимо, чтобы были определены параметры, которыми пользователь не управляет непосредственно, если они могут быть использованы администраторами;

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

c) все ли интерфейсы описаны для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса необходимо пояснение режимов его функционирования при наличии или отсутствии привилегии;

d) вся ли информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса непротиворечивы во всей документации.

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

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

11.6.2.3.6 Шаг оценивания 2:ADV_FSP.1-6

ИСО/МЭК 15408-3 ADV_FSP.1.4C: *Функциональная спецификация должна полностью представить ФБО.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни в одном из этих документов не должны быть описаны функции безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

11.6.2.4 Действие ADV_FSP.1.2E

11.6.2.4.1 Шаг оценивания 2:ADV_FSP.1-7

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением функциональных требований безопасности ОО.

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

11.6.2.4.2 Шаг оценивания 2:ADV_FSP.1-8

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

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

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

11.6.3 Оценка проекта верхнего уровня (ADV_HLD.1)

11.6.3.1 Цели

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

11.6.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня.

11.6.3.3 Действие ADV_HLD.1.1E

11.6.3.3.1 Шаг оценивания 2:ADV_HLD.1-1

ИСО/МЭК 15408-3 ADV_HLD.1.1C: *Представление проекта верхнего уровня должно быть неформальным.*

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

Если весь проект верхнего уровня является неформальным, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

11.6.3.3.2 Шаг оценивания 2:ADV_HLD.1-2

ИСО/МЭК 15408-3 ADV_HLD.1.2C: *Проект верхнего уровня должен быть внутренне непротиворечивым.*

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

11.6.3.3.3 Шаг оценивания 2:ADV_HLD.1-3

ИСО/МЭК 15408-3 ADV_HLD.1.3C: *Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.*

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах подсистем.

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

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

Подсистемы, используемые для описания проекта верхнего уровня, не обязательно называются «подсистемами», но необходимо, чтобы они представляли собой подобный уровень декомпозиции. Например, при декомпозиции проекта могут быть использованы понятия «слои» или «менеджеры».

11.6.3.3.4 Шаг оценивания 2:ADV_HLD.1-4

ИСО/МЭК 15408-3 ADV_HLD.1.4C: *Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.*

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

Описание режима безопасного функционирования подсистемы — это описание того, что делает подсистема. Оно должно включать в себя описание любых действий, выполнение которых может быть предпи-

сано подсистеме с учетом ее функций и влияния, которое может оказать подсистема на состояние безопасности ОО (например, изменения в субъектах, объектах, базах данных безопасности).

11.6.3.3.5 Шаг оценивания 2:ADV_HLD.1-5

ИСО/МЭК 15408-3 ADV_HLD.1.5C: *Проект верхнего уровня должен идентифицировать любые базовые аппаратные, программно-аппаратные и/или программные средства, требуемые ФБО, с представлением функций, обеспечиваемых поддерживающими механизмами защиты, реализованными в этих аппаратных, программно-аппаратных и/или программных средствах.*

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

11.6.3.3.6 Шаг оценивания 2:ADV_HLD.1-6

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

11.6.3.3.7 Шаг оценивания 2:ADV_HLD.1-7

ИСО/МЭК 15408-3 ADV_HLD.1.6C: *Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.*

Оценщик должен проверить, идентифицированы ли в проекте верхнего уровня интерфейсы подсистем ФБО.

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

11.6.3.3.8 Шаг оценивания 2:ADV_HLD.1-8

ИСО/МЭК 15408-3 ADV_HLD.1.7C: *Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.*

Оценщик должен проверить, идентифицировано ли в проекте верхнего уровня, какие интерфейсы подсистем ФБО являются внешне видимыми.

11.6.3.4 Действие ADV_HLD.1.2E

11.6.3.4.1 Шаг оценивания 2:ADV_HLD.1-9

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, является ли он точным отображением функциональных требований безопасности ОО.

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

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

11.6.3.4.2 Шаг оценивания 2:ADV_HLD.1-10

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

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

11.6.4 Оценка соответствия представлений (ADV_RCR.1)

11.6.4.1 Цели

Цель данного подвида деятельности — сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ и функциональной спецификации в проекте верхнего уровня.

11.6.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией;

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

11.6.4.3 Действие ADV_RCR.1.1E

11.6.4.3.1 Шаг оценивания 2:ADV_RCR.1-1

ИСО/МЭК 15408-3 ADV_RCR.1.1C: *Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.*

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

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

Оценщик анализирует соответствие между функциями безопасности ОО в краткой спецификации ОО и в функциональной спецификации. Оценщик проверяет непротиворечивость и точность данного соответствия. Там, где материалы анализа соответствия указывают на связь между описанием функции безопасности в краткой спецификации ОО и описанием интерфейса в функциональной спецификации, оценщик верифицирует, что описанные функциональные возможности безопасности являются одними и теми же. Если функции безопасности, описанные в краткой спецификации ОО, точно и полно представлены в описаниях соответствующих интерфейсов, рассматриваемый шаг оценивания считают выполненным.

Данный шаг оценивания может быть выполнен совместно с шагами оценивания ADV_FSP.1-7 и ADV_FSP.1-8.

11.6.4.3.2 Шаг оценивания 2:ADV_RCR.1-2

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

Оценщик использует материалы анализа соответствия, функциональную спецификацию и проект верхнего уровня, чтобы удостовериться в возможности отобразить каждую функцию безопасности, идентифицированную в функциональной спецификации, на какую-либо подсистему ФБО, описанную в проекте верхнего уровня. Для каждой функции безопасности материалы соответствия указывают, какие подсистемы ФБО предполагают поддержку данной функции безопасности. Оценщик верифицирует, что проект верхнего уровня содержит описание корректной реализации каждой функции безопасности.

11.7 Вид деятельности «Руководства»

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

11.7.1 Замечания по применению

Вид деятельности «Руководства» применяют к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО должна быть описана в ЗБ.

11.7.2 Оценка руководства администратора (AGD_ADM.1)

11.7.2.1 Цели

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

11.7.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска.

11.7.2.3 Замечания по применению

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

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

11.7.2.4 Действие AGD_ADM.1.1E

11.7.2.4.1 Шаг оценивания 2:AGD_ADM.1-1

ИСО/МЭК 15408-3 AGD_ADM.1.1C: *Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описаны ли в нем относящиеся к администрированию функции безопасности и интерфейсы, доступные администратору ОО.

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

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

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

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

b) параметры, устанавливаемые администратором, их допустимые значения и значения по умолчанию;

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

11.7.2.4.2 Шаг оценивания 2:AGD_ADM.1-2

ИСО/МЭК 15408-3 AGD_ADM.1.2C: *Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описан ли в нем безопасный способ администрирования ОО.

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

11.7.2.4.3 Шаг оценивания 2:AGD_ADM.1-3

ИСО/МЭК 15408-3 AGD_ADM.1.3C: *Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, содержит ли оно предупреждения относительно функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

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

11.7.2.4.4 Шаг оценивания 2:AGD_ADM.1-4

ИСО/МЭК 15408-3 AGD_ADM.1.4C: *Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство администратора должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

11.7.2.4.5 Шаг оценивания 2:AGD_ADM.1-5

ИСО/МЭК 15408-3 AGD_ADM.1.5C: *Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.*

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

Для каждого параметра безопасности в руководстве администратора должны быть описаны предназначение параметра, допустимые значения параметра и его значение по умолчанию, а также безопасные и небезопасные настройки этих параметров как по отдельности, так и в сочетании.

11.7.2.4.6 Шаг оценивания 2:AGD_ADM.1-6

ИСО/МЭК 15408-3 AGD_ADM.1.6C: *Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.*

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

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

11.7.2.4.7 Шаг оценивания 2:AGD_ADM.1-7

ИСО/МЭК 15408-3 AGD_ADM.1.7C: *Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.7.2.4.8 Шаг оценивания 2:AGD_ADM.1-8

ИСО/МЭК 15408-3 AGD_ADM.1.8C: *Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

11.7.3 Оценка руководства пользователя (AGD_USR.1)

11.7.3.1 Цели

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

11.7.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска.

11.7.3.3 Замечания по применению

В ЗБ могут быть определены несколько различных ролей или групп пользователей, опознаваемых объектом оценки и взаимодействующих с ФБО. Возможности этих ролей и связанные с ними привилегии описывают в ЗБ в классе FMT «Управление безопасностью». Различные роли и группы пользователей должны быть рассмотрены в руководстве пользователя.

11.7.3.4 Действие AGD_USR.1.1E

11.7.3.4.1 Шаг оценивания 2:AGD_USR.1-1

ИСО/МЭК 15408-3 AGD_USR.1.1C: *Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.*

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

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

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

11.7.3.4.2 Шаг оценивания 2:AGD_USR.1-2

ИСО/МЭК 15408-3 AGD_USR.1.2C: *Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.*

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

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

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

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

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

b) параметры, устанавливаемые пользователем, их допустимые значения и значения по умолчанию;

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

11.7.3.4.3 Шаг оценивания 2:AGD_USR.1-3

ИСО/МЭК 15408-3 AGD_USR.1.3C: *Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство пользователя, чтобы сделать заключение, содержит ли оно предупреждения относительно доступных пользователю функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

В руководстве пользователя должны быть идентифицированы функции и привилегии, которые могут быть применены, требуемые для них типы команд и объяснения таких команд. В руководстве пользователя должны быть приведены предупреждающие сообщения относительно использования функций и привилегий, подлежащих контролю. Предупреждающие сообщения должны быть связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

11.7.3.4.4 Шаг оценивания 2:AGD_USR.1-4

ИСО/МЭК 15408-3 AGD_USR.1.4C: *Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство пользователя должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

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

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

11.7.3.4.5 Шаг оценивания 2:AGD_USR.1-5

ИСО/МЭК 15408-3 AGD_USR.1.5C: *Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.7.3.4.6 Шаг оценивания 2:AGD_USR.1-6

ИСО/МЭК 15408-3 AGD_USR.1.6C: *Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

11.8 Вид деятельности «Тестирование»

Цель данного вида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО установить, ведут ли себя ФБО как предписано в проектной документации и в соответствии с функциональными требованиями безопасности ОО, определенными в ЗБ.

11.8.1 Замечания по применению

Оценщик анализирует тесты разработчика, чтобы определить степень их достаточности для демонстрации того, что функции безопасности выполняются в соответствии со спецификацией и чтобы понять подход разработчика к тестированию. Оценщик также выполняет некоторое подмножество документированных тестов разработчика, чтобы получить уверенность в результатах тестов разработчика. Оценщик использует результаты этого анализа в качестве исходных данных для независимого тестирования подмножества ФБО. По отношению к данному подмножеству тесты оценщика реализуют подход к тестированию, отличный от подхода, реализуемого тестами разработчика, в особенности, если тесты разработчика имеют недостатки.

Другие факторы, влияющие на объем и состав подмножества тестов оценщика, должны быть рассмотрены в подвиде деятельности, связанном с независимым тестированием (ATE_IND.2 «Выборочное независимое тестирование»). Один из таких факторов, оказывающих влияние на состав подмножества тестов, — это известные из общедоступных источников слабые места, к информации о которых оценщику необходимо получить доступ (например, в рамках системы оценки).

Для определения адекватности тестовой документации разработчика или разработки новых тестов оценщик должен понять ожидаемый режим выполнения функций безопасности применительно к требованиям, которым они должны удовлетворять. Оценщик может предпочесть анализировать функции безопасности ФБО поочередно, рассматривая конкретное требование ЗБ, а также — соответствующие части функциональной спецификации и документации руководств для понимания ожидаемого режима функционирования ОО.

11.8.2 Оценка покрытия (ATE_COV.1)

11.8.2.1 Цели

Цель данного подвида деятельности — сделать заключение, показывает ли свидетельство разработчика о покрытии тестами разработчика соответствие между тестами, идентифицированными в тестовой документации, и функциональной спецификацией.

11.8.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) функциональная спецификация;

b) тестовая документация;

c) свидетельство о покрытии тестами.

11.8.2.3 Замечания по применению

Материалы анализа покрытия тестами, представляемые разработчиком, требуются для того, чтобы показать соответствие между тестами, предоставленными в качестве свидетельства оценки, и функциональной спецификацией. Однако нет необходимости в том, чтобы в материалах анализа покрытия было продемонстрировано, что все функции безопасности были подвергнуты тестированию или что все внешние интерфейсы ФБО были подвергнуты тестированию. Подобные недостатки, при наличии, должны быть рассмотрены оценщиком в процессе выполнения подвида деятельности по независимому тестированию (ATE_IND.2).

11.8.2.4 Действие ATE_COV.1.1E

11.8.2.4.1 Шаг оценивания 2:ATE_COV.1-1

ИСО/МЭК 15408-3 ATE_COV.1.1C: *Свидетельство покрытия тестами должно показать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.*

Оценщик должен исследовать свидетельство о покрытии тестами, чтобы сделать заключение, является ли точным соответствие между тестами, идентифицированными в тестовой документации, и функциональной спецификацией.

Демонстрация соответствия может принимать форму таблицы или матрицы. Свидетельство о покрытии тестами, требуемое для рассматриваемого компонента, скорее покажет степень покрытия тестами, а не его полноту. В тех случаях, когда показана недостаточность покрытия, оценщику, чтобы это компенсировать, следует повысить уровень независимого тестирования.

На рисунке 8 отражена концептуальная структура соответствия между функциями безопасности, описанными в функциональной спецификации, и тестами, выделенными в тестовой документации для тестирования этих функций. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями тестов или общей целью выполняемого теста.

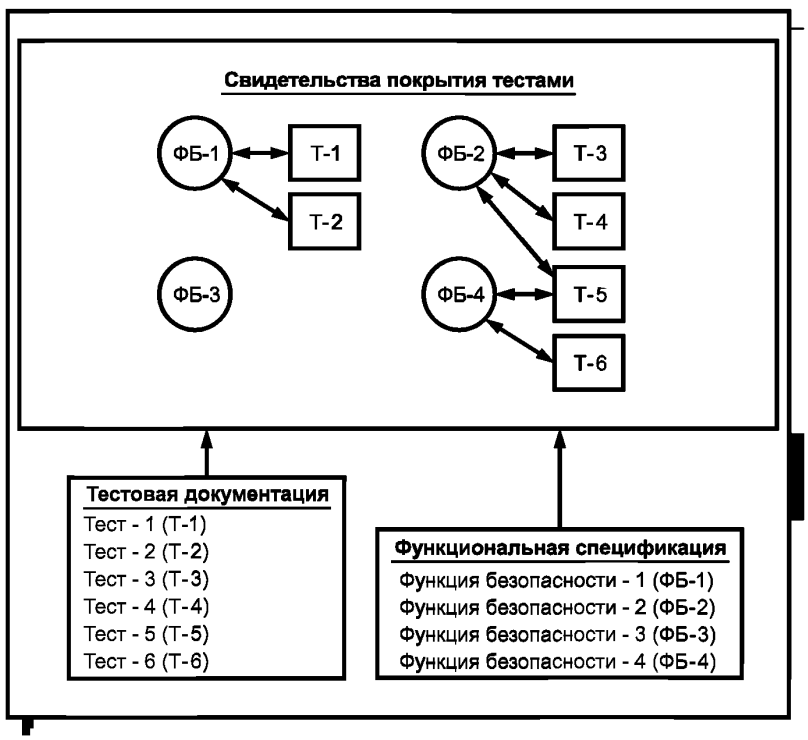


Рисунок 8 — Концептуальная структура свидетельства покрытия тестами

Идентификация тестов и функций безопасности, представленных в свидетельстве о покрытии тестами, должна быть однозначной, обеспечивая четкое соответствие между идентифицированными тестами и функциональной спецификацией тестируемых функций безопасности.

На рисунке 8 функция безопасности ФБ-3 не сопоставлена с какими бы то ни было тестами; следовательно, относительно функциональной спецификации покрытие тестами является неполным. Неполное покрытие, тем не менее, не будет влиять на вердикт по рассматриваемому подвиду деятельности, поскольку свидетельство о покрытии тестами не обязательно должно показывать полное покрытие тестами идентифицированных в функциональной спецификации функций безопасности.

11.8.3 Оценка функциональных тестов (ATE_FUN.1)

11.8.3.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли документация функциональных тестов разработчика достаточной для демонстрации того, что функции безопасности выполняются в соответствии со спецификациями.

11.8.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) процедуры тестирования.

11.8.3.3 Замечания по применению

Степень требуемого покрытия ФБО тестовой документацией зависит от соответствующего компонента доверия, связанного с покрытием тестами.

Для представленных тестов разработчика оценщик делает заключение, являются ли тесты повторимыми, и определяет степень возможности использования тестов разработчика при проведении оценщиком независимого тестирования. Любую функцию безопасности, для которой результаты тестирования разработчиком указывают, что она может быть не выполнена в соответствии со спецификациями, оценщику следует подвергнуть независимому тестированию, чтобы сделать заключение, выполнена ли она в соответствии со спецификациями или нет.

Тестовая документация должна идентифицировать все случаи использования привилегированных режимов для установления/отмены условий тестирования для последующих тестов. Тестовая документация должна описывать, почему было необходимо использовать привилегированные режимы для достижения необходимых условий (например, для обеспечения генерации средствами тестирования определенных объектов, необходимых для выполнения некоторого теста, которые не могут быть созданы непривилегированными пользователями), а также — каким образом осуществляется выход из привилегированных режимов до проведения шагов по тестированию, демонстрирующих функциональные возможности безопасности ОО. Следовательно, несмотря на то, что тестовая конфигурация может не соответствовать описанию ОО в ЗБ, в процессе установления условий тестирования тестовая документация должна содержать описание, каким образом конфигурацию можно вернуть в состояние, которое соответствует конфигурации, описанной в ЗБ, для выполнения шагов по тестированию.

11.8.3.4 Действие ATE_FUN.1.1E

11.8.3.4.1 Шаг оценивания 2:ATE_FUN.1-1

ИСО/МЭК 15408-3 ATE_FUN.1.1C: *Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.*

Оценщик должен проверить, что тестовая документация включает в себя планы тестирования, описание процедур тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

11.8.3.4.2 Шаг оценивания 2:ATE_FUN.1-2

ИСО/МЭК 15408-3 ATE_FUN.1.2C: *Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей проводимых тестов.*

Оценщик должен проверить, что в плане тестирования идентифицированы подлежащие тестированию функции безопасности.

Одним из методов, который может быть использован для идентификации проверяемой функции безопасности, является ссылка на соответствующую часть (части) функциональной спецификации, в которой определена конкретная функция безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.3 Шаг оценивания 2:ATE_FUN.1-3

Оценщик должен исследовать план тестирования, чтобы сделать заключение, содержит ли он описание целей выполняемых тестов.

План тестирования предоставляет информацию о том, каким образом должны быть протестированы функции безопасности, а также информацию о тестируемой конфигурации ОО, используемой при проведении тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.4 Шаг оценивания 2:ATE_FUN.1-4

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласована ли тестируемая конфигурация ОО с той конфигурацией, которая идентифицирована для оценки в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ. Оценщик верифицирует, что в тестовой документации разработчика определены тестируемые конфигурации и они согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

11.8.3.4.5 Шаг оценивания 2:ATE_FUN.1-5

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласован ли он с описанием процедур тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.8.3.4.6 Шаг оценивания 2:ATE_FUN.1-6

ИСО/МЭК 15408-3 ATE_FUN.1.3C: *Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.*

Оценщик должен проверить, что в описании процедур тестирования идентифицирован каждый из подлежащих тестированию режимов выполнения функций безопасности.

Одним из методов, который может быть использован для идентификации подлежащего тестированию режима выполнения функции безопасности, является ссылка на соответствующую часть (части) спецификации проекта, которая определяет конкретный подлежащий тестированию режим выполнения функции безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.7 Шаг оценивания 2:ATE_FUN.1-7

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции, позволяющие установить воспроизводимые начальные условия выполнения тестов, включая зависимости, связанные с порядком следования, при их наличии.

Для того чтобы установить начальные условия выполнения тестов, возможно, потребуется выполнить некоторые шаги. Например, необходимо добавить учетные записи пользователей прежде, чем их можно будет удалить. Пример зависимостей, связанных с порядком следования тестов, от результатов других тестов — необходимо тестирование функции аудита прежде, чем можно будет полагаться на нее при создании записей аудита для другого механизма безопасности, такого как управления доступом. Другой пример зависимости, связанной с порядком следования тестов, — при выполнении одного набора тестов генерируется файл данных, используемых в качестве исходных данных для другого набора тестов.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.8 Шаг оценивания 2:ATE_FUN.1-8

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции для того, чтобы иметь воспроизводимый способ инициирования выполнения функций безопасности и наблюдения за режимом их выполнения.

Инициирующее воздействие обычно обеспечивается внешним по отношению к функции безопасности способом через ИФБО. После того как входные данные (инициирующее воздействие) предоставлены ИФБО, через ИФБО можно наблюдать режим выполнения функции безопасности. Воспроизводимость не обеспечивается, если процедуры тестирования не содержат достаточных подробностей для однозначного описания инициирующего воздействия и режима выполнения, ожидаемого в результате инициирующего воздействия.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.9 Шаг оценивания 2:ATE_FUN.1-9

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение об их согласованности с процедурами тестирования.

Если описание процедур тестирования — это собственно процедуры тестирования, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

11.8.3.4.10 Шаг оценивания 2:ATE_FUN.1-10

ИСО/МЭК 15408-3 ATE_FUN.1.4C: *Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.*

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о достаточности включенных в нее ожидаемых результатов выполнения тестов.

Ожидаемые результаты тестирования необходимы, чтобы сделать заключение, действительно ли тест был успешно выполнен. Описание ожидаемых результатов тестирования достаточно, если оно однозначно и согласуется с ожидаемым режимом выполнения ФБО, обусловленным подходом к тестированию.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.3.4.11 Шаг оценивания 2:ATE_FUN.1-11

ИСО/МЭК 15408-3 ATE_FUN.1.5C: *Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.*

Оценщик должен проверить, что ожидаемые результаты тестирования в тестовой документации согласуются с представленными фактическими результатами тестирования.

Сравнение представленных разработчиком фактических и ожидаемых результатов тестирования выявит какие бы то ни было несоответствия результатов.

Возможно, что непосредственное сравнение фактических результатов не может быть выполнено до того, как будет выполнено некоторое преобразование или синтез данных. В подобных случаях в тестовой документации разработчика должен быть описан процесс преобразования или синтеза фактических данных.

Например, разработчику может потребоваться проверить содержимое буфера сообщений после того, как имело место сетевое соединение, чтобы определить содержимое буфера. Буфер сообщения будет содержать бинарную последовательность. Эту бинарную последовательность, как правило, преобразуют в другую форму представления данных, чтобы сделать тест более содержательным. Преобразование этого бинарного представления данных в представление более высокого уровня должно быть достаточно подробно описано разработчиком, чтобы позволить оценщику выполнить процесс преобразования (т.е. необходимо описать, используется ли синхронный или асинхронный метод передачи данных, число стоповых битов, битов четности и т.д.).

Следует отметить, что описание процесса преобразования или синтеза фактических данных оценщик использует не для того, чтобы фактически исполнить необходимую модификацию, а для того, чтобы оценить корректность этого процесса. Преобразование ожидаемых результатов тестирования в формат, позволяющий их легко сравнивать с фактическими результатами тестов, возложено на разработчика.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Если ожидаемые и фактические результаты тестирования для какого-либо из тестов не совпадают, то правильность выполнения функции безопасности не продемонстрирована. Такая ситуация окажет влияние на усилия оценщика по независимому тестированию, выражающееся в необходимости тестирования соответствующей функции безопасности. Оценщику также следует рассмотреть вопрос об увеличении выборки свидетельств, на основе которых должен быть выполнен рассматриваемый шаг оценивания.

11.8.3.4.12 Шаг оценивания 2:ATE_FUN.1-12

Оценщик должен привести в отчете информацию об усилиях разработчика по тестированию, выделив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании разработчиком, зафиксированная в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные разработчиком на тестирование ОО. Смысл предо-

ставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий разработчика по тестированию. Не обязательно, чтобы информация о тестировании разработчиком в ТОО была точной копией конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, позволяющие другим оценщикам и сотрудникам органов оценки понять подход разработчика к тестированию, объем выполненного тестирования, тестируемые конфигурации ОО и общий результат тестирования разработчиком.

Информация об усилиях разработчика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были протестированы;

b) подход к тестированию. Описание общей стратегии тестирования, которую применил разработчик;

c) объем тестирования, выполненного разработчиком. Описание степени покрытия тестами и глубины тестирования разработчиком;

d) результаты тестирования. Описание общих результатов тестирования разработчиком.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, связанной с усилиями разработчика по тестированию, которую следует привести в ТОО.

11.8.4 Оценка путем независимого тестирования (ATE_IND.2)

11.8.4.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО сделать заключение, соответствуют ли спецификациям режимы функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения выборки тестов разработчика.

11.8.4.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска;

f) тестовая документация;

g) материалы анализа покрытия тестами;

h) материалы анализа глубины тестирования;

i) ОО, пригодный для тестирования.

11.8.4.3 Действие ATE_IND.2.1E

11.8.4.3.1 Шаг оценивания 2:ATE_IND.2-1

ИСО/МЭК 15408-3 ATE_IND.2.1C: *ОО должен быть пригоден для тестирования.*

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено более одной подлежащей оценке конфигурации. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

При использовании любых средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

11.8.4.3.2 Шаг оценивания 2:ATE_IND.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности ADO_IGS.1 «Процедуры установки,

генерации и запуска» позволит считать выполненным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику необходимо выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания ADO_IGS.1-2.

11.8.4.3.3 Шаг оценивания 2:ATE_IND.2-3

ИСО/МЭК 15408-3 ATE_IND.2.2C: *Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.*

Оценщик должен исследовать набор ресурсов, предоставленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, использованных разработчиком для функционального тестирования ФБО.

Данный набор ресурсов может, кроме всего прочего, включать в себя доступное лабораториям и специальное испытательное оборудование. Ресурсы, которые не являются идентичными ресурсам, использованным разработчиком, должны быть эквивалентны им с точки зрения любого влияния, которое они могут оказать на результаты тестирования.

11.8.4.4 Действие ATE_IND.2.2E

11.8.4.4.1 Шаг оценивания 2:ATE_IND.2-4

Оценщик должен определить тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, приемлемую для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества ФБО, содержащего как можно большее число функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое число функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, стратегия тестирования, принятая оценщиком, должна находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику необходимо рассмотреть следующие факторы:

a) свидетельства тестирования разработчиком. Свидетельства тестирования разработчиком включают в себя: анализ покрытия тестами, анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком будут обеспечивать понимание того, каким образом разработчиком в ходе тестирования были проверены функции безопасности. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует, в особенности, рассмотреть:

1) усиление тестирования, выполненного разработчиком, для определенной функции (функций) безопасности. Оценщик может выполнить большее число тестов того же самого типа, чтобы путем изменения параметров более строго протестировать функцию безопасности;

2) дополнение стратегии тестирования, примененной разработчиком, для определенной функции (функций) безопасности. Оценщик может изменить подход к тестированию определенной функции безопасности, тестируя ее с использованием другой стратегии тестирования;

b) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

c) поддержание некоторого баланса между видами деятельности по оценке. Усилия оценщика, затраченные на вид деятельности по тестированию, должны быть соразмерны с усилиями, затраченными на любой другой вид деятельности по оценке.

Оценщик выбирает определенные функции безопасности для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества ФБО:

a) строгость тестирования разработчиком функций безопасности. Все функции безопасности, идентифицированные в функциональной спецификации, должны иметь относящиеся к ним свидетельства тестиро-

вания разработчиком, как это требуется в ATE_COV.2 «Анализ покрытия». Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество ФБО;

b) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что функция безопасности или ее аспект выполняется в соответствии со спецификациями, то оценщику следует включить подобные функции безопасности в тестируемое подмножество;

c) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места неизвестны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функций безопасности;

d) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

e) утверждение о СФБ, сделанное в ЗБ. Все функции безопасности, для которых было сделано конкретное утверждение о СФБ, следует включить в тестируемое подмножество ФБО;

f) сложность функции безопасности. Для сложных функций безопасности может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, что, в свою очередь, не будет способствовать экономичным оценкам. С другой стороны, сложные функции безопасности — это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

g) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы могут обеспечивать несколько функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

h) типы интерфейсов ОО (например, программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть возможность включения тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

i) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

Выше сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.4.4.2 Шаг оценивания 2:ATE_IND.2-5

Оценщик должен разработать тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Установив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

a) подход, который будет использован, например, будет ли функция безопасности протестирована через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет применен альтернативный тестированию подход (например, в исключительных обстоятельствах — экспертиза кода);

b) интерфейс(ы) функции безопасности, который(е) будет(ут) использован(ы) для инициирования выполнения функции безопасности и наблюдения ее реакции;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования выполнения функции безопасности (например, генераторы пакетов), либо для наблюдения за функцией безопасности (например, сетевые анализаторы).

Оценщик может посчитать практичным тестировать каждую функцию безопасности с помощью ряда наборов тестов, где каждый набор тестов будет использован для тестирования конкретного режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

11.8.4.4.3 Шаг оценивания 2:ATE_IND.2-6

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для тестирования ОО, но это не мешает ему выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты должны быть внесены в тестовую документацию.

11.8.4.4.4 Шаг оценивания 2:ATE_IND.2-7

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестов:

a) идентификационную информацию тестируемого режима выполнения функции безопасности;

b) инструкции по подключению и настройке всего необходимого оборудования для тестирования, как это требуется для выполнения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения функции безопасности;

f) описание всех ожидаемых результатов и необходимого анализа, проводимого по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО;

h) фактические результаты тестирования.

Уровень детализации должен быть таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут различаться (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, приведенную на этом шаге оценивания (например, фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

11.8.4.4.5 Шаг оценивания 2:ATE_IND.2-8

Оценщик должен проверить, что все фактические результаты тестирования соответствуют ожидаемым результатам тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая документация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

11.8.4.5 Действие ATE_IND.2.3E

11.8.4.5.1 Шаг оценивания 2:ATE_IND.2-9

Оценщик должен провести тестирование, используя выборку тестов, предусмотренных в плане и процедурах тестирования разработчика.

Общая цель данного шага оценивания состоит в выполнении тестов разработчика в количестве, достаточном для подтверждения правильности результатов тестирования разработчиком. Оценщик должен определить размер выборки и тесты разработчика, которые составят данную выборку.

С учетом общих усилий оценщика по виду деятельности, связанному с тестированием, обычно следует выполнить около 20 % тестов разработчика, хотя этот процент может варьироваться в зависимости от характера ОО и представленных свидетельств тестирования.

Все тесты разработчика могут быть сопоставлены с конкретными функциями безопасности. Следовательно, факторы, которые необходимо рассмотреть при выборе тестов для включения в выборку, подобны тем, которые перечислены на шаге оценивания ATE_IND.2-4 для выбора тестируемого подмножества ФБО. Дополнительно, для выбора тестов разработчика, включаемых в выборку, оценщик может избрать метод случайной выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

11.8.4.5.2 Шаг оценивания 2:ATE_IND.2-10

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Противоречия между ожидаемыми результатами тестирования разработчиком и фактическими результатами тестирования заставляют оценщика разрешать эти несоответствия. Противоречия, с которыми столкнулся оценщик, могут быть разрешены разработчиком путем убедительного объяснения и устранения противоречий.

Если удовлетворительное объяснение или устранение противоречий не может быть достигнуто, то уверенность оценщика в результатах тестирования разработчиком может уменьшиться; у оценщика даже может возникнуть необходимость в увеличении объема выборки, чтобы восстановить уверенность в результатах тестирования разработчиком. Если увеличение объема выборки не оправдает ожиданий оценщика, может потребоваться повторение всей совокупности тестов разработчика. В конечном счете, для адекватного тестирования подмножества ФБО, идентифицированного на шаге оценивания ATE_IND.2-4, недостаточность тестов разработчика приведет к необходимости корректировки тестов разработчика или разработки оценщиком новых тестов.

11.8.4.5.3 Шаг оценивания 2:ATE_IND.2-11

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию, объем выполненного оценщиком тестирования, объем выполненного разработчиком тестирования, тестируемые конфигурации ОО и общий результат вида деятельности по тестированию.

Информация, относящаяся к усилиям оценщика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были протестированы;

b) выбранный размер подмножества. Число протестированных в течение оценки функций безопасности и логическое обоснование этого размера;

c) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

d) протестированные функции безопасности. Краткий перечень функций безопасности, обоснованно включенных в подмножество;

e) выполненные тесты разработчика. Число выполненных тестов разработчика и краткое описание критериев, использованных для выбора данных тестов;

f) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует привести в ТОО.

11.9 Вид деятельности «Оценка уязвимостей»

Вид деятельности «Оценка уязвимостей» предназначен для того, чтобы сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО. Это заключение должно быть основано на анализе, выполненном разработчиком, и поддержано тестированием проникновения, выполненным оценщиком.

11.9.1 Оценка стойкости функций безопасности ОО (AVA_SOF.1)

11.9.1.1 Цели

Цель данного подвида деятельности — сделать заключение, приведены ли в ЗБ утверждения о СФБ для всех вероятностных или перестановочных механизмов и поддержаны ли утверждения о СФБ, приведенные разработчиком в ЗБ, корректным анализом.

11.9.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) материалы анализа стойкости функций безопасности ОО.

11.9.1.3 Замечания по применению

Анализ СФБ выполняют для механизмов, которые по своей природе являются вероятностными или перестановочными, таких как механизм пароля или биометрия. Хотя криптографические механизмы также являются вероятностными и зачастую описываются в терминах стойкости, AVA_SOF.1 «Оценка стойкости функции безопасности» не применим к криптографическим механизмам. Для таких механизмов оценщику следует руководствоваться указаниями системы оценки.

Хотя анализ СФБ выполняют на базе отдельных механизмов, общее заключение о СФБ базируется на функциях. Если для обеспечения некоторой функции безопасности применяют более одного вероятностного или перестановочного механизма, проанализирован должен быть каждый отдельный механизм. Способ объединения этих механизмов для обеспечения функции безопасности определит общий уровень СФБ для этой функции. Оценщику необходима информация о проекте, чтобы понять, как механизмы работают вместе, чтобы обеспечить функцию, и минимальный уровень для такой информации предоставляют через зависимость от ADV_HLD.1 «Описательный проект верхнего уровня». Фактическая проектная информация, доступная оценщику, определяется ОУД, и эту доступную информацию, когда требуется, следует использовать для поддержки анализа, выполняемого оценщиком.

О СФБ в отношении многодоменных ОО см. в 9.3.6 «Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1).

11.9.1.4 Действие AVA_SOF.1.1E

11.9.1.4.1 Шаг оценивания 2:AVA_SOF.1-1

ИСО/МЭК 15408-3 AVA_SOF.1.1C: *Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого в ЗБ имеется утверждение о СФБ, выраженное как уровень СФБ.

Если утверждения о СФБ выражены исключительно в метрике СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Уровень СФБ выражают как базовую СФБ, среднюю СФБ или высокую СФБ, которые определены в терминах потенциала нападения, — см. ИСО/МЭК 15408-1, раздел 2. Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ как некотором уровне, который превышает общее требование СФБ.

Руководство по определению потенциала нападения, необходимого для осуществления нападения, и, следовательно, определению СФБ как некоторого уровня см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

Материалы анализа СФБ включают в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

11.9.1.4.2 Шаг оценивания 2:AVA_SOF.1-2

ИСО/МЭК 15408-3 AVA_SOF.1.2C: *Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого имеется утверждение о СФБ в ЗБ, выраженное в некоторой метрике.

Если утверждения о СФБ выражены исключительно как уровни СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ в метрике, которая удовлетворяет или превосходит общее требование СФБ.

Анализ СФБ включает в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

11.9.1.4.3 Шаг оценивания 2:AVA_SOF.1-3

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, являются ли обоснованными любые утверждения или предположения, поддерживающие анализ.

Например, может быть неверным предположение, что конкретная реализация генератора псевдослучайных чисел будет обладать энтропией, необходимой для отбора данного механизма безопасности в число тех, для которых уместен анализ СФБ.

Ожидается, что предположения, сопровождающие анализ СФБ, отражают самый плохой случай, за исключением случая, являющегося в соответствии с ЗБ несостоятельным. Когда существует ряд различных возможных сценариев, зависящих от поведения человека-пользователя или нарушителя, следует предположить сценарий, который представляет самую низкую стойкость, если этот сценарий не был признан ранее несостоятельным.

Например, утверждение о стойкости, основанное на максимальной теоретически возможной области значений пароля (т.е. комбинаций всех печатных символов ASCII), обычно не является самым плохим случаем, потому что человеку свойственно использовать пароли на естественном языке, существенно уменьшая область значений пароля и ассоциированную с ней стойкость. Однако такое предположение может быть приемлемым, если в конкретном ОО применены меры ИТ, идентифицированные в ЗБ, такие как фильтры паролей, с целью минимизировать использование паролей на естественном языке.

11.9.1.4.4 Шаг оценивания 2:AVA_SOF.1-4

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, корректны ли любые алгоритмы, принципы, характеристики и вычисления, поддерживающие анализ.

Характер данного шага оценивания сильно зависит от типа рассматриваемого механизма. В А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А) представлен пример анализа СФБ для функции идентификации и аутентификации, которая реализована с использованием механизма пароля; при анализе рассмотрена максимальная область значений пароля, чтобы, в конечном счете, прийти к некоторому уровню СФБ. Для биометрии при анализе рассматривают разрешающую способность и другие факторы, влияющие на чувствительность механизма к обману.

СФБ, выраженная как некоторый уровень, основана на минимальном потенциале нападения, требуемом, чтобы нанести поражение механизму безопасности. Уровни СФБ определены в терминах потенциала нападения в ИСО/МЭК 15408-1, раздел 2.

Руководство по определению потенциала нападения см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

11.9.1.4.5 Шаг оценивания 2:AVA_SOF.1-5

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, каждое ли утверждение о СФБ удовлетворено или превышено.

Руководство по ранжированию утверждений о СФБ см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

11.9.1.4.6 Шаг оценивания 2:AVA_SOF.1-6

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, все ли функции с заявленной СФБ удовлетворяют минимальному уровню стойкости, определенному в ЗБ.

11.9.1.5 Действие AVA_SOF.1.2E

11.9.1.5.1 Шаг оценивания 2:AVA_SOF.1-7

Оценщик должен исследовать функциональную спецификацию, проект верхнего уровня, руководство пользователя и руководство администратора, чтобы сделать заключение, для всех ли вероятностных или перестановочных механизмов имеется утверждение о СФБ.

Идентификация разработчиком функций безопасности, которые реализованы вероятностными или перестановочными механизмами, должна быть верифицирована в процессе оценки ЗБ. Однако, поскольку краткая спецификация ОО может быть единственным свидетельством, доступным при выполнении этих действий, идентификация таких механизмов может быть неполной. Дополнительные свидетельства оценки, требуемые в качестве исходных данных для этого подвида деятельности, могут идентифицировать дополнительные вероятностные или перестановочные механизмы, ранее не идентифицированные в ЗБ. Если это так, то ЗБ должно быть соответствующим образом обновлено, чтобы отразить дополнительные утверждения о СФБ, а разработчику будет необходимо представить материалы дополнительного анализа, в которых должны быть логически обоснованы утверждения о СФБ, в качестве исходных данных для действия оценщика AVA_SOF.1.1E.

11.9.1.5.2 Шаг оценивания 2:AVA_SOF.1-8

Оценщик должен исследовать утверждения о СФБ, чтобы сделать заключение, являются ли они корректными.

Если материалы анализа СФБ включают в себя утверждения или предположения (например, о возможном числе попыток аутентификации в минуту), оценщику следует независимо подтвердить, что они корректны. Это может быть достигнуто путем тестирования или независимого анализа.

11.9.2 Оценка анализа уязвимостей (AVA_VLA.1)

11.9.2.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, явные уязвимости, пригодные для использования.

11.9.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска;

g) материалы анализа уязвимостей;

h) материалы анализа утверждений о стойкости функции;

i) ОО, пригодный для тестирования.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа оценки).

11.9.2.3 Замечания по применению

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной установки, генерации и запуска.

Рассмотрение пригодных для использования уязвимостей определяется целями безопасности и функциональными требованиями в ЗБ. Например, если меры по предотвращению обхода функций безопасности не требуются в ЗБ (FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена» отсутствуют), то уязвимости, на которых базируется обход, рассматривать не следует.

Уязвимости могут быть или не быть идентифицированы в общедоступных источниках и могут требовать или не требовать навыка для их использования. Эти два фактора являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована только потому, что она идентифицирована в общедоступных источниках.

Следующие термины использованы в данном руководстве с конкретным значением:

a) уязвимость — слабость в ОО, которая может быть использована, чтобы нарушить политику безопасности в некоторой среде;

b) анализ уязвимостей — систематический поиск уязвимостей в ОО и оценка найденных уязвимостей, чтобы сделать заключение об их значимости для предопределенной среды ОО;

c) явная уязвимость — уязвимость, которая является открытой для использования, требующего минимума понимания ОО, технических познаний и ресурсов;

d) потенциальная уязвимость — уязвимость, существование которой в ОО предположено (на основании теоретически допускаемого маршрута нападения), но не подтверждено;

e) пригодная для использования уязвимость — уязвимость, которая может быть использована в предопределенной среде ОО;

f) непригодная для использования уязвимость — уязвимость, которая не может быть использована в предопределенной среде ОО;

g) остаточная уязвимость — непригодная для использования уязвимость, которая могла бы быть использована нарушителем с более высоким потенциалом нападения, чем ожидается в предопределенной среде ОО;

h) тестирование проникновения — тестирование, выполняемое с целью сделать заключение о пригодности к использованию в предопределенной среде ОО идентифицированных потенциальных уязвимостей ОО.

11.9.2.4 Действие AVA_VLA.1.1E

11.9.2.4.1 Шаг оценивания 2:AVA_VLA.1-1

ИСО/МЭК 15408-3 AVA_VLA.1.1C: *Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска явных способов, которыми пользователь может нарушить ПБО.*

ИСО/МЭК 15408-3 AVA_VLA.1.2C: *Документация анализа уязвимостей должна содержать описание решения в отношении явных уязвимостей.*

ИСО/МЭК 15408-3 AVA_VLA.1.3C: *Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.*

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, вся ли относящаяся к этому анализу информация рассмотрена при поиске явных уязвимостей.

Предполагается, что анализ уязвимостей, выполненный разработчиком, охватывает поиск разработчиком явных уязвимостей, по меньшей мере, во всех поставляемых для оценки материалах и общедоступных источниках информации. Оценщику следует использовать поставляемые для оценки материалы не для выполнения независимого анализа уязвимостей (что не требуется AVA_VLA.1 «Анализ уязвимостей разработчиком»), а как основу для оценки поиска разработчиком явных уязвимостей.

Информация в общедоступных источниках является очень динамичной. Поэтому возможно, что о новых уязвимостях будет сообщено в общедоступных источниках в период между временем, когда разработчик выполняет анализ уязвимостей, и временем завершения оценки. Моментом прекращения мониторинга информации в общедоступных источниках является выпуск органом оценки результатов оценки; поэтому за указаниями следует обращаться к органу оценки.

11.9.2.4.2 Шаг оценивания 2:AVA_VLA.1-2

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

Предполагается, что разработчик выполнил поиск явных уязвимостей, основываясь на знании ОО и информации из общедоступных источников. Требование задано только по идентификации явных уязвимостей, при этом подробный анализ не предполагается. Разработчик фильтрует эту информацию на основе вышеизложенного определения и показывает, что явные уязвимости являются непригодными для использования в предопределенной среде.

Оценщику необходимо обратить внимание на три аспекта анализа, выполненного разработчиком:

a) были ли при анализе разработчиком рассмотрены все поставляемые для оценки материалы;

b) приняты ли соответствующие меры для предотвращения использования явных уязвимостей в предопределенной среде;

c) остались ли некоторые явные уязвимости неидентифицированными.

Оценщику не следует беспокоиться, являются ли идентифицированные уязвимости явными или не являются, если это не используется разработчиком в качестве основы для заключения о непригодности уязвимостей для использования. В этом случае оценщик проверяет правильность утверждений, делая заключение о противодействии нарушителю с низким потенциалом нападения по отношению к идентифицированной уязвимости.

Понятие «явные уязвимости» не связано с понятием «потенциал нападения». Последний определяется оценщиком в ходе независимого анализа уязвимостей. Так как эти действия не выполняются для AVA_VLA.1 «Анализ уязвимостей разработчиком», то обычно поиск и фильтрация информации на основе потенциала нападения оценщиком не осуществляются. Однако оценщик может еще обнаружить потенциальные уязвимости в ходе оценки, а заключение, как их следует учитывать, сделать путем ссылки на определение явных уязвимостей и понятие низкого потенциала нападения.

Заключение, остались ли некоторые явные уязвимости неидентифицированными, ограничивается оценкой правильности анализа, выполненного разработчиком, сравнением с информацией об уязвимостях из общедоступных источников, а также сравнением с любыми последующими уязвимостями, идентифицированными оценщиком в ходе выполнения других действий по оценке.

Уязвимость считают непригодной для использования, если выполнено одно или более условие из следующих условий:

a) функции или меры безопасности в (ИТ или не-ИТ) среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными

пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования;

b) уязвимость является пригодной для использования, но только нарушителями, обладающими умеренным или высоким потенциалом нападения. Например, уязвимость распределенного ОО к нападениям, связанным с перехватом сеанса, требует потенциала нападения выше, чем необходимо для использования явной уязвимости. Такие уязвимости должны быть приведены в ТОО в качестве остаточных уязвимостей;

c) в ЗБ либо не утверждается о противостоянии определенной угрозе, либо не утверждается о следовании определенной политике безопасности организации, которая может быть нарушена. Например, для межсетевого экрана, в ЗБ которого не заявлена политика доступности и который уязвим к TCP SYN-атакам (нападение на общепринятый протокол Интернета, которое лишает хосты способности обслуживания запросов на соединение), не следует делать отрицательного заключения по данному действию оценщика только на основе одной этой уязвимости.

Руководство по определению потенциала нападения, необходимого для использования уязвимости, см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

11.9.2.4.3 Шаг оценивания 2:AVA_VLA.1-3

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, согласуются ли они с ЗБ и руководствами.

Анализ уязвимостей разработчиком может быть направлен на некоторую уязвимость с предложением конкретных конфигураций или настроек функций ОО. Если такие ограничения применения считают действенными и согласованными с ЗБ, то предполагают, что все такие конфигурации/настройки адекватно описаны в руководствах, чтобы их мог применить потребитель.

11.9.2.5 Действие AVA_VLA.1.2E

11.9.2.5.1 Шаг оценивания 2:AVA_VLA.1-4

Оценщик должен подготовить тесты проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик готовит к тестированию проникновения:

a) то, что необходимо, чтобы попытаться опровергнуть анализ разработчика в случаях, когда обоснование разработчиком непригодности уязвимости для использования является, по мнению оценщика, сомнительным;

b) то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей предопределенной среде, к явной уязвимости, не рассмотренной разработчиком. Оценщику необходимо иметь доступ к текущей информации (например, от органа оценки) о явных уязвимостях из общедоступных источников, которые могли быть не рассмотрены разработчиком; оценщик также мог идентифицировать потенциальные уязвимости в результате выполнения других действий по оценке.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, которые являются явными. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем пригодность к использованию может быть определена. Если в результате исследований в ходе оценки оценщик обнаружит некоторую уязвимость, не относящуюся к явным, то она должна быть приведена в ТОО как остаточная уязвимость.

Поняв предполагаемую явную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности, оценщик рассматривает:

a) интерфейсы функций безопасности, которые будут использованы для инициирования выполнения ФБО и наблюдения их реакции;

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости).

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использован для тестирования конкретной явной уязвимости.

11.9.2.5.2 Шаг оценивания 2:AVA_VLA.1-5

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на материалах анализа уязвимостей, выполненного разработчиком, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Тестовая документация должна включать в себя:

a) идентификацию тестируемой явной уязвимости ОО;

b) инструкции по подключению и настройке всего необходимого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и анализа, который следует проводить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО.

Цель данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

11.9.2.5.3 Шаг оценивания 2:AVA_VLA.1-6

Оценщик должен провести тестирование проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик использует документацию для тестов проникновения, подготовленных на шаге оценивания AVA_VLA.1-4, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может подготовить специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию для тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

11.9.2.5.4 Шаг оценивания 2:AVA_VLA.1-7

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общий результат должен быть идентичным. Любые различия следует логически обосновать.

11.9.2.5.5 Шаг оценивания 2:AVA_VLA.1-8

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, что ОО (в своей предопределенной среде) не имеет пригодных для использования явных уязвимостей.

Если результаты показывают, что ОО имеет явные уязвимости, пригодные для использования в его предопределенной среде, то это приводит к отрицательному вердикту по данному действию оценщика.

11.9.2.5.6 Шаг оценивания 2:AVA_VLA.1-9

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию проникновения, объем выполненного тестирования проникновения, тестируемые конфигурации ОО и общий результат действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были подвергнуты тестированию проникновения;

b) функции безопасности, подвергнутые тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

11.9.2.5.7 Шаг оценивания 2:AVA_VLA.1-10

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

a) ее источник (например, стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанную с ней функцию (функции) безопасности, недостигнутую цель (цели), нарушенную политику (политики) безопасности организации, реализованную угрозу (угрозы);

c) описание;

d) пригодна ли она для использования в предопределенной среде или нет (т.е. пригодная для использования или является остаточной уязвимостью);

e) идентификацию участника оценки (например, разработчик, оценщик), который ее идентифицировал.

12 Оценка по ОУД3

12.1 Введение

ОУД3 обеспечивает умеренный уровень доверия. Для обеспечения понимания режимов безопасного функционирования ОО функции безопасности анализируют с использованием функциональной спецификации, документации руководств и проекта верхнего уровня ОО. Данный анализ должен быть поддержан независимым тестированием подмножества функций безопасности ОО, свидетельством тестирования разработчиком, основанным на функциональной спецификации и проекте верхнего уровня, выборочным подтверждением результатов тестирования разработчиком, анализом стойкости функций безопасности и свидетельством поиска разработчиком явных уязвимостей. Дополнительно доверие достигают применением мер управления средой разработки, управления конфигурацией ОО и свидетельства безопасных процедур поставки.

12.2 Цели

Цель данного раздела заключается в определении минимальных усилий, необходимых для успешного выполнения оценки по ОУД3, и в предоставлении руководства по способам и средствам выполнения оценки.

12.3 Организация оценки по ОУД3

Оценка по ОУД3 предусматривает следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) виды деятельности по оценке по ОУД3, включающие в себя:

1) оценку ЗБ (раздел 9);

2) оценку управления конфигурацией (12.4);

3) оценку документов поставки и эксплуатации (12.5);

4) оценку документов разработки (12.6);

5) оценку руководств (12.7);

6) оценку поддержки жизненного цикла (12.8);

7) оценку тестов (12.9);

8) тестирование (12.9);

9) оценку оценки уязвимостей (12.10);

c) задачу оформления результатов оценки (раздел 7).

Виды деятельности по оценке следуют из требований доверия ОУД3, содержащихся в ИСО/МЭК 15408-3.

Оценка ЗБ начинается до выполнения любых подвидов деятельности по оценке ОО, так как ЗБ обеспечивает основание и контекст для выполнения этих подвидов деятельности.

В настоящем разделе приведено описание подвидов деятельности, выполняемых при оценке по ОУД3. Хотя выполнение подвидов деятельности может, в общем случае, начинаться более или менее случайным образом, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

12.4 Вид деятельности «Управление конфигурацией»

Цель вида деятельности «Управление конфигурацией» состоит в том, чтобы помочь потребителю в идентификации оцененного ОО и удостовериться в том, что элементы конфигурации уникально идентифицированы, а также удостовериться в адекватности процедур, используемых разработчиком для управления и отслеживания изменений, вносимых в ОО. При этом детально должно быть рассмотрено, какие изменения отслеживают и каким образом вносят потенциальные изменения.

12.4.1 Оценка возможностей УК (ACM_CAP.3)

12.4.1.1 Цели

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

12.4.1.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация управления конфигурацией.

12.4.1.3 Действие ACM_CAP.3.1E

12.4.1.3.1 Шаг оценивания 3:ACM_CAP.3-1

ИСО/МЭК 15408-3 ACM_CAP.3.1C: *Маркировка ОО должна быть уникальна для каждой версии ОО.*

Оценщик должен проверить, что версия ОО, представленная для оценки, уникально маркирована.

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

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

12.4.1.3.2 Шаг оценивания 3:ACM_CAP.3-2

ИСО/МЭК 15408-3 ACM_CAP.3.2C: *ОО должен быть помечен маркировкой.*

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

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

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО может отображать свое наименование и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем физического нанесения на нем соответствующего номера.

12.4.1.3.3 Шаг оценивания 3:ACM_CAP.3-3

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, должна быть возможность связать любое помеченное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Таким образом обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей версией руководства, необходимой для функционирования данного ОО в соответствии с его ЗБ. Оценщик может использовать список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласована с ЗБ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.4.1.3.4 Шаг оценивания 3:ACM_CAP.3-4

ИСО/МЭК 15408-3 ACM_CAP.3.3C: *Документация УК должна включать в себя список конфигурации и план УК.*

Оценщик должен проверить, что представленная документация УК включает в себя список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

12.4.1.3.5 Шаг оценивания 3:ACM_CAP.3-5

Оценщик должен проверить, что представленная документация УК содержит план УК.

12.4.1.3.6 Шаг оценивания 3:ACM_CAP.3-6

ИСО/МЭК 15408-3 ACM_CAP.3.4C: *Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен проверить, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

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

12.4.1.3.7 Шаг оценивания 3:ACM_CAP.3-7

ИСО/МЭК 15408-3 ACM_CAP.3.5C: *Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.*

Оценщик должен исследовать список конфигурации, чтобы сделать заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP «Область УК».

12.4.1.3.8 Шаг оценивания 3:ACM_CAP.3-8

ИСО/МЭК 15408-3 ACM_CAP.3.6C: *Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.*

Оценщик должен исследовать способ идентификации элементов конфигурации, чтобы сделать заключение, что он описывает, каким образом элементы конфигурации идентифицируют уникально.

12.4.1.3.9 Шаг оценивания 3:ACM_CAP.3-9

ИСО/МЭК 15408-3 ACM_CAP.3.7C: *Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен исследовать элементы конфигурации с целью сделать заключение, что способ их идентификации соответствует документации УК.

Доверие к тому, что система УК однозначно идентифицирует все элементы конфигурации, должно быть достигнуто путем изучения идентификаторов элементов конфигурации. Как для элементов конфигурации, которые составляют ОО, так и для проектов элементов конфигурации, которые представлены разработчиком в качестве свидетельств оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором в соответствии с методом уникальной идентификации, описанным в документации УК.

12.4.1.3.10 Шаг оценивания 3:ACM_CAP.3-10

ИСО/МЭК 15408-3 ACM_CAP.3.8C: *План УК должен содержать описание, как используется система УК.*

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

Описания, содержащиеся в плане УК, могут включать в себя:

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

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

c) процедуры, используемые для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

d) процедуры, используемые для исключения проблем параллелизма, возникающих в результате одновременных изменений элементов конфигурации;

e) свидетельство, генерируемое в результате применения процедур. Например, при изменении элемента конфигурации система УК могла бы зафиксировать описание изменения, ответственность за изменение, идентификацию всех затронутых элементов конфигурации, статус изменения (например, «не завершено» или «завершено»), а также дату и время внесения изменения. Эта информация могла бы быть внесена в журнал аудита проведенных изменений или в протокол контроля изменений;

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

12.4.1.3.11 Шаг оценивания 3:ACM_CAP.3-11

ИСО/МЭК 15408-3 ACM_CAP.3.9C: *Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.*

Оценщик должен проверить документацию УК, чтобы удостовериться, что она включает в себя записи системы УК, определенные планом УК.

Выходные материалы системы УК должны обеспечивать свидетельство, позволяющее оценщику быть уверенным, что план УК применяется, а все элементы конфигурации поддерживаются системой УК, как это требуется в ACM_CAP.3.10C. Пример выходных материалов мог бы включать в себя формы контроля изменений или формы разрешения доступа к элементам конфигурации.

12.4.1.3.12 Шаг оценивания 3:ACM_CAP.3-12

Оценщик должен исследовать свидетельство, чтобы сделать заключение, что система УК используется в соответствии с планом УК.

Оценщику необходимо осуществить и исследовать выборку из свидетельства, охватывающую каждый тип операций под УК, выполняемых на элементах конфигурации (например, создание, модификация, удаление, возврат к более ранней версии), с целью подтвердить, что все операции системы УК выполнены в соответствии с задокументированными процедурами. Оценщик подтверждает, что свидетельство включает в себя всю информацию, идентифицированную для этой операции в плане УК. При исследовании свидетельства может потребоваться доступ к используемым инструментальным средствам УК. Оценщику разрешается остановиться на выборочной проверке свидетельства.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Дополнительная уверенность в правильном функционировании системы УК и эффективном сопровождении элементов конфигурации может быть получена проведением интервью с отобранными для этого участниками разработки. При проведении подобных интервью оценщику следует стремиться более глубоко понять практическое применение системы УК, а также убедиться, что процедуры УК применяются в соответствии с документацией УК. Однако такие интервью следует проводить скорее в дополнение, а не вместо изучения документального свидетельства; при этом они могут и не потребоваться, если документальное свидетельство полностью удовлетворяет требованиям. Тем не менее, учитывая широкую область применения плана УК, возможно, что некоторые аспекты (например, роли и обязанности) могут быть непонятны из одного только плана и протоколов УК. Это один из случаев, когда для дополнительного разъяснения понадобится интервью.

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

12.4.1.3.13 Шаг оценивания 3:ACM_CAP.3-13

ИСО/МЭК 15408-3 ACM_CAP.3.10C: *Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.*

Оценщик должен проверить, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

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

Руководства по выборке см. в А.2 «Выборка» (приложение А).

12.4.1.3.14 Шаг оценивания 3:ACM_CAP.3-14

ИСО/МЭК 15408-3 ACM_CAP.3.11C: *Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.*

Оценщик должен исследовать меры контроля доступа в УК, описанные в плане УК, чтобы сделать заключение об их эффективности по предотвращению несанкционированного доступа к элементам конфигурации.

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

12.4.2 Оценка области УК (ACM_SCP.1)

12.4.2.1 Цели

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

12.4.2.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является список элементов конфигурации.

12.4.2.3 Действие ACM_SCP.1.1E

12.4.2.3.1 Шаг оценивания 3:ACM_SCP.1-1

ИСО/МЭК 15408-3 ACM_SCP.1.1C: *Список элементов конфигурации должен включать следующее: представление реализации и свидетельства оценки, требуемые компонентами доверия из ЗБ.*

Оценщик должен проверить, что список элементов конфигурации содержит совокупность элементов, требуемую ИСО/МЭК 15408.

Как минимум, список должен содержать следующее:

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

b) свидетельства оценки, требуемые компонентами доверия в ЗБ.

12.5 Вид деятельности «Поставка и эксплуатация»

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

12.5.1 Оценка поставки (ADO_DEL.1)

12.5.1.1 Цели

Цель данного подвида деятельности — сделать заключение, описаны ли в документации поставки все процедуры, применяемые для поддержания безопасности ОО при его распространении по объектам использования.

12.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация поставки.

12.5.1.3 Действие ADO_DEL.1.1E

12.5.1.3.1 Шаг оценивания 3:ADO_DEL.1-1

ИСО/МЭК 15408-3 ADO_DEL.1.1C: *Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.*

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

При интерпретации термина «необходимые» требуется учитывать природу ОО и информацию, содержащуюся в ЗБ. Уровень предоставляемой защиты должен быть соразмерен с предположениями, угрозами, политикой безопасности организации и целями безопасности, идентифицированными в ЗБ. В некоторых случаях они могут не быть явно выражены по отношению к поставке. Оценщику следует сделать заключе-

ние о сбалансированности выбранного подхода, при котором поставка не является очевидно слабым звеном по отношению к безопасному в остальном процессу разработки.

В документации поставки должны быть описаны надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки. В этих процедурах должно быть описано, какие части ОО должны быть охвачены подобными процедурами. В документации поставки должны быть приведены процедуры как для распространения физических копий, так и распространения в электронном виде (например, через Интернет), где это применимо. Процедуры поставки относятся к ОО в целом, включая применяемое программное обеспечение, аппаратные средства, программно-аппаратные средства и документацию.

Акцент в документации поставки, вероятно, будет сделан на мерах, связанных с целостностью, поскольку для поддержки целостности ОО в процессе его поставки требуется применение технических мер. Однако при поставке некоторых ОО должны быть обеспечены конфиденциальность и доступность; процедуры, относящиеся к этим аспектам безопасной поставки, должны также быть рассмотрены в документации.

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

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

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

12.5.1.4 Подразумеваемое действие оценщика

12.5.1.4.1 Шаг оценивания 3:ADO_DEL.1-2

ИСО/МЭК 15408-3 ADO_DEL.1.2D: *Разработчик должен использовать процедуры поставки.*

Оценщик должен исследовать процедуры процесса поставки, чтобы сделать заключение о применении этих процедур.

Подход, предпринятый оценщиком для проверки применения процедур поставки, будет зависеть от природы ОО и самого процесса поставки. В дополнение к исследованию собственно процедур оценщику необходимо получить и определенную уверенность в их действительном применении. Некоторые возможные подходы перечислены ниже.

a) Посещение объекта (объектов) распространения, где можно наблюдать практическое применение процедур.

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

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

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

Для только что разработанного ОО возможно, что процедуры поставки еще необходимо отработать. В подобных случаях оценщику придется удовлетвориться тем, что имеются соответствующие процедуры и средства выполнения предстоящих поставок и что весь привлекаемый персонал знает свои обязанности. Оценщик может запросить «пробный прогон» поставки, если это практически осуществимо. Если разработчик производит другие подобные продукты, то для приобретения доверия может быть полезно исследование процедур при их применении.

12.5.2 Оценка установки, генерации и запуска (ADO_IGS.1)

12.5.2.1 Цели

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

12.5.2.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) руководство администратора;

b) процедуры безопасной установки, генерации и запуска;

c) ОО, пригодный для тестирования.

12.5.2.3 Замечания по применению

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

12.5.2.4 Действие ADO_IGS.1.1E

12.5.2.4.1 Шаг оценивания 3:ADO_IGS.1-1

ИСО/МЭК 15408-3 ADO_IGS.1.1C: *Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.*

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

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, если ОО поставлен в рабочем состоянии), то данный шаг оценивания (или отдельные его части) не применяют и поэтому считают удовлетворенным.

12.5.2.5 Действие ADO_IGS.1.2E

12.5.2.5.1 Шаг оценивания 3:ADO_IGS.1-2

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

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

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

a) изменения задаваемых при инсталляции характеристик безопасности сущностей, находящихся под управлением ФБО;

b) обработки исключительных ситуаций и проблем;

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

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

12.6 Вид деятельности «Разработка»

Вид деятельности «Разработка» предназначен для оценки проектной документации на предмет ее достаточности для понимания того, каким образом ФБО предоставляют функции безопасности ОО. Это понимание должно быть достигнуто путем экспертизы все более уточненных описаний в проектной документации ФБО. Проектная документация состоит из функциональной спецификации (которая описывает внешние интерфейсы ОО) и проекта верхнего уровня (который описывает архитектуру ОО в терминах внутренних подсистем). Имеется также описание соответствия представлений (которое отображает представления ОО друг на друга, чтобы продемонстрировать их согласованность).

12.6.1 Замечания по применению

Требования ИСО/МЭК 15408 к проектной документации ранжированы по уровню формализации. В ИСО/МЭК 15408 рассмотрены следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ — это документ, который составлен на естественном языке. Методология не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки. Ниже дифференцировано содержание различных неформальных документов.

Неформальная функциональная спецификация включает в себя описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых интерфейсов ФБО. Например, если операционная система предоставляет пользователю средства идентификации пользователя, создания, модификации или удаления файлов, установления разрешения другим пользователям на доступ к файлам и взаимодействия с удаленными машинами, то ее функциональная спецификация, как правило, содержит описание каждой из этих функций. Если имеются также функции аудита,

связанные с обнаружением и регистрацией таких событий, то описание указанных функций аудита также обычно включают в состав функциональной спецификации; и хотя пользователь формально не обращается к этим функциям непосредственно через внешний интерфейс, на них определенно влияет все то, что происходит на уровне внешнего пользовательского интерфейса.

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

Необязательно, чтобы неформальная демонстрация соответствия была в повествовательной форме; может быть достаточно простого двухмерного отображения (например, в виде таблицы).

12.6.2 Оценка функциональной спецификации (ADV_FSP.1)

12.6.2.1 Цели

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

12.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора.

12.6.2.3 Действие ADV_FSP.1.1E

12.6.2.3.1 Шаг оценивания 3:ADV_FSP.1-1

ИСО/МЭК 15408-3 ADV_FSP.1.1C: *Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.*

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

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

12.6.2.3.2 Шаг оценивания 3:ADV_FSP.1-2

ИСО/МЭК 15408-3 ADV_FSP.1.2C: *Функциональная спецификация должна быть внутренне непротиворечивой.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о ее внутренней непротиворечивости.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.6.2.3.3 Шаг оценивания 3:ADV_FSP.1-3

ИСО/МЭК 15408-3 ADV_FSP.1.3C: *Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

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

Термин «внешний» относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО — это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы возможен доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 9 показан ОО, включающий в себя ФБО-части (заштрихованы) и не-ФБО-части (не заштрихо-

ваны). Данный ОО имеет три внешних интерфейса: интерфейс **c** — непосредственный интерфейс ФБО; интерфейс **b** — косвенный интерфейс ФБО; интерфейс **a** — интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы **b** и **c** составляют ИФБО.

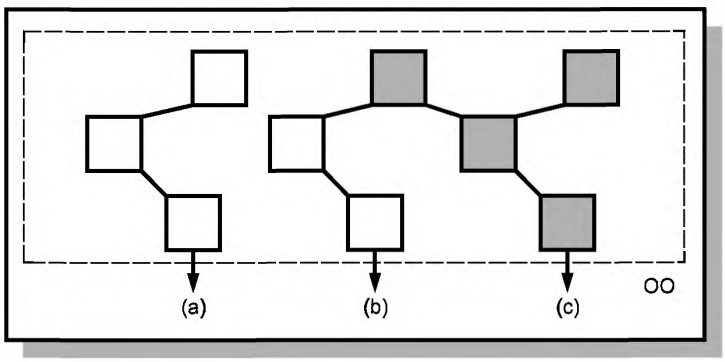


Рисунок 9 — Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях из ИСО/МЭК 15408-2 (или в компонентах, дополнительных по отношению к ИСО/МЭК 15408-2), будут иметь своего рода внешне видимые проявления. И хотя не обязательно все из них являются интерфейсами, через которые могут быть протестированы функции безопасности, все они до некоторой степени являются внешне видимыми, а поэтому должны быть включены в функциональную спецификацию.

Руководство по определению границ ОО см. в А.6 «Границы ОО» (приложение А).

12.6.2.3.4 Шаг оценивания 3:ADV_FSP.1-4

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

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

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е. в его ЗБ включены компоненты требований из семейств FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена»), то в функциональной спецификации должны быть описаны все внешние интерфейсы, но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е. интерфейсы **b** и **c** на рисунке 9) должны быть описаны полностью, в то время как другие интерфейсы описывают только в объеме, достаточном для понимания того, что ФБО являются недоступными через рассматриваемый интерфейс (т.е. что интерфейс относится к типу **a**, а не типу **b** на рисунке 9). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс — это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, запрашиваются программой, у которой есть соответствующие привилегии. Все программы, выполняемые в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру и выполняемые в непривилегированном режиме, не способны влиять на ПБО (т.е. такие программы являются интерфейсами типа **a**, а не **b** на

рисунке 9), а следовательно, могут не быть включены в функциональную спецификацию. Несмотря на то, что архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

12.6.2.3.5 Шаг оценивания 3:ADV_FSP.1-5

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

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

a) все ли относящиеся к безопасности, вводимые пользователем параметры (или характеристики этих параметров) определены. Для полноты необходимо, чтобы были определены параметры, которыми пользователь не управляет непосредственно, если они могут быть использованы администраторами;

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

c) все ли интерфейсы описаны для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса необходимо пояснение режимов его функционирования при наличии или отсутствии привилегии;

d) вся ли информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса непротиворечивы во всей документации.

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

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

12.6.2.3.6 Шаг оценивания 3:ADV_FSP.1-6

ИСО/МЭК 15408-3 ADV_FSP.1.4C: *Функциональная спецификация должна полностью представить ФБО.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни в одном из этих документов не должны быть описаны функции безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

12.6.2.4 Действие ADV_FSP.1.2E

12.6.2.4.1 Шаг оценивания 3:ADV_FSP.1-7

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением функциональных требований безопасности ОО.

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

12.6.2.4.2 Шаг оценивания 3:ADV_FSP.1-8

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

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

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

12.6.3 Оценка проекта верхнего уровня (ADV_HLD.2)

12.6.3.1 Цели

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

12.6.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня.

12.6.3.3 Действие ADV_HLD.2.1E

12.6.3.3.1 Шаг оценивания 3:ADV_HLD.2-1

ИСО/МЭК 15408-3 ADV_HLD.2.1C: *Представление проекта верхнего уровня должно быть неформальным.*

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

Если весь проект верхнего уровня является неформальным, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

12.6.3.3.2 Шаг оценивания 3:ADV_HLD.2-2

ИСО/МЭК 15408-3 ADV_HLD.2.2C: *Проект верхнего уровня должен быть внутренне непротиворечивым.*

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

12.6.3.3.3 Шаг оценивания 3:ADV_HLD.2-3

ИСО/МЭК 15408-3 ADV_HLD.2.3C: *Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.*

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах подсистем.

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

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

Подсистемы, используемые для описания проекта верхнего уровня, не обязательно называются «подсистемами», но необходимо, чтобы они представляли собой подобный уровень декомпозиции. Например, при декомпозиции проекта могут быть использованы понятия «слои» или «менеджеры».

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

12.6.3.3.4 Шаг оценивания 3:ADV_HLD.2-4

ИСО/МЭК 15408-3 ADV_HLD.2.4C: *Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.*

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

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

12.6.3.3.5 Шаг оценивания 3:ADV_HLD.2-5

ИСО/МЭК 15408-3 ADV_HLD.2.5C: *Проект верхнего уровня должен идентифицировать любые базовые аппаратные, программно-аппаратные и/или программные средства, требуемые ФБО, с представлением функций, обеспечиваемых поддерживающими механизмами защиты, реализованными в этих аппаратных, программно-аппаратных и/или программных средствах.*

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

Если проект верхнего уровня содержит требования безопасности для среды ИТ, которые не включены в ЗБ, или если они отличаются от требований, включенных в ЗБ, такая несогласованность должна быть учтена оценщиком при выполнении действия ADV_HLD.2.2E.

12.6.3.3.6 Шаг оценивания 3:ADV_HLD.2-6

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

Представление функций, предоставляемых базовой абстрактной машиной, на базе которой функционирует ОО, не обязательно необходимо на том же уровне детализации, что и представление функций,

являющихся частью ФБО. В представлении должно быть пояснено, каким образом ОО использует функции, предоставленные для поддержки целей безопасности для ОО аппаратными, программно-аппаратными и программными средствами, реализующими требования безопасности для среды ИТ, от которой зависит ОО.

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

12.6.3.3.7 Шаг оценивания 3:ADV_HLD.2-7

ИСО/МЭК 15408-3 ADV_HLD.2.6C: *Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.*

Оценщик должен проверить, идентифицированы ли в проекте верхнего уровня интерфейсы подсистем ФБО.

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

12.6.3.3.8 Шаг оценивания 3:ADV_HLD.2-8

ИСО/МЭК 15408-3 ADV_HLD.2.7C: *Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.*

Оценщик должен проверить, идентифицировано ли в проекте верхнего уровня, какие интерфейсы подсистем ФБО являются внешне видимыми.

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

12.6.3.3.9 Шаг оценивания 3:ADV_HLD.2-9

ИСО/МЭК 15408-3 ADV_HLD.2.8C: *Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, содержится ли в нем описание назначения и методов использования всех интерфейсов каждой подсистемы, и дается ли, при необходимости, подробное описание результатов, нештатных ситуаций и сообщений об ошибках.

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

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

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

12.6.3.3.10 Шаг оценивания 3:ADV_HLD.2-10

ИСО/МЭК 15408-3 ADV_HLD.2.9C: *Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.*

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

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

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

12.6.3.4 Действие ADV_HLD.2.2E

12.6.3.4.1 Шаг оценивания 3:ADV_HLD.2-11

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, является ли он точным отображением функциональных требований безопасности ОО.

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

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

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

12.6.3.4.2 Шаг оценивания 3:ADV_HLD.2-12

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

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

12.6.4 Оценка соответствия представлений (ADV_RCR.1)

12.6.4.1 Цели

Цель данного подвида деятельности — сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ и функциональной спецификации в проекте верхнего уровня.

12.6.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией;

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

12.6.4.3 Действие ADV_RCR.1.1E

12.6.4.3.1 Шаг оценивания 3:ADV_RCR.1-1

ИСО/МЭК 15408-3 ADV_RCR.1.1C: *Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного пред-*

ставления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

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

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

Оценщик анализирует соответствие между функциями безопасности ОО в краткой спецификации ОО и в функциональной спецификации. Оценщик проверяет непротиворечивость и точность данного соответствия. Там, где материалы анализа соответствия указывают на связь между описанием функции безопасности в краткой спецификации ОО и описанием интерфейса в функциональной спецификации, оценщик верифицирует, что описанные функциональные возможности безопасности являются одними и теми же. Если функции безопасности, описанные в краткой спецификации ОО, точно и полно представлены в описаниях соответствующих интерфейсов, рассматриваемый шаг оценивания считают выполненным.

Данный шаг оценивания может быть выполнен совместно с шагами оценивания ADV_FSP.1-7 и ADV_FSP.1-8.

12.6.4.3.2 Шаг оценивания 3:ADV_RCR.1-2

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

Оценщик использует материалы анализа соответствия, функциональную спецификацию и проект верхнего уровня, чтобы удостовериться в возможности отобразить каждую функцию безопасности, идентифицированную в функциональной спецификации, на какую-либо подсистему ФБО, описанную в проекте верхнего уровня. Для каждой функции безопасности материалы соответствия указывают, какие подсистемы ФБО предполагают поддержку данной функции безопасности. Оценщик верифицирует, что проект верхнего уровня содержит описание корректной реализации каждой функции безопасности.

12.7 Вид деятельности «Руководства»

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

12.7.1 Замечания по применению

Вид деятельности «Руководства» применяют к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО должна быть описана в ЗБ.

12.7.2 Оценка руководства администратора (AGD_ADM.1)

12.7.2.1 Цели

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

12.7.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска;

g) документация определения жизненного цикла.

12.7.2.3 Замечания по применению

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

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

12.7.2.4 Действие AGD_ADM.1.1E

12.7.2.4.1 Шаг оценивания 3:AGD_ADM.1-1

ИСО/МЭК 15408-3 AGD_ADM.1.1C: *Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описаны ли в нем относящиеся к администрированию функции безопасности и интерфейсы, доступные администратору ОО.

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

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

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

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

b) параметры, устанавливаемые администратором, их допустимые значения и значения по умолчанию;

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

12.7.2.4.2 Шаг оценивания 3:AGD_ADM.1-2

ИСО/МЭК 15408-3 AGD_ADM.1.2C: *Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описан ли в нем безопасный способ администрирования ОО.

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

12.7.2.4.3 Шаг оценивания 3:AGD_ADM.1-3

ИСО/МЭК 15408-3 AGD_ADM.1.3C: *Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, содержит ли оно предупреждения относительно функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

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

12.7.2.4.4 Шаг оценивания 3:AGD_ADM.1-4

ИСО/МЭК 15408-3 AGD_ADM.1.4C: *Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство администратора должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

12.7.2.4.5 Шаг оценивания 3:AGD_ADM.1-5

ИСО/МЭК 15408-3 AGD_ADM.1.5C: *Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.*

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

Для каждого параметра безопасности в руководстве администратора должны быть описаны предназначение параметра, допустимые значения параметра и его значение по умолчанию, а также безопасные и небезопасные настройки этих параметров как по отдельности, так и в сочетании.

12.7.2.4.6 Шаг оценивания 3:AGD_ADM.1-6

ИСО/МЭК 15408-3 AGD_ADM.1.6C: *Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.*

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

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

12.7.2.4.7 Шаг оценивания 3:AGD_ADM.1-7

ИСО/МЭК 15408-3 AGD_ADM.1.7C: *Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.7.2.4.8 Шаг оценивания 3:AGD_ADM.1-8

ИСО/МЭК 15408-3 AGD_ADM.1.8C: *Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

12.7.3 Оценка руководства пользователя (AGD_USR.1)

12.7.3.1 Цели

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

12.7.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска.

12.7.3.3 Замечания по применению

В ЗБ могут быть определены несколько различных ролей или групп пользователей, опознаваемых объектом оценки и взаимодействующих с ФБО. Возможности этих ролей и связанные с ними привилегии описывают в ЗБ в классе FMT «Управление безопасностью». Различные роли и группы пользователей должны быть рассмотрены в руководстве пользователя.

12.7.3.4 Действие AGD_USR.1.1E

12.7.3.4.1 Шаг оценивания 3:AGD_USR.1-1

ИСО/МЭК 15408-3 AGD_USR.1.1C: *Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.*

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

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

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

12.7.3.4.2 Шаг оценивания 3:AGD_USR.1-2

ИСО/МЭК 15408-3 AGD_USR.1.2C: *Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.*

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

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

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

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

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

b) параметры, устанавливаемые пользователем, их допустимые значения и значения по умолчанию;

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

12.7.3.4.3 Шаг оценивания 3:AGD_USR.1-3

ИСО/МЭК 15408-3 AGD_USR.1.3C: *Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство пользователя, чтобы сделать заключение, содержит ли оно предупреждения относительно доступных пользователю функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

В руководстве пользователя должны быть идентифицированы функции и привилегии, которые могут быть применены, требуемые для них типы команд и объяснения таких команд. В руководстве пользователя должны быть приведены предупреждающие сообщения относительно использования функций и привилегий, подлежащих контролю. Предупреждающие сообщения должны быть связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

12.7.3.4.4 Шаг оценивания 3:AGD_USR.1-4

ИСО/МЭК 15408-3 AGD_USR.1.4C: *Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство пользователя должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

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

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

12.7.3.4.5 Шаг оценивания 3:AGD_USR.1-5

ИСО/МЭК 15408-3 AGD_USR.1.5C: *Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.7.3.4.6 Шаг оценивания 3:AGD_USR.1-6

ИСО/МЭК 15408-3 AGD_USR.1.6C: *Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

12.8 Вид деятельности «Поддержка жизненного цикла»

Вид деятельности «Поддержка жизненного цикла» предназначен для определения достаточности процедур, применяемых разработчиком во время разработки и сопровождения ОО. Такие процедуры предназначены для защиты ОО и связанной с ним информации о проекте от вмешательства или раскрытия. Вмешательство в процесс разработки может позволить преднамеренно внести уязвимости в ОО. Раскрытие информации о проекте может облегчить использование уязвимостей. Адекватность рассматриваемых процедур будет зависеть от свойств ОО и процесса его разработки.

12.8.1 Оценка безопасности разработки (ALC_DVS.1)

12.8.1.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли меры и средства контроля безопасности в среде разработки достаточными для обеспечения конфиденциальности и целостности проекта и реализации ОО. Это необходимо для обеспечения того, чтобы безопасная эксплуатация ОО не была скомпрометирована.

12.8.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация по безопасности разработки.

Кроме того, оценщику может понадобиться исследование других поставок, чтобы сделать заключение о том, что меры и средства контроля безопасности полностью определены и их применяют. В частности, оценщику может понадобиться исследование документации разработчика по управлению конфигурацией (исходные данные подвидов деятельности ACM_CAP.4 «Поддержка генерации, процедуры приемки» и ACM_SCP.2 «Охват УК отслеживания проблем»). Также требуется свидетельство применения процедур.

12.8.1.3 Действие ALC_DVS.1.1E

12.8.1.3.1 Шаг оценивания 3:ALC_DVS.1-1

ИСО/МЭК 15408-3 ALC_DVS.1.1C: *Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.*

Оценщик должен исследовать документацию по безопасности разработки, чтобы сделать заключение, содержит ли она подробное описание всех используемых в среде разработки мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта и реализации ОО.

Оценщик определяет, какая информация из ЗБ требуется в первую очередь при вынесении заключения о необходимой защите, особенно из разделов ЗБ об угрозах, политике безопасности организации и предположениях, хотя такая информация может и не быть представлена в явном виде. Изложение в ЗБ целей безопасности для среды также может быть полезно в этом отношении.

Если в ЗБ не имеется такой информации в явном виде, оценщик должен принять решение о необходимых мерах, основываясь на рассмотрении предполагаемой среды для ОО. В тех случаях, когда меры разработчика признаны недостаточными, необходимо, чтобы было представлено четкое и логическое обоснование для оценки уязвимостей, потенциально пригодных для использования.

При исследовании документации оценщик рассматривает следующие типы мер безопасности:

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

b) процедурные, например распространяющиеся:

- на предоставление доступа к среде разработки или к конкретным объектам среды, таким как оборудование разработки,
- на отмену прав доступа лиц при их исключении из состава разработчиков,
- на передачу защищаемого материала из среды разработки,
- на встречу и сопровождение посетителей среды разработки,
- на роли и обязанности по обеспечению непрерывного применения мер безопасности и обнаружения нарушений безопасности;

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

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

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

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

12.8.1.3.2 Шаг оценивания 3:ALC_DVS.1-2

Оценщик должен исследовать политики обеспечения конфиденциальности и целостности при разработке, чтобы сделать заключение о достаточности применяемых мер безопасности.

При рассмотрении политик учитывают следующее:

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

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

Оценщику следует сделать заключение, описаны ли эти политики в документации по безопасности разработки, совместимы ли применяемые меры безопасности с политиками, являются ли они достаточно полными.

Необходимо отметить, что процедуры управления конфигурацией способствуют защите целостности ОО, и оценщику следует избегать частичного перекрытия с шагами оценивания, проводимыми в рамках подвида деятельности ACM_CAP «Возможности УК». Например, документация УК может описывать процедуры безопасности, необходимые для контроля ролей или лиц, которым следует предоставить доступ к среде разработки и которые могут модифицировать ОО.

Тогда как требования ACM_CAP зафиксированы, требования для ALC_DVS «Безопасность разработки», предписывающие только необходимые меры, зависят от типа ОО и от информации, которая может быть представлена в разделе ЗБ «Среда безопасности». Например, ЗБ может идентифицировать политику безопасности организации, в которой требуется наличие формы допуска у персонала разработчиков ОО. Тогда оценщику в ходе выполнения данного подвида деятельности необходимо сделать заключение, была ли применена такая политика.

12.8.1.3.3 Шаг оценивания 3:ALC_DVS.1-3

ИСО/МЭК 15408-3 ALC_DVS.1.2C: *Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.*

Оценщик должен проверить документацию по безопасности разработки, чтобы сделать заключение, формируют ли документальное свидетельство в результате применения процедур.

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

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.8.1.4 Действие ALC_DVS.1.2E

12.8.1.4.1 Шаг оценивания 3:ALC_DVS.1-4

Оценщик должен исследовать документацию по безопасности разработки и связанные с ней свидетельства, чтобы сделать заключение, применены ли меры безопасности.

На этом шаге оценивания от оценщика требуется сделать заключение, применены ли меры безопасности, описанные в документации по безопасности разработки, таким образом, при котором целостность ОО и конфиденциальность связанной с ним документации адекватно защищены. Например, данное заключение могло бы быть сделано по результатам исследования представленных документальных свидетельств. Документальные свидетельства следует дополнить непосредственным ознакомлением со средой разработки. Непосредственное ознакомление со средой разработки предоставит оценщику возможность:

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

b) исследовать документальные свидетельства применения процедур;

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

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

12.9 Вид деятельности «Тестирование»

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

12.9.1 Замечания по применению

Объем и состав подмножества тестов оценщика зависят от нескольких факторов, рассматриваемых в подвидах деятельности, связанных с независимым тестированием (ATE_IND.2 «Выборочное независимое тестирование»). Один из таких факторов, оказывающих влияние на состав подмножества тестов, — это известные из общедоступных источников слабые места, к информации о которых оценщику необходимо получить доступ (например, в рамках системы оценки).

В ИСО/МЭК 15408 для повышения гибкости применения компонентов семейств вопросы покрытия тестами и глубины тестирования рассмотрены отдельно от функциональных тестов. Тем не менее, требования соответствующих семейств предназначены для совместного применения в целях подтверждения, что ФБО выполняются согласно их спецификации. Такая тесная связь семейств привела к некоторому дублированию работы оценщика по подвидам деятельности. Настоящие замечания по применению позволяют минимизировать повторения текста при описании подвидов деятельности одного и того же вида деятельности и ОУД.

12.9.1.1 Понимание ожидаемого режима функционирования ОО

Прежде чем адекватность тестовой документации может быть надлежащим образом оценена и прежде чем могут быть созданы новые тесты, оценщику необходимо понять желательный ожидаемый режим выполнения функций безопасности применительно к требованиям, которым они должны удовлетворять.

Оценщик может предпочесть анализировать функции безопасности ФБО поочередно. Для каждой функции безопасности оценщик исследует конкретное требование ЗБ и соответствующие части функциональной спецификации, проекта верхнего уровня и руководств для понимания ожидаемого режима функционирования ОО.

Понимая ожидаемый режим функционирования ОО, оценщик исследует план тестирования, чтобы определить подход к тестированию. В большинстве случаев подход к тестированию будет предусматривать инициирование выполнения некоторой функции безопасности через внешние или внутренние интерфейсы и наблюдение ее реакции. Тем не менее, в некоторых случаях функция безопасности не может быть адекватно протестирована через интерфейс (как, например, в случае с тестированием функциональных возможностей защиты остаточной информации); в подобных случаях необходимо использовать другой способ.

12.9.1.2 Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности

В тех случаях, когда практически нецелесообразно или несоразмерно осуществлять тестирование через интерфейс, в плане тестирования следует определить альтернативный подход к верификации ожидаемого режима выполнения. Сделать заключение о пригодности альтернативного подхода — обязанность оценщика. Оценивая пригодность альтернативных подходов, следует учесть, что:

a) приемлемым альтернативным подходом является анализ представления реализации для заключения, что требуемый режим функционирования будет демонстрироваться ОО. Это может означать экспертизу кода для программного ОО или, возможно, экспертизу фотошаблона (маски) микросхем для аппаратного ОО;

b) приемлемым является использование свидетельства помодульного или интегрированного тестирования разработчиком, даже если это несоизмеримо с представленными на оценку проектом нижнего уровня или реализацией. Если при верификации ожидаемого режима выполнения функции безопасности используется свидетельство помодульного или интегрированного тестирования разработчиком, следует внимательно отнестись к подтверждению того, что данное свидетельство тестирования отражает текущую реализацию ОО. Если конкретная подсистема или модули подверглись изменению после проведения тестирования, то обычно потребуется свидетельство, что изменения были отслежены и учтены в ходе анализа или проведения последующего тестирования.

Дополнительные по отношению к тестированию усилия с использованием альтернативных подходов следует предпринять только тогда, когда и разработчик, и оценщик сделают заключение, что не существует других практичных способов проведения тестирования ожидаемого режима выполнения некоторой функции безопасности. Такая альтернатива позволяет разработчику минимизировать затраты (времени и/или денег) на тестирование при описанных выше обстоятельствах; она не предназначена для того, чтобы дать оценщику большую свободу требовать произвольную дополнительную информацию относительно ОО, а также для того, чтобы заменить тестирование.

12.9.1.3 Верификация адекватности тестов

Для тестов необходимо заранее установить требуемые начальные условия их выполнения. Они могут быть определены через параметры, которые должны быть установлены, или через упорядочение тестов в тех случаях, когда завершение одного теста устанавливает необходимые предварительные условия выполнения другого теста. Оценщик должен сделать заключение о полноте предварительных условий выполнения тестов и их приемлемости с точки зрения того, что они не приведут к смещению наблюдаемых результатов тестирования по отношению к ожидаемым результатам тестирования.

Шаги тестирования и ожидаемые результаты тестирования определяют действия и параметры, относящиеся к интерфейсам, а также способ верификации ожидаемых результатов и что они собой представ-

ляют. Оценщик должен сделать заключение о согласованности шагов тестирования и ожидаемых результатов тестирования с функциональной спецификацией и проектом верхнего уровня. Тесты должны верифицировать задокументированный в этих спецификациях режим выполнения. Это означает, что для каждой характеристики режима выполнения функции безопасности, явным образом описанной в функциональной спецификации и проекте верхнего уровня, должны быть тесты и описание ожидаемых результатов тестирования, чтобы верифицировать данный режим выполнения.

Несмотря на то, что все ФБО должны быть протестированы разработчиком, исчерпывающее тестирование их интерфейсов не требуется. Основная цель данного вида деятельности состоит в том, чтобы сделать заключение о достаточности тестирования каждой функции безопасности на соответствие заявленным в функциональной спецификации и проекте верхнего уровня режимам выполнения. Процедуры тестирования обеспечат понимание того, каким образом разработчиком в ходе тестирования были опробованы функции безопасности. Оценщик будет использовать данную информацию при разработке дополнительных тестов для независимого тестирования ОО.

12.9.2 Оценка покрытия (ATE_COV.2)

12.9.2.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли тестирование (как это документально зафиксировано) достаточным, чтобы установить, что ФБО были систематическим методом протестированы на соответствие функциональной спецификации.

12.9.2.2 Исходные данные

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) материалы анализа покрытия тестами.

12.9.2.3 Действие ATE_COV.2.1E

12.9.2.3.1 Шаг оценивания 3:ATE_COV.2-1

ИСО/МЭК 15408-3 ATE_COV.2.1C: *Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.*

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение, является ли точным соответствие между тестами, идентифицированными в тестовой документации, и функциональной спецификацией.

Демонстрация соответствия может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов, достаточно наличие такого отображения. В других случаях может потребоваться некоторое обоснование (на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

На рисунке 10 отражена концептуальная структура соответствия между функциями безопасности, описанными в функциональной спецификации, и тестами, выделенными в тестовой документации для тестирования этих функций. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями тестов или общей целью выполняемого теста.

Идентификация тестов и функций безопасности, представленных в материалах анализа покрытия тестами, должна быть однозначной. Материалы анализа покрытия тестами позволят оценщику сопоставить идентифицированные тесты с тестовой документацией, а тестируемые функции безопасности — с функциональной спецификацией.

12.9.2.3.2 Шаг оценивания 3:ATE_COV.2-2

Оценщик должен исследовать план тестирования, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих замечаниях по применению:

a) «Понимание ожидаемого режима функционирования ОО»;

b) «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

12.9.2.3.3 Шаг оценивания 3:ATE_COV.2-3

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к функциональной спецификации, можно найти в замечаниях по применению «Верификация адекватности тестов».

12.9.2.3.4 Шаг оценивания 3:ATE_COV.2-4

ИСО/МЭК 15408-3 ATE_COV.2.2C: *Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.*

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение о полноте соответствия между ФБО, описанными в функциональной спецификации, и тестами, идентифицированными в тестовой документации.

Все функции безопасности и интерфейсы, которые описаны в функциональной спецификации, должны быть представлены в материалах анализа покрытия тестами и сопоставлены с тестами для утверждения о полноте, хотя исчерпывающее тестирование интерфейсов спецификации не требуется. Как показано на рисунке 10, для всех функций безопасности имеются относящиеся к ним тесты, а следовательно, в данном примере продемонстрировано полное покрытие тестами. Неполнота покрытия была бы очевидна, если бы некоторая функция безопасности была идентифицирована в материалах анализа покрытия тестами, но никакие тесты не могли быть к ней отнесены.

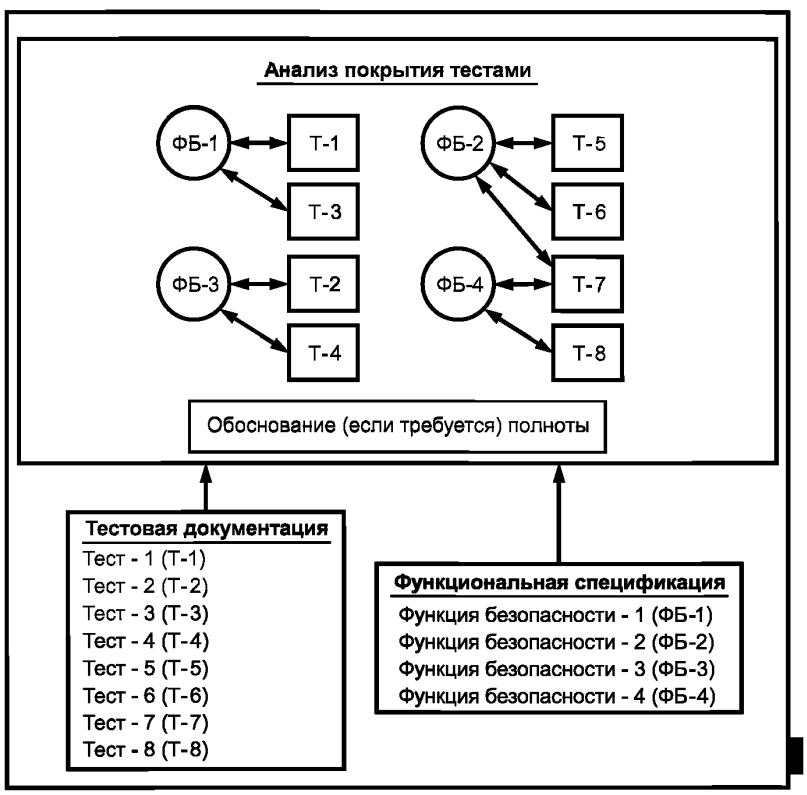


Рисунок 10 — Концептуальная структура анализа покрытия тестами

12.9.3 Оценка глубины (ATE_DPT.1)

12.9.3.1 Цели

Цель данного подвида деятельности — сделать заключение, тестировал ли разработчик ФБО на соответствие проекту верхнего уровня.

12.9.3.2 Исходные данные

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) тестовая документация;

e) материалы анализа глубины тестирования.

12.9.3.3 Действие ATE_DPT.1.1E

12.9.3.3.1 Шаг оценивания 3:ATE_DPT.1-1

ИСО/МЭК 15408-3 ATE_DPT.1.1C: *Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.*

Оценщик должен исследовать материалы анализа глубины тестирования на предмет сопоставления тестов, идентифицированных в тестовой документации, и проекта верхнего уровня.

В материалах анализа глубины тестирования должны быть идентифицированы все подсистемы, описанные в проекте верхнего уровня, и представлено сопоставление тестов с этими подсистемами. Соответствие может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов, достаточно наличия такого отображения. В других случаях может потребоваться некоторое обоснование (обычно на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

Все детали проекта, специфицированные в проекте верхнего уровня, сопоставленные с требованиями безопасности ОО и удовлетворяющие им, являются предметом тестирования, а следовательно, должны быть сопоставлены с тестовой документацией. На рисунке 11 отражена концептуальная структура сопоставления подсистем, описанных в проекте верхнего уровня, и тестов, изложенных в тестовой документации ОО и используемых для их тестирования. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями между тестами или общей целью выполняемого теста.

12.9.3.3.2 Шаг оценивания 3:ATE_DPT.1-2

Оценщик должен исследовать план тестирования разработчика, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих замечаниях по применению:

a) «Понимание ожидаемого режима функционирования ОО»;

b) «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Тестирование ФБО может быть выполнено с использованием внешних интерфейсов, внутренних интерфейсов или комбинации тех и других. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования функций безопасности. В частности, оценщик делает заключение, является ли тестирование с использованием внутренних интерфейсов функций безопасности необходимым или эти внутренние интерфейсы могут быть надлежащим образом протестированы (хотя и неявным образом) с использованием внешних интерфейсов. Это решение, как и его логическое обоснование, остается за оценщиком.

12.9.3.3.3 Шаг оценивания 3:ATE_DPT.1-3

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к проекту верхнего уровня, можно найти в замечаниях по применению «Верификация адекватности тестов».

12.9.3.3.4 Шаг оценивания 3:ATE_DPT.1-4

Оценщик должен проверить материалы анализа глубины тестирования, чтобы удостовериться, что ФБО в том виде, в котором они определены в проекте верхнего уровня, полностью сопоставлены с тестами, представленными в тестовой документации.

Материалы анализа глубины тестирования обеспечивают полное изложение соответствия между проектом верхнего уровня, планом и процедурами тестирования. Все подсистемы и внутренние интерфейсы, описанные в проекте верхнего уровня, должны быть представлены в материалах анализа глубины тестирования. Для всех подсистем и внутренних интерфейсов, представленных в материалах анализа глубины тестирования, должны иметься сопоставленные с ними тесты для того, чтобы можно было утверждать о полноте. Как показано на рисунке 11, для всех подсистем и внутренних интерфейсов имеются относящиеся к ним тесты, а следовательно, в данном примере продемонстрирована полнота глубины тестирования.

Неполнота тестирования была бы очевидна, если бы подсистема или внутренний интерфейс были идентифицированы в материалах анализа глубины тестирования, но никакие тесты не могли быть к ним отнесены.

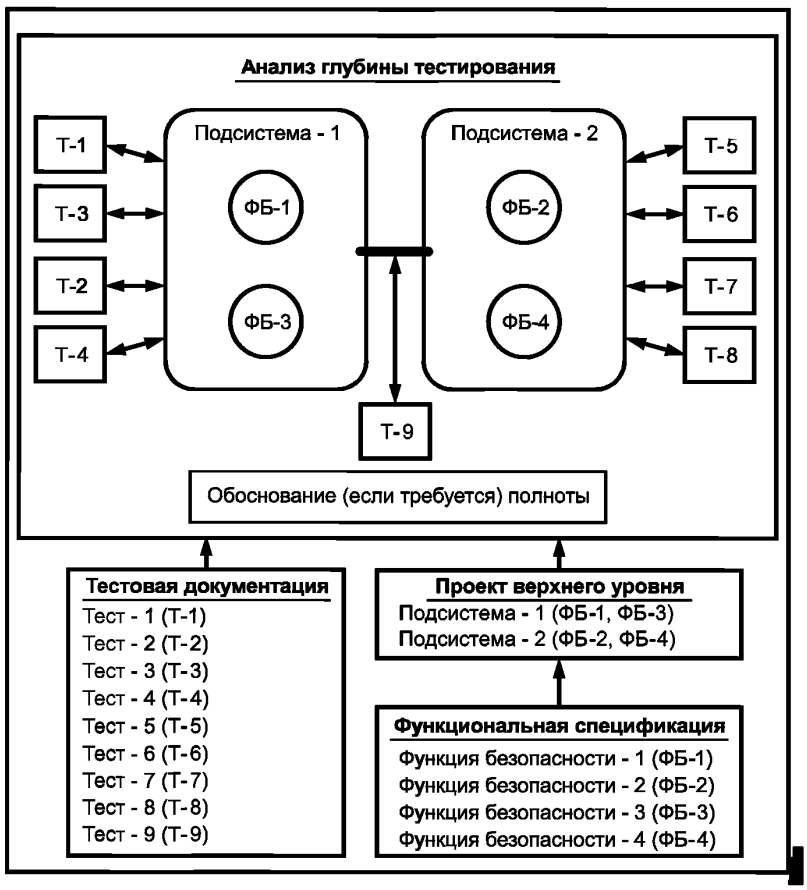


Рисунок 11 — Концептуальная структура анализа глубины тестирования

12.9.4 Оценка функциональных тестов (ATE_FUN.1)

12.9.4.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли документация функциональных тестов разработчика достаточной для демонстрации того, что функции безопасности выполняются в соответствии со спецификациями.

12.9.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) процедуры тестирования.

12.9.4.3 Замечания по применению

Степень требуемого покрытия ФБО тестовой документацией зависит от соответствующего компонента доверия, связанного с покрытием тестами.

Для представленных тестов разработчика оценщик делает заключение, являются ли тесты повторимыми, и определяет степень возможности использования тестов разработчика при проведении оценщиком независимого тестирования. Любую функцию безопасности, для которой результаты тестирования разработчиком указывают, что она может быть не выполнена в соответствии со спецификациями, оценщику сле-

дует подвергнуть независимому тестированию, чтобы сделать заключение, выполнена ли она в соответствии со спецификациями или нет.

Тестовая документация должна идентифицировать все случаи использования привилегированных режимов для установления/отмены условий тестирования для последующих тестов. Тестовая документация должна описывать, почему было необходимо использовать привилегированные режимы для достижения необходимых условий (например, для обеспечения генерации средствами тестирования определенных объектов, необходимых для выполнения некоторого теста, которые не могут быть созданы непривилегированными пользователями), а также – каким образом осуществляется выход из привилегированных режимов до проведения шагов по тестированию, демонстрирующих функциональные возможности безопасности ОО. Следовательно, несмотря на то, что тестовая конфигурация может не соответствовать описанию ОО в ЗБ, в процессе установления условий тестирования тестовая документация должна содержать описание, каким образом конфигурацию можно вернуть в состояние, которое соответствует конфигурации, описанной в ЗБ, для выполнения шагов по тестированию.

12.9.4.4 Действие ATE_FUN.1.1E

12.9.4.4.1 Шаг оценивания 3:ATE_FUN.1-1

ИСО/МЭК 15408-3 ATE_FUN.1.1C: *Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.*

Оценщик должен проверить, что тестовая документация включает в себя планы тестирования, описание процедур тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

12.9.4.4.2 Шаг оценивания 3:ATE_FUN.1-2

ИСО/МЭК 15408-3 ATE_FUN.1.2C: *Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей проводимых тестов.*

Оценщик должен проверить, что в плане тестирования идентифицированы подлежащие тестированию функции безопасности.

Одним из методов, который может быть использован для идентификации проверяемой функции безопасности, является ссылка на соответствующую часть (части) функциональной спецификации, в которой определена конкретная функция безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.3 Шаг оценивания 3:ATE_FUN.1-3

Оценщик должен исследовать план тестирования, чтобы сделать заключение, содержит ли он описание целей выполняемых тестов.

План тестирования предоставляет информацию о том, каким образом должны быть протестированы функции безопасности, а также информацию о тестируемой конфигурации ОО, используемой при проведении тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.4 Шаг оценивания 3:ATE_FUN.1-4

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласована ли тестируемая конфигурация ОО с той конфигурацией, которая идентифицирована для оценки в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ. Оценщик верифицирует, что в тестовой документации разработчика определены тестируемые конфигурации и они согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей, не относится к среде тестирования, а предположение относительно единой точки подключения к сети, относится к среде тестирования.

12.9.4.4.5 Шаг оценивания 3:ATE_FUN.1-5

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласован ли он с описанием процедур тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.9.4.4.6 Шаг оценивания 3:ATE_FUN.1-6

ИСО/МЭК 15408-3 ATE_FUN.1.3C: *Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.*

Оценщик должен проверить, что в описании процедур тестирования идентифицирован каждый из подлежащих тестированию режимов выполнения функций безопасности.

Одним из методов, который может быть использован для идентификации подлежащего тестированию режима выполнения функции безопасности, является ссылка на соответствующую часть (части) спецификации проекта, которая определяет конкретный подлежащий тестированию режим выполнения функции безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.7 Шаг оценивания 3:ATE_FUN.1-7

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции, позволяющие установить воспроизводимые начальные условия выполнения тестов, включая зависимости, связанные с порядком следования, при их наличии.

Для того чтобы установить начальные условия выполнения тестов, возможно, потребуется выполнить некоторые шаги. Например, необходимо добавить учетные записи пользователей прежде, чем их можно будет удалить. Пример зависимостей, связанных с порядком следования тестов, от результатов других тестов — необходимо тестирование функции аудита прежде, чем можно будет полагаться на нее при создании записей аудита для другого механизма безопасности, такого как управления доступом. Другой пример зависимости, связанной с порядком следования тестов, — при выполнении одного набора тестов генерируется файл данных, используемых в качестве исходных данных для другого набора тестов.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.8 Шаг оценивания 3:ATE_FUN.1-8

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции для того, чтобы иметь воспроизводимый способ инициирования выполнения функций безопасности и наблюдения за режимом их выполнения.

Инициирующее воздействие обычно обеспечивается внешним по отношению к функции безопасности способом через ИФБО. После того как входные данные (инициирующее воздействие) предоставлены ИФБО, через ИФБО можно наблюдать режим выполнения функции безопасности. Воспроизводимость не обеспечивается, если процедуры тестирования не содержат достаточных подробностей для однозначного описания инициирующего воздействия и режима выполнения, ожидаемого в результате инициирующего воздействия.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.9 Шаг оценивания 3:ATE_FUN.1-9

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение о его согласованности с процедурами тестирования.

Если описание процедур тестирования — это собственно процедуры тестирования, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.9.4.4.10 Шаг оценивания 3:ATE_FUN.1-10

ИСО/МЭК 15408-3 ATE_FUN.1.4C: *Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.*

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о достаточности включенных в нее ожидаемых результатов выполнения тестов.

Ожидаемые результаты тестирования необходимы, чтобы сделать заключение, действительно ли тест был успешно выполнен. Описание ожидаемых результатов тестирования достаточно, если оно однозначно и согласуется с ожидаемым режимом выполнения ФБО, обусловленным подходом к тестированию.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.4.4.11 Шаг оценивания 3:ATE_FUN.1-11

ИСО/МЭК 15408-3 ATE_FUN.1.5C: *Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.*

Оценщик должен проверить, что ожидаемые результаты тестирования в тестовой документации согласуются с представленными фактическими результатами тестирования.

Сравнение представленных разработчиком фактических и ожидаемых результатов тестирования выявит какие бы то ни было несоответствия результатов.

Возможно, что непосредственное сравнение фактических результатов не может быть выполнено до того, как будет выполнено некоторое преобразование или синтез данных. В подобных случаях в тестовой документации разработчика должен быть описан процесс преобразования или синтеза фактических данных.

Например, разработчику может потребоваться проверить содержимое буфера сообщений после того, как имело место сетевое соединение, чтобы определить содержимое буфера. Буфер сообщения будет содержать бинарную последовательность. Эту бинарную последовательность, как правило, преобразуют в другую форму представления данных, чтобы сделать тест более содержательным. Преобразование этого бинарного представления данных в представление более высокого уровня должно быть достаточно подробно описано разработчиком, чтобы позволить оценщику выполнить процесс преобразования (т.е. необходимо описать, используется ли синхронный или асинхронный метод передачи данных, число стоповых битов, битов четности и т.д.).

Следует отметить, что описание процесса преобразования или синтеза фактических данных оценщик использует не для того, чтобы фактически исполнить необходимую модификацию, а для того, чтобы оценить корректность этого процесса. Преобразование ожидаемых результатов тестирования в формат, позволяющий их легко сравнивать с фактическими результатами тестов, возложено на разработчика.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Если ожидаемые и фактические результаты тестирования для какого-либо из тестов не совпадают, то правильность выполнения функции безопасности не продемонстрирована. Такая ситуация окажет влияние на усилия оценщика по независимому тестированию, выражающееся в необходимости тестирования соответствующей функции безопасности. Оценщику также следует рассмотреть вопрос об увеличении выборки свидетельств, на основе которых должен быть выполнен рассматриваемый шаг оценивания.

12.9.4.4.12 Шаг оценивания 3:ATE_FUN.1-12

Оценщик должен привести в отчете информацию об усилиях разработчика по тестированию, выделив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании разработчиком, зафиксированная в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные разработчиком на тестирование ОО. Смысл предоставления данной информации состоит в том, чтобы привести краткий содержательный обзор усилий разработчика по тестированию. Не обязательно, чтобы информация о тестировании разработчиком в ТОО была точной копией конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, позволяющие другим оценщикам и сотрудникам органов оценки понять подход разработчика к тестированию, объем выполненного тестирования, тестируемые конфигурации ОО и общий результат тестирования разработчиком.

Информация об усилиях разработчика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, подвергнутые тестированию;

b) подход к тестированию. Описание общей стратегии тестирования, которую применил разработчик;

c) объем тестирования, выполненного разработчиком. Описание степени покрытия тестами и глубины тестирования разработчиком;

d) результаты тестирования. Описание общих результатов тестирования разработчиком.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, связанной с усилиями разработчика по тестированию, которую следует привести в ТОО.

12.9.5 Оценка путем независимого тестирования (ATE_IND.2)

12.9.5.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования подмножества ФБО сделать заключение, соответствуют ли спецификациям режимы функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения выборки тестов разработчика.

12.9.5.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска;

f) тестовая документация;

g) материалы анализа покрытия тестами;

h) материалы анализа глубины тестирования;

i) ОО, пригодный для тестирования.

12.9.5.3 Действие ATE_IND.2.1E

12.9.5.3.1 Шаг оценивания 3:ATE_IND.2-1

ИСО/МЭК 15408-3 ATE_IND.2.1C: *ОО должен быть пригоден для тестирования.*

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено более одной подлежащей оценке конфигурации. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

При использовании любых средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

12.9.5.3.2 Шаг оценивания 3:ATE_IND.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности ADO_IGS.1 «Процедуры установки, генерации и запуска» позволит считать выполненным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику необходимо выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания ADO_IGS.1-2.

12.9.5.3.3 Шаг оценивания 3:ATE_IND.2-3

ИСО/МЭК 15408-3 ATE_IND.2.2C: *Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.*

Оценщик должен исследовать набор ресурсов, предоставленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, использованных разработчиком для функционального тестирования ФБО.

Данный набор ресурсов может, кроме всего прочего, включать в себя доступное лабораториям и специальное испытательное оборудование. Ресурсы, которые не являются идентичными ресурсам, ис-

пользованным разработчиком, должны быть эквивалентны им с точки зрения любого влияния, которое они могут оказать на результаты тестирования.

12.9.5.4 Действие ATE_IND.2.2E

12.9.5.4.1 Шаг оценивания 3:ATE_IND.2-4

Оценщик должен определить тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, приемлемую для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмножества ФБО, содержащего как можно большее число функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое число функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, стратегия тестирования, принятая оценщиком, должна находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику необходимо рассмотреть следующие факторы:

a) свидетельства тестирования разработчиком. Свидетельства тестирования разработчиком включают в себя: анализ покрытия тестами, анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком будут обеспечивать понимание того, каким образом разработчиком в ходе тестирования были проверены функции безопасности. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует, в особенности, рассмотреть:

1) усиление тестирования, выполненного разработчиком, для определенной функции (функций) безопасности. Оценщик может выполнить большее число тестов того же самого типа, чтобы путем изменения параметров более строго протестировать функцию безопасности;

2) дополнение стратегии тестирования, примененной разработчиком, для определенной функции (функций) безопасности. Оценщик может изменить подход к тестированию определенной функции безопасности, тестируя ее с использованием другой стратегии тестирования;

b) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

c) поддержание некоторого баланса между видами деятельности по оценке. Усилия оценщика, затраченные на вид деятельности по тестированию, должны быть соразмерны с усилиями, затраченными на любой другой вид деятельности по оценке.

Оценщик выбирает определенные функции безопасности для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества ФБО:

a) строгость тестирования разработчиком функций безопасности. Все функции безопасности, идентифицированные в функциональной спецификации, должны иметь относящиеся к ним свидетельства тестирования разработчиком, как это требуется в ATE_COV.2 «Анализ покрытия». Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество ФБО;

b) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что функция безопасности или ее аспект выполняется в соответствии со спецификациями, то оценщику следует включить подобные функции безопасности в тестируемое подмножество;

c) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места неизвестны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функций безопасности;

d) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

e) утверждение о СФБ, сделанное в ЗБ. Все функции безопасности, для которых было сделано конкретное утверждение о СФБ, следует включить в тестируемое подмножество ФБО;

f) сложность функции безопасности. Для сложных функций безопасности может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, что, в свою очередь, не будет способствовать экономичным оценкам. С другой стороны, сложные функции безопасности — это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

g) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы могут обеспечивать несколько функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

h) типы интерфейсов ОО (например, программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть возможность включения тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

i) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут широко быть представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

Выше сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.5.4.2 Шаг оценивания 3:ATE_IND.2-5

Оценщик должен разработать тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Установив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

a) подход, который будет использован, например, будет ли функция безопасности протестирована через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет применен альтернативный тестированию подход (например, в исключительных обстоятельствах — экспертиза кода);

b) интерфейс(ы) функции безопасности, который(е) будет(ут) использован(ы) для инициирования выполнения функции безопасности и наблюдения ее реакции;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования выполнения функции безопасности (например, генераторы пакетов), либо для наблюдения за функцией безопасности (например, сетевые анализаторы).

Оценщик может посчитать практичным тестировать каждую функцию безопасности с помощью ряда наборов тестов, где каждый набор тестов будет использован для тестирования конкретного режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

12.9.5.4.3 Шаг оценивания 3:ATE_IND.2-6

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для тестирования ОО, но это не мешает ему выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты должны быть внесены в тестовую документацию.

12.9.5.4.4 Шаг оценивания 3:ATE_IND.2-7

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестов:

a) идентификационную информацию тестируемого режима выполнения функции безопасности;

b) инструкции по подключению и настройке всего необходимого оборудования для тестирования, как это требуется для выполнения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения функции безопасности;

f) описание всех ожидаемых результатов и необходимого анализа, проводимого по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО;

h) фактические результаты тестирования.

Уровень детализации должен быть таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут различаться (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, приведенную на этом шаге оценивания (например, фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

12.9.5.4.5 Шаг оценивания 3:ATE_IND.2-8

Оценщик должен проверить, что все фактические результаты тестирования соответствуют ожидаемым результатам тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая документация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

12.9.5.5 Действие ATE_IND.2.3E

12.9.5.5.1 Шаг оценивания 3:ATE_IND.2-9

Оценщик должен провести тестирование, используя выборку тестов, предусмотренных в плане и процедурах тестирования разработчика.

Общая цель данного шага оценивания состоит в выполнении тестов разработчика в количестве, достаточном для подтверждения правильности результатов тестирования разработчиком. Оценщик должен определить размер выборки и тесты разработчика, которые составят данную выборку.

С учетом общих усилий оценщика по виду деятельности, связанному с тестированием, обычно следует выполнить около 20 % тестов разработчика, хотя этот процент может варьироваться в зависимости от характера ОО и представленных свидетельств тестирования.

Все тесты разработчика могут быть сопоставлены с конкретными функциями безопасности. Следовательно, факторы, которые необходимо рассмотреть при выборе тестов для включения в выборку, подобны тем, которые перечислены на шаге оценивания ATE_IND.2-4 для выбора тестируемого подмножества ФБО. Дополнительно, для выбора тестов разработчика, включаемых в выборку, оценщик может избрать метод случайной выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

12.9.5.5.2 Шаг оценивания 3:ATE_IND.2-10

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Противоречия между ожидаемыми результатами тестирования разработчиком и фактическими результатами тестирования заставляют оценщика разрешать эти несоответствия. Противоречия, с которыми столкнулся оценщик, могут быть разрешены разработчиком путем убедительного объяснения и устранения противоречий.

Если удовлетворительное объяснение или устранение противоречий не может быть достигнуто, то уверенность оценщика в результатах тестирования разработчиком может уменьшиться; у оценщика даже может возникнуть необходимость в увеличении объема выборки, чтобы восстановить уверенность в результатах тестирования разработчиком. Если увеличение объема выборки не оправдает ожиданий оценщика, может потребоваться повторение всей совокупности тестов разработчика. В конечном счете, для адекватного тестирования подмножества ФБО, идентифицированного на шаге оценивания ATE_IND.2-4, недостаточность тестов разработчика приведет к необходимости корректировки тестов разработчика или разработки оценщиком новых тестов.

12.9.5.5.3 Шаг оценивания 3:ATE_IND.2-11

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию. Смысл предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию, объем выполненного оценщиком тестирования, объем выполненного разработчиком тестирования, тестируемые конфигурации ОО и общий результат вида деятельности по тестированию.

Информация, относящаяся к усилиям оценщика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были протестированы;

b) выбранный размер подмножества. Число протестированных в течение оценки функций безопасности и логическое обоснование этого размера;

c) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

d) протестированные функции безопасности. Краткий перечень функций безопасности, обоснованно включенных в подмножество;

e) выполненные тесты разработчика. Число выполненных тестов разработчика и краткое описание критериев, использованных для выбора данных тестов;

f) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует привести в ТОО.

12.10 Вид деятельности «Оценка уязвимостей»

Вид деятельности «Оценка уязвимостей» предназначен для того, чтобы сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО. Это заключение должно быть основано на анализе, выполненном разработчиком и оценщиком, и поддержано тестированием, выполненным оценщиком.

12.10.1 Оценка неправильного применения (AVA_MSU.1)

12.10.1.1 Цели

Цель данного подвида деятельности — сделать заключение, не являются ли руководства вводящими в заблуждение, необоснованными или противоречивыми, были ли учтены процедуры безопасности для всех режимов функционирования и будет ли использование руководств способствовать предотвращению и обнаружению небезопасных состояний ОО.

12.10.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска;

g) тестовая документация.

12.10.1.3 Замечания по применению

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной установки, генерации и запуска. Здесь к процедурам установки, генерации и запуска относятся все процедуры перевода ОО из состояния при поставке в состояние функционирования, ответственным за выполнение которых является администратор.

12.10.1.4 Действие AVA_MSU.1.1E

12.10.1.4.1 Шаг оценивания 3:AVA_MSU.1-1

ИСО/МЭК 15408-3 AVA_MSU.1.1C: *Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.*

Оценщик должен исследовать руководства и другие свидетельства оценки, чтобы сделать заключение, идентифицированы ли в руководствах все возможные режимы эксплуатации ОО (включая, если применимо, функционирование после сбоя или ошибки в работе), их последствия и значение для поддержания безопасной эксплуатации.

Другие свидетельства оценки, в особенности функциональная спецификация и тестовая документация, представляют собой источник информации, который оценщику следует использовать, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию.

Оценщику следует сосредоточиться одновременно на одной функции безопасности, сопоставляя руководства для безопасного использования данной функции безопасности с другими свидетельствами оценки, чтобы сделать заключение, достаточны ли руководства в части, относящейся к данной функции безопасности, для ее безопасного использования (т.е. согласовано ли оно с ПБО). Оценщику следует также рассмотреть соотношения между функциями, осуществляя поиск потенциальных конфликтов.

12.10.1.4.2 Шаг оценивания 3:AVA_MSU.1-2

ИСО/МЭК 15408-3 AVA_MSU.1.2C: *Руководства должны быть полны, понятны, непротиворечивы и обоснованны.*

Оценщик должен исследовать руководства, чтобы сделать заключение, являются ли они понятными и внутренне непротиворечивыми.

Руководства являются непонятными, если они так или иначе могут быть неправильно истолкованы администратором или пользователем и использованы путем, причиняющим ущерб ОО или безопасности, обеспечиваемой ОО.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

12.10.1.4.3 Шаг оценивания 3:AVA_MSU.1-3

Оценщик должен исследовать руководства и другие свидетельства оценки, чтобы сделать заключение, являются ли руководства полными и обоснованными.

Оценщику следует использовать знание ОО, приобретенное при выполнении других видов деятельности по оценке, чтобы сделать заключение, являются ли руководства полными.

В частности, оценщику следует рассмотреть функциональную спецификацию и краткую спецификацию ОО. Предполагается, что все функции безопасности, описание которых содержится в этих документах, описаны в руководствах надлежащим образом, чтобы дать возможность их безопасного администрирования и использования. Оценщик может в качестве вспомогательного средства подготовить неформальное отображение между руководствами и этими документами. Какие-либо пропуски в этом отображении могут указывать на неполноту.

Руководства являются необоснованными, если они содержат требования к использованию ОО или среде функционирования, которые противоречат ЗБ или являются чрезмерно обременительными для поддержания безопасности.

Оценщику следует учесть, что результаты, полученные в процессе выполнения шагов оценивания подвида деятельности AGD_ADM, предоставят полезные исходные данные для данного исследования.

12.10.1.4.4 Шаг оценивания 3:AVA_MSU.1-4

ИСО/МЭК 15408-3 AVA_MSU.1.3C: *Руководства должны содержать список всех предположений относительно среды эксплуатации.*

Оценщик должен исследовать руководства, чтобы сделать заключение, все ли предположения относительно предопределенной среды четко сформулированы.

Оценщик анализирует предположения ЗБ относительно предопределенной среды безопасности ОО и сравнивает их с руководствами, чтобы удостовериться, все ли предположения из ЗБ относительно предопределенной среды безопасности ОО, которые имеют отношение к администратору или пользователю, соответствующим образом описаны в руководствах.

12.10.1.4.5 Шаг оценивания 3:AVA_MSU.1-5

ИСО/МЭК 15408-3 AVA_MSU.1.4C: *Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль над процедурами, физическими мерами и персоналом).*

Оценщик должен исследовать руководства, чтобы сделать заключение, все ли требования для внешних мер безопасности четко сформулированы.

Оценщик анализирует руководства, чтобы удостовериться, перечислены ли в них все внешние процедурные меры, меры физической защиты, управления персоналом и связностью. Цели безопасности в ЗБ для не-ИТ среды указывают на то, что требуется.

12.10.1.5 Действие AVA_MSU.1.2E

12.10.1.5.1 Шаг оценивания 3:AVA_MSU.1-6

Оценщик должен выполнить все процедуры администратора и пользователя (если применимо), необходимые для конфигурирования и установки ОО, чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Конфигурация и инсталляция требуют, чтобы оценщик перевел ОО из состояния при поставке в состояние, в котором ОО функционирует и осуществляет ПБО, согласованную с целями безопасности, специфицированными в ЗБ.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя и администратора, обычно поставляемых потребителю ОО. Любые встретившиеся трудности в процессе такого применения процедур могут указывать на неполноту, непонятность, противоречивость или необоснованность руководств.

Работа, выполненная для удовлетворения данного шага оценивания, может также способствовать удовлетворению действия оценщика ADO_IGS.1.2E.

12.10.1.6 Действие AVA_MSU.1.3E

12.10.1.6.1 Шаг оценивания 3:AVA_MSU.1-7

Оценщик должен исследовать руководства, чтобы сделать заключение, предоставлены ли потребителю руководства, достаточные, чтобы эффективно администрировать и использовать функции безопасности ОО, а также обнаруживать небезопасные состояния.

ОО могут использовать разнообразные способы содействия потребителю в эффективном, с точки зрения безопасности, использовании ОО. Один ОО может использовать функциональные возможности (характеристики), чтобы предупредить потребителя, когда ОО находится в небезопасном состоянии, в то время как другие ОО могут быть поставлены с расширенными руководствами, содержащими предложения, советы, процедуры и т.д. по наиболее эффективному использованию существующих характеристик безопасности, например с руководством по использованию аудита как вспомогательного средства при обнаружении небезопасных состояний.

Чтобы вынести вердикт для этого шага оценивания, оценщик рассматривает функциональные возможности ОО, его назначение и предопределенную среду, а также предположения о его использовании или о пользователях. Оценщику следует прийти к заключению, что если возможен переход ОО в небезопасное состояние, то имеется ли обоснованное ожидание, что использование руководства позволит своевременно обнаружить небезопасное состояние. Заключение о потенциальной возможности перехода ОО в небезопасные состояния может быть сделано с использованием поставляемых для оценки материалов, таких как ЗБ, функциональная спецификация и проект верхнего уровня ФБО.

12.10.2 Оценка стойкости функций безопасности ОО (AVA_SOF.1)

12.10.2.1 Цели

Цель данного подвида деятельности — сделать заключение, приведены ли в ЗБ утверждения о СФБ для всех вероятностных или перестановочных механизмов и поддержаны ли утверждения о СФБ, приведенные разработчиком в ЗБ, корректным анализом.

12.10.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) материалы анализа стойкости функций безопасности ОО.

12.10.2.3 Замечания по применению

Анализ СФБ выполняют для механизмов, которые по своей природе являются вероятностными или перестановочными, таких как механизм пароля или биометрия. Хотя криптографические механизмы также являются вероятностными и зачастую описываются в терминах стойкости, AVA_SOF.1 «Оценка стойкости функции безопасности» не применим к криптографическим механизмам. Для таких механизмов оценщику следует руководствоваться указаниями системы оценки.

Хотя анализ СФБ выполняют на базе отдельных механизмов, общее заключение о СФБ базируется на функциях. Если для обеспечения некоторой функции безопасности применяют более одного вероятностного или перестановочного механизма, проанализирован должен быть каждый отдельный механизм. Способ объединения этих механизмов для обеспечения функции безопасности определит общий уровень СФБ для этой функции. Оценщику необходима информация о проекте, чтобы понять, как механизмы работают вместе, чтобы обеспечить функцию, и минимальный уровень для такой информации предоставляют через зависимость от ADV_HLD.1 «Описательный проект верхнего уровня». Фактическая проектная информация, доступная оценщику, определяется ОУД, и эту доступную информацию, когда требуется, следует использовать для поддержки анализа, выполняемого оценщиком.

О СФБ в отношении многодоменных ОО см. в 9.3.6 «Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1).

12.10.2.4 Действие AVA_SOF.1.1E

12.10.2.4.1 Шаг оценивания 3:AVA_SOF.1-1

ИСО/МЭК 15408-3 AVA_SOF.1.1C: *Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого в ЗБ имеется утверждение о СФБ, выраженное как уровень СФБ.

Если утверждения о СФБ выражены исключительно в метрике СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Уровень СФБ выражают как базовую СФБ, среднюю СФБ или высокую СФБ, которые определены в терминах потенциала нападения, — см. ИСО/МЭК 15408-1, раздел 2. Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ как некотором уровне, который превышает общее требование СФБ.

Руководство по определению потенциала нападения, необходимого для осуществления нападения, и, следовательно, определению СФБ как некоторого уровня см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

Материалы анализа СФБ включают в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

12.10.2.4.2 Шаг оценивания 3:AVA_SOF.1-2

ИСО/МЭК 15408-3 AVA_SOF.1.2C: *Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого имеется утверждение о СФБ в ЗБ, выраженное в некоторой метрике.

Если утверждения о СФБ выражены исключительно как уровни СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ в метрике, которая удовлетворяет или превосходит общее требование СФБ.

Анализ СФБ включает в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

12.10.2.4.3 Шаг оценивания 3:AVA_SOF.1-3

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, являются ли обоснованными любые утверждения или предположения, поддерживающие анализ.

Например, может быть неверным предположение, что конкретная реализация генератора псевдослучайных чисел будет обладать энтропией, необходимой для отбора данного механизма безопасности в число тех, для которых уместен анализ СФБ.

Ожидается, что предположения, сопровождающие анализ СФБ, отражают самый плохой случай, за исключением случая, являющегося в соответствии с ЗБ несостоятельным. Когда существует ряд различных возможных сценариев, зависящих от поведения человека-пользователя или нарушителя, следует предположить сценарий, который представляет самую низкую стойкость, если этот сценарий не был признан ранее несостоятельным.

Например, утверждение о стойкости, основанное на максимальной теоретически возможной области значений пароля (т.е. комбинаций всех печатных символов ASCII), обычно не является самым плохим случаем, потому что человеку свойственно использовать пароли на естественном языке, существенно уменьшая область значений пароля и ассоциированную с ней стойкость. Однако такое предположение может быть приемлемым, если в конкретном ОО применены меры ИТ, идентифицированные в ЗБ, такие как фильтры паролей, с целью минимизировать использование паролей на естественном языке.

12.10.2.4.4 Шаг оценивания 3:AVA_SOF.1-4

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, корректны ли любые алгоритмы, принципы, характеристики и вычисления, поддерживающие анализ.

Характер данного шага оценивания сильно зависит от типа рассматриваемого механизма. В А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А) представлен пример анализа СФБ для функции идентификации и аутентификации, которая реализована с использованием механизма пароля; при анализе рассмотрена максимальная область значений пароля, чтобы, в конечном счете, прийти к некоторому уровню СФБ. Для биометрии при анализе рассматривают разрешающую способность и другие факторы, влияющие на чувствительность механизма к обману.

СФБ, выраженная как некоторый уровень, основана на минимальном потенциале нападения, требуемом, чтобы нанести поражение механизму безопасности. Уровни СФБ определены в терминах потенциала нападения в ИСО/МЭК 15408-1, раздел 2.

Руководство по определению потенциала нападения см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

12.10.2.4.5 Шаг оценивания 3:AVA_SOF.1-5

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, каждое ли утверждение о СФБ удовлетворено или превышено.

Руководство по ранжированию утверждений о СФБ см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

12.10.2.4.6 Шаг оценивания 3:AVA_SOF.1-6

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, все ли функции с заявленной СФБ удовлетворяют минимальному уровню стойкости, определенному в ЗБ.

12.10.2.5 Действие AVA_SOF.1.2E

12.10.2.5.1 Шаг оценивания 3:AVA_SOF.1-7

Оценщик должен исследовать функциональную спецификацию, проект верхнего уровня, руководство пользователя и руководство администратора, чтобы сделать заключение, для всех ли вероятностных или перестановочных механизмов имеется утверждение о СФБ.

Идентификация разработчиком функций безопасности, которые реализованы вероятностными или перестановочными механизмами, должна быть верифицирована в процессе оценки ЗБ. Однако, поскольку краткая спецификация ОО может быть единственным свидетельством, доступным при выполнении этих действий, идентификация таких механизмов может быть неполной. Дополнительные свидетельства оценки, требуемые в качестве исходных данных для этого подвида деятельности, могут идентифицировать дополнительные вероятностные или перестановочные механизмы, ранее не идентифицированные в ЗБ. Если это так, то ЗБ должно быть соответствующим образом обновлено, чтобы отразить дополнительные утверждения о СФБ, а разработчику будет необходимо представить материалы дополнительного анализа, в которых должны быть логически обоснованы утверждения о СФБ, в качестве исходных данных для действия оценщика AVA_SOF.1.1E.

12.10.2.5.2 Шаг оценивания 3:AVA_SOF.1-8

Оценщик должен исследовать утверждения о СФБ, чтобы сделать заключение, являются ли они корректными.

Если материалы анализа СФБ включают в себя утверждения или предположения (например, о возможном числе попыток аутентификации в минуту), оценщику следует независимо подтвердить, что они корректны. Это может быть достигнуто путем тестирования или независимого анализа.

12.10.3 Оценка анализа уязвимостей (AVA_VLA.1)

12.10.3.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, явные уязвимости, пригодные для использования.

12.10.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска;

g) материалы анализа уязвимостей;

h) материалы анализа утверждений о стойкости функции;

i) ОО, пригодный для тестирования.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа оценки).

12.10.3.3 Замечания по применению

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной установки, генерации и запуска.

Рассмотрение пригодных для использования уязвимостей определяется целями безопасности и функциональными требованиями в ЗБ. Например, если меры по предотвращению обхода функций безопасности не требуются в ЗБ (FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена» отсутствуют), то уязвимости, на которых базируется обход, рассматривать не следует.

Уязвимости могут быть или не быть идентифицированы в общедоступных источниках и могут требовать или не требовать навыка для их использования. Эти два фактора являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована только потому, что она идентифицирована в общедоступных источниках.

Следующие термины использованы в данном руководстве с конкретным значением:

a) уязвимость — слабость в ОО, которая может быть использована, чтобы нарушить политику безопасности в некоторой среде;

b) анализ уязвимостей — систематический поиск уязвимостей в ОО и оценка найденных уязвимостей, чтобы сделать заключение об их значимости для предопределенной среды ОО;

c) явная уязвимость — уязвимость, которая является открытой для использования, требующего минимума понимания ОО, технических познаний и ресурсов;

d) потенциальная уязвимость — уязвимость, существование которой в ОО предположено (на основании теоретически допускаемого маршрута нападения), но не подтверждено;

e) пригодная для использования уязвимость — уязвимость, которая может быть использована в предопределенной среде ОО;

f) непригодная для использования уязвимость — уязвимость, которая не может быть использована в предопределенной среде ОО;

g) остаточная уязвимость — непригодная для использования уязвимость, которая могла бы быть использована нарушителем с более высоким потенциалом нападения, чем ожидается в предопределенной среде ОО;

h) тестирование проникновения — тестирование, выполняемое с целью сделать заключение о пригодности к использованию в предопределенной среде ОО идентифицированных потенциальных уязвимостей ОО.

12.10.3.4 Действие AVA_VLA.1.1E

12.10.3.4.1 Шаг оценивания 3:AVA_VLA.1-1

ИСО/МЭК 15408-3 AVA_VLA.1.1C: *Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска явных способов, которыми пользователь может нарушить ПБО.*

ИСО/МЭК 15408-3 AVA_VLA.1.2C: *Документация анализа уязвимостей должна содержать описание решения в отношении явных уязвимостей.*

ИСО/МЭК 15408-3 AVA_VLA.1.3C: *Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.*

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, вся ли относящаяся к этому анализу информация рассмотрена при поиске явных уязвимостей.

Предполагается, что анализ уязвимостей, выполненный разработчиком, охватывает поиск разработчиком явных уязвимостей, по меньшей мере, во всех поставляемых для оценки материалах и общедоступных источниках информации. Оценщику следует использовать поставляемые для оценки материалы не для выполнения независимого анализа уязвимостей (что не требуется AVA_VLA.1 «Анализ уязвимостей разработчиком»), а как основу для оценки поиска разработчиком явных уязвимостей.

Информация в общедоступных источниках является очень динамичной. Поэтому возможно, что о новых уязвимостях будет сообщено в общедоступных источниках в период между временем, когда разработчик выполняет анализ уязвимостей, и временем завершения оценки. Моментом прекращения мониторинга информации в общедоступных источниках является выпуск органом оценки результатов оценки; поэтому за указаниями следует обращаться к органу оценки.

12.10.3.4.2 Шаг оценивания 3:AVA_VLA.1-2

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

Предполагается, что разработчик выполнил поиск явных уязвимостей, основываясь на знании ОО и информации из общедоступных источников. Требование задано только по идентификации явных уязвимостей, при этом подробный анализ не предполагается. Разработчик фильтрует эту информацию на основе вышеизложенного определения и показывает, что явные уязвимости являются непригодными для использования в предопределенной среде.

Оценщику необходимо обратить внимание на три аспекта анализа, выполненного разработчиком:

a) были ли при анализе разработчиком рассмотрены все поставляемые для оценки материалы;

b) приняты ли соответствующие меры для предотвращения использования явных уязвимостей в предопределенной среде;

c) остались ли некоторые явные уязвимости неидентифицированными.

Оценщику не следует беспокоиться, являются ли идентифицированные уязвимости явными или не являются, если это не используется разработчиком в качестве основы для заключения о непригодности уязвимостей для использования. В этом случае оценщик проверяет правильность утверждений, делая заключение о противодействии нарушителю с низким потенциалом нападения по отношению к идентифицированной уязвимости.

Понятие «явные уязвимости» не связано с понятием «потенциал нападения». Последний определяется оценщиком в ходе независимого анализа уязвимостей. Так как эти действия не выполняются для AVA_VLA.1 «Анализ уязвимостей разработчиком», то обычно поиск и фильтрация информации на основе потенциала нападения оценщиком не осуществляются. Однако оценщик может еще обнаружить потенциальные уязвимости в ходе оценки, а заключение, как их следует учитывать, сделать путем ссылки на определение явных уязвимостей и понятие низкого потенциала нападения.

Заключение, остались ли некоторые явные уязвимости неидентифицированными, ограничивается оценкой правильности анализа, выполненного разработчиком, сравнением с информацией об уязвимостях из общедоступных источников, а также сравнением с любыми последующими уязвимостями, идентифицированными оценщиком в ходе выполнения других действий по оценке.

Уязвимость считают непригодной для использования, если выполнено одно или более условие из следующих условий:

a) функции или меры безопасности в (ИТ или не-ИТ) среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования;

b) уязвимость является пригодной для использования, но только нарушителями, обладающими умеренным или высоким потенциалом нападения. Например, уязвимость распределенного ОО к нападениям, связанным с перехватом сеанса, требует потенциала нападения выше, чем необходимо для использования явной уязвимости. Такие уязвимости должны быть приведены в ТОО в качестве остаточных уязвимостей;

c) в ЗБ либо не утверждается о противостоянии определенной угрозе, либо не утверждается о следовании определенной политике безопасности организации, которая может быть нарушена. Например, для межсетевого экрана, в ЗБ которого не заявлена политика доступности и который уязвим к TCP SYN-атакам

(нападение на общепринятый протокол Интернета, которое лишает хосты способности обслуживания запросов на соединение), не следует делать отрицательного заключения по данному действию оценщика только на основе одной этой уязвимости.

Руководство по определению потенциала нападения, необходимого для использования уязвимости, см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

12.10.3.4.3 Шаг оценивания 3:AVA_VLA.1-3

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, согласуются ли они с ЗБ и руководствами.

Анализ уязвимостей разработчиком может быть направлен на некоторую уязвимость с предложением конкретных конфигураций или настроек функций ОО. Если такие ограничения применения считают действенными и согласованными с ЗБ, то предполагают, что все такие конфигурации/настройки адекватно описаны в руководствах, чтобы их мог применить потребитель.

12.10.3.5 Действие AVA_VLA.1.2E

12.10.3.5.1 Шаг оценивания 3:AVA_VLA.1-4

Оценщик должен подготовить тесты проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик готовит к тестированию проникновения:

a) то, что необходимо, чтобы попытаться опровергнуть анализ разработчика в случаях, когда обоснование разработчиком непригодности уязвимости для использования является, по мнению оценщика, сомнительным;

b) то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей предопределенной среде, к явной уязвимости, не рассмотренной разработчиком. Оценщику необходимо иметь доступ к текущей информации (например, от органа оценки) о явных уязвимостях из общедоступных источников, которые могли быть не рассмотрены разработчиком; необходимо, чтобы оценщик также мог идентифицировать потенциальные уязвимости в результате выполнения других действий по оценке.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, которые являются явными. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем пригодность к использованию может быть определена. Если в результате исследований в ходе оценки оценщик обнаружит некоторую уязвимость, не относящуюся к явным, то она должна быть приведена в ТОО как остаточная уязвимость.

Поняв предполагаемую явную уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности, оценщик рассматривает:

a) интерфейсы функций безопасности, которые будут использованы для инициирования выполнения ФБО и наблюдения их реакции;

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости).

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использован для тестирования конкретной явной уязвимости.

12.10.3.5.2 Шаг оценивания 3:AVA_VLA.1-5

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на материалах анализа уязвимостей, выполненного разработчиком, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Тестовая документация должна включать в себя:

a) идентификацию тестируемой явной уязвимости ОО;

b) инструкции по подключению и настройке всего необходимого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и анализа, который следует проводить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО.

Цель данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

12.10.3.5.3 Шаг оценивания 3:AVA_VLA.1-6

Оценщик должен провести тестирование проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик использует документацию для тестов проникновения, подготовленных на шаге оценивания AVA_VLA.1-4, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может подготовить специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию для тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, существование которых оценщик предположил во время предварительно запланированного тестирования.

12.10.3.5.4 Шаг оценивания 3:AVA_VLA.1-7

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общие результаты должен быть идентичными. Любые различия следует логически обосновать.

12.10.3.5.5 Шаг оценивания 3:AVA_VLA.1-8

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, что ОО (в своей предопределенной среде) не имеет пригодных для использования явных уязвимостей.

Если результаты показывают, что ОО имеет явные уязвимости, пригодные для использования в его предопределенной среде, то это приводит к отрицательному вердикту по данному действию оценщика.

12.10.3.5.6 Шаг оценивания 3:AVA_VLA.1-9

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию проникновения, объем выполненного тестирования проникновения, тестируемые конфигурации ОО и общий результат действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были подвергнуты тестированию проникновения;

b) функции безопасности, подвергнутые тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

12.10.3.5.7 Шаг оценивания 3:AVA_VLA.1-10

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

a) ее источник (например, стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанную с ней функцию (функции) безопасности, не достигнутую цель (цели), нарушенную политику (политики) безопасности организации, реализованную угрозу (угрозы);

c) описание;

d) пригодна ли она для использования в предопределенной среде или нет (т.е. пригодная для использования или является остаточной уязвимостью);

e) идентификацию участника оценки (например, разработчик, оценщик), который ее идентифицировал.

13 Оценка по ОУД4

13.1 Введение

ОУД4 обеспечивает уровень доверия в диапазоне от умеренного до высокого. Для обеспечения понимания режимов безопасного функционирования ОО функции безопасности анализируют с использованием функциональной спецификации, документации руководств, проектов верхнего и нижнего уровня ОО, а также подмножества представления реализации. Данный анализ должен быть поддержан независимым тестированием подмножества функций безопасности ОО, свидетельством тестирования разработчиком, основанным на функциональной спецификации и проекте верхнего уровня, выборочным подтверждением результатов тестирования разработчиком, анализом стойкости функций безопасности, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим стойкость к нападениям проникновения, выполняемым нарушителем, обладающим низким потенциалом нападения. Доверия дополнительно достигают применением неформальной модели политики безопасности ОО, мер управления средой разработки, автоматизированного управления конфигурацией ОО и свидетельства безопасных процедур поставки.

13.2 Цели

Цель данного раздела заключается в определении минимальных усилий, необходимых для успешного выполнения оценки по ОУД4, и предоставлении руководства по способам и средствам выполнения оценки.

13.3 Организация оценки по ОУД4

Оценка по ОУД4 предусматривает следующее:

a) задачу получения исходных данных для оценки (раздел 7);

b) виды деятельности по оценке по ОУД4, включающие в себя:

1) оценку ЗБ (раздел 9);

2) оценку управления конфигурацией (13.4);

3) оценку документов поставки и эксплуатации (13.5);

4) оценку документов разработки (13.6);

5) оценку руководств (13.7);

6) оценку поддержки жизненного цикла (13.8);

7) оценку тестов (13.9);

8) тестирование (13.9);

9) оценку оценки уязвимостей (13.10);

c) задачу оформления результатов оценки (раздел 7).

Виды деятельности по оценке следуют из требований доверия ОУД4, содержащихся в ИСО/МЭК 15408-3.

Оценка ЗБ начинается до выполнения любых подвидов деятельности по оценке ОО, так как ЗБ обеспечивает основание и контекст для выполнения этих подвидов деятельности.

В настоящем разделе приведено описание подвидов деятельности, выполняемых при оценке по ОУД4. Хотя выполнение подвидов деятельности может, в общем случае, начинаться более или менее случайным образом, некоторые зависимости между подвидами деятельности должны быть учтены оценщиком.

Руководство по учету зависимостей см. в А.4 «Зависимости» (приложение А).

13.4 Вид деятельности «Управление конфигурацией»

Цель вида деятельности «Управление конфигурацией» состоит в том, чтобы помочь потребителю в идентификации оцененного ОО и удостовериться в том, что элементы конфигурации уникально идентифицированы, а также удостовериться в адекватности процедур, используемых разработчиком для управления и отслеживания изменений, вносимых в ОО. При этом детально должно быть рассмотрено, какие изменения отслеживают, каким образом вносят потенциальные изменения, а также степень использования автоматизации для уменьшения возможности ошибок.

13.4.1 Оценка автоматизации УК (ACM_AUT.1)

13.4.1.1 Цели

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

13.4.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация управления конфигурацией.

13.4.1.3 Действие ACM_AUT.1.1E

13.4.1.3.1 Шаг оценивания 4:ACM_AUT.1-1

ИСО/МЭК 15408-3 ACM_AUT.1.1C: *Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО проводятся только санкционированные изменения.*

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

13.4.1.3.2 Шаг оценивания 4:ACM_AUT.1-2

Оценщик должен исследовать автоматизированные средства контроля доступа, чтобы сделать заключение об их эффективности для предотвращения несанкционированной модификации представления реализации ОО.

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

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

13.4.1.3.3 Шаг оценивания 4:ACM_AUT.1-3

ИСО/МЭК 15408-3 ACM_AUT.1.2C: *Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.*

Оценщик должен проверить документацию УК в части автоматизированных средств поддержки генерации ОО из его представления реализации.

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

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

13.4.1.3.4 Шаг оценивания 4:ACM_AUT.1-4

Оценщик должен исследовать автоматизированные процедуры генерации, чтобы сделать заключение, могут ли они быть использованы для поддержки генерации ОО.

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

Следует отметить, что это требование является только требованием предоставления поддержки. Например, подход, при котором исполняемые файлы Unix помещаются под управление конфигурацией, следует считать достаточным для достижения данной цели, учитывая, что такой подход к автоматизации существенно содействовал бы точной генерации ОО. Автоматизированные процедуры могут способствовать определению надлежащих элементов конфигурации, которые необходимо использовать при генерации ОО.

13.4.1.3.5 Шаг оценивания 4:ACM_AUT.1-5

ИСО/МЭК 15408-3 ACM_AUT.1.3C: *План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.*

Оценщик должен проверить, что план УК содержит информацию относительно автоматизированных инструментальных средств, используемых в системе УК.

13.4.1.3.6 Шаг оценивания 4:ACM_AUT.1-6

ИСО/МЭК 15408-3 ACM_AUT.1.4C: *План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.*

Оценщик должен исследовать информацию, относящуюся к автоматизированным инструментальным средствам, представленным в плане УК, чтобы сделать заключение, что в нем описано, как эти средства используются.

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

a) функциональности, обеспечиваемой инструментальными средствами;

b) использования этой функциональности разработчиком для управления изменениями в представлении реализации;

c) использования этой функциональности разработчиком для поддержки генерации ОО.

13.4.1.4 Подразумеваемое действие оценщика

13.4.1.4.1 Шаг оценивания 4:ACM_AUT.1-7

ИСО/МЭК 15408-3 ACM_AUT.1.1D: *Разработчик должен использовать систему УК.*

Оценщик должен исследовать систему УК, чтобы сделать заключение, что использованы те автоматизированные инструментальные средства и процедуры, которые описаны в плане УК.

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

13.4.2 Оценка возможностей УК (ACM_CAP.4)

13.4.2.1 Цели

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

13.4.2.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) ЗБ;

b) ОО, пригодный для тестирования;

c) документация управления конфигурацией.

13.4.2.3 Действие ACM_CAP.4.1E

13.4.2.3.1 Шаг оценивания 4:ACM_CAP.4-1

ИСО/МЭК 15408-3 ACM_CAP.4.1C: *Маркировка ОО должна быть уникальна для каждой версии ОО.*

Оценщик должен проверить, что версия ОО, представленная для оценки, уникально маркирована.

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

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

13.4.2.3.2 Шаг оценивания 4:ACM_CAP.4-2

ИСО/МЭК 15408-3 ACM_CAP.4.2C: *ОО должен быть помечен маркировкой.*

Оценщик должен проверить, что ОО, представленный для оценки, имеет собственную маркировку.

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

ОО может предоставить способ, посредством которого он может быть легко идентифицирован. Например, программный ОО может отображать свое наименование и номер версии при запуске программы или в ответ на запрос через командную строку. Аппаратный или программно-аппаратный ОО может быть идентифицирован путем физического нанесения на нем соответствующего номера.

13.4.2.3.3 Шаг оценивания 4:ACM_CAP.4-3

Оценщик должен проверить непротиворечивость используемой маркировки ОО.

Если ОО помечен несколько раз, то необходима согласованность меток. Например, должна быть предусмотрена возможность связать любое помеченное руководство, поставляемое в составе ОО, с оцененным функционирующим ОО. Этим обеспечивается уверенность потребителя в том, что он приобрел оцененную версию ОО, установил эту же версию и располагает надлежащей версией руководства, необходимой для функционирования данного ОО в соответствии с его ЗБ. Оценщик может использовать список конфигурации, который является частью представленной документации УК, чтобы верифицировать согласованное использование идентификаторов.

Оценщик также верифицирует, что маркировка ОО согласована с ЗБ.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.4.2.3.4 Шаг оценивания 4:ACM_CAP.4-4

ИСО/МЭК 15408-3 ACM_CAP.4.3C: *Документация УК должна включать в себя список конфигурации, план УК и план приемки под УК.*

Оценщик должен проверить, что представленная документация УК включает в себя список конфигурации.

Список конфигурации идентифицирует элементы, находящиеся под управлением конфигурацией.

13.4.2.3.5 Шаг оценивания 4:ACM_CAP.4-5

Оценщик должен проверить, что представленная документация УК содержит план УК.

13.4.2.3.6 Шаг оценивания 4:ACM_CAP.4-6

Оценщик должен проверить, что представленная документация УК содержит план приемки.

13.4.2.3.7 Шаг оценивания 4:ACM_CAP.4-7

ИСО/МЭК 15408-3 ACM_CAP.4.4C: *Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен проверить, что список конфигурации уникально идентифицирует каждый элемент конфигурации.

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

13.4.2.3.8 Шаг оценивания 4:ACM_CAP.4-8

ИСО/МЭК 15408-3 ACM_CAP.4.5C: *Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.*

Оценщик должен исследовать список конфигурации, чтобы сделать заключение, что он идентифицирует элементы конфигурации, входящие в состав ОО.

Минимальный состав элементов конфигурации, которые необходимо включить в список конфигурации, задается требованиями семейства ACM_SCP «Область УК».

13.4.2.3.9 Шаг оценивания 4:ACM_CAP.4-9

ИСО/МЭК 15408-3 ACM_CAP.4.6C: *Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.*

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

13.4.2.3.10 Шаг оценивания 4:ACM_CAP.4-10

ИСО/МЭК 15408-3 ACM_CAP.4.7C: *Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.*

Оценщик должен исследовать элементы конфигурации, чтобы сделать заключение, что способ их идентификации соответствует документации УК.

Доверие к тому, что система УК однозначно идентифицирует все элементы конфигурации, должно быть достигнуто путем изучения идентификаторов элементов конфигурации. Как для элементов конфигурации, которые составляют ОО, так и для проектов элементов конфигурации, которые представлены разработ-

чиком в качестве свидетельств оценки, оценщик подтверждает, что каждый элемент конфигурации обладает уникальным идентификатором в соответствии с методом уникальной идентификации, который описан в документации УК.

13.4.2.3.11 Шаг оценивания 4:ACM_CAP.4-11

ИСО/МЭК 15408-3 ACM_CAP.4.8C: *План УК должен содержать описание, как используется система УК.*

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

Описания, содержащиеся в плане УК, могут включать в себя:

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

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

c) процедуры, используемые для обеспечения того, чтобы только уполномоченные лица могли изменять элементы конфигурации;

d) процедуры, используемые для исключения проблем параллелизма, возникающих в результате одновременных изменений элементов конфигурации;

e) свидетельство, генерируемое в результате применения процедур. Например, при изменении элемента конфигурации система УК могла бы зафиксировать описание изменения, ответственность за изменение, идентификацию всех затронутых элементов конфигурации, статус изменения (например, «не завершено» или «завершено»), а также дату и время внесения изменения. Эта информация могла бы быть внесена в журнал аудита проведенных изменений или в протокол контроля изменений;

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

13.4.2.3.12 Шаг оценивания 4:ACM_CAP.4-12

ИСО/МЭК 15408-3 ACM_CAP.4.9C: *Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.*

Оценщик должен проверить документацию УК, чтобы удостовериться, что она включает в себя записи системы УК, определенные планом УК.

Выходные материалы системы УК должны обеспечивать свидетельство, позволяющее оценщику быть уверенным, что план УК применяется, а все элементы конфигурации поддерживаются системой УК, как это требуется в ACM_CAP.4.10C. Пример выходных материалов мог бы включать в себя формы контроля изменений или формы разрешения доступа к элементам конфигурации.

13.4.2.3.13 Шаг оценивания 4:ACM_CAP.4-13

Оценщик должен исследовать свидетельство, чтобы сделать заключение, что система УК используется в соответствии с планом УК.

Оценщику необходимо осуществить и исследовать выборку из свидетельства, охватывающую каждый тип операций под УК, выполняемых на элементах конфигурации (например, создание, модификация, удаление, возврат к более ранней версии), чтобы подтвердить, что все операции системы УК выполнены в соответствии с задокументированными процедурами. Оценщик подтверждает, что свидетельство включает в себя всю информацию, идентифицированную для этой операции в плане УК. При исследовании свидетельства может потребоваться доступ к используемым инструментальным средствам УК. Оценщику разрешается остановиться на выборочной проверке свидетельства.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Дополнительная уверенность в правильном функционировании системы УК и эффективном сопровождении элементов конфигурации может быть получена проведением интервью с отобранными для этого участниками разработки. При проведении подобных интервью оценщику следует стремиться более глубоко понять практическое применение системы УК, а также убедиться, что процедуры УК применяются в соответствии с документацией УК. Однако такие интервью следует проводить скорее в дополнение, а не вместо изучения документального свидетельства; при этом они могут и не потребоваться, если документальное свидетельство полностью удовлетворяет требованиям. Тем не менее, учитывая широкую область применения плана УК, возможно, что некоторые аспекты (например, роли и обязанности) могут быть непонятны из одного только плана и протоколов УК. Это один из случаев, когда для дополнительного разъяснения понадобится интервью.

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

13.4.2.3.14 Шаг оценивания 4:ACM_CAP.4-14

ИСО/МЭК 15408-3 ACM_CAP.4.10C: *Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.*

Оценщик должен проверить, что элементы конфигурации, идентифицированные в списке конфигурации, сопровождаются системой УК.

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

Руководства по выборке см. в А.2 «Выборка» (приложение А).

13.4.2.3.15 Шаг оценивания 4:ACM_CAP.4-15

ИСО/МЭК 15408-3 ACM_CAP.4.11C: *Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.*

Оценщик должен исследовать меры контроля доступа в УК, описанные в плане УК, чтобы сделать заключение об их эффективности по предотвращению несанкционированного доступа к элементам конфигурации.

Оценщик может использовать несколько методов для заключения об эффективности мер контроля доступа в УК. Например, оценщик может опробовать меры контроля доступа, чтобы удостовериться, что процедуры нельзя обойти. Оценщик может использовать выходные материалы, сгенерированные процедурами системы УК и уже подвергавшиеся исследованию на шаге оценивания ACM_CAP.4-13. Оценщику может быть также продемонстрирована система УК, чтобы он убедился, что используемые меры контроля доступа выполняются эффективно.

Разработчик должен предусмотреть автоматизированные меры управления доступом как часть системы УК, а их пригодность может быть подтверждена в соответствии с компонентом ACM_AUT.1 «Частичная автоматизация УК».

13.4.2.3.16 Шаг оценивания 4:ACM_CAP.4-16

ИСО/МЭК 15408-3 ACM_CAP.4.12C: *Система УК должна поддерживать генерацию ОО.*

Оценщик должен проверить документацию УК в части процедур поддержки генерации ОО.

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

Оценщик должен убедиться в существовании процедур поддержки генерации в документации УК. Процедуры поддержки генерации, предоставленные разработчиком, могут быть автоматизированы, и в таком случае их существование может быть подтверждено в соответствии с шагом оценивания 4:ACM_AUT.1-3.

13.4.2.3.17 Шаг оценивания 4:ACM_CAP.4-17

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

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

Оценщику следует иметь в виду, что система УК не обязательно обладает способностью генерировать ОО, но она должна оказывать поддержку процессу, который будет способствовать уменьшению вероятности субъективной ошибки.

13.4.2.3.18 Шаг оценивания 4:ACM_CAP.4-18

ИСО/МЭК 15408-3 ACM_CAP.4.13C: *План приемки должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.*

Оценщик должен исследовать процедуры приемки, чтобы сделать заключение, что в них описаны критерии приемки, которые необходимо применять к вновь созданным или модифицированным элементам конфигурации.

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

a) на каждой стадии «сборки» ОО (например, для модулей, их интеграции, системы в целом);

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

c) для ранее оцененных компонентов.

Описание критериев приемки может содержать идентификацию:

a) ролей разработчиков или отдельных лиц, ответственных за приемку таких элементов конфигурации;

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

13.4.3 Оценка области УК (ACM_SCP.2)

13.4.3.1 Цели

Цель данного подвида деятельности — сделать заключение, выполняет ли разработчик управление конфигурацией для представления реализации ОО, проекта, тестов, руководств администратора и пользователя, документации УК и недостатков безопасности.

13.4.3.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является список элементов конфигурации.

13.4.3.3 Действие ACM_SCP.2.1E

13.4.3.3.1 Шаг оценивания 4:ACM_SCP.2-1

ИСО/МЭК 15408-3 ACM_SCP.2.1C: *Список элементов конфигурации должен включать в себя следующее: представление реализации, недостатки безопасности и свидетельства оценки, требуемые компонентами доверия из ЗБ.*

Оценщик должен проверить, чтобы список элементов конфигурации содержал совокупность элементов, требуемую ИСО/МЭК 15408.

Как минимум, список должен включать в себя следующее:

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

b) свидетельства оценки, требуемые компонентами доверия в ЗБ;

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

13.5 Вид деятельности «Поставка и эксплуатация»

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

13.5.1 Оценка поставки (ADO_DEL.2)

13.5.1.1 Цели

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

13.5.1.2 Исходные данные

Свидетельством оценки для этого подвида деятельности является документация поставки.

13.5.1.3 Действие ADO_DEL.2.1E

13.5.1.3.1 Шаг оценивания 4:ADO_DEL.2-1

ИСО/МЭК 15408-3 ADO_DEL.2.1C: *Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.*

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

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

В документации поставки должны быть описаны надлежащие процедуры для определения идентификации ОО и поддержания целостности ОО или его составных частей во время пересылки. В этих процедурах должно быть описано, какие части ОО должны быть охвачены подобными процедурами. В документации поставки должны быть приведены процедуры как для распространения физических копий, так и распространения в электронном виде (например, через Интернет), где это применимо. Процедуры поставки относятся к ОО в целом, включая применяемое программное обеспечение, аппаратные средства, программно-аппаратные средства и документацию.

Акцент в документации поставки, вероятно, будет сделан на мерах, связанных с целостностью, поскольку для поддержки целостности ОО в процессе его поставки требуется применение технических мер. Однако при поставке некоторых ОО должны быть обеспечены конфиденциальность и доступность; процедуры, относящиеся к этим аспектам безопасной поставки, должны также быть рассмотрены в документации.

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

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

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

13.5.1.3.2 Шаг оценивания 4:ADO_DEL.2-2

ИСО/МЭК 15408-3 ADO_DEL.2.2C: *Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.*

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

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

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

13.5.1.3.3 Шаг оценивания 4:ADO_DEL.2-3

ИСО/МЭК 15408-3 ADO_DEL.2.3C: *Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика даже в тех случаях, когда разработчик ничего не отсылал к месту использования.*

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

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

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

13.5.1.4 Подразумеваемое действие оценщика

13.5.1.4.1 Шаг оценивания 4:ADO_DEL.2-4

ИСО/МЭК 15408-3 ADO_DEL.2.2D: *Разработчик должен использовать процедуры поставки.*

Оценщик должен исследовать процедуры процесса поставки, чтобы сделать заключение о применении этих процедур.

Подход, предпринятый оценщиком для проверки применения процедур поставки, будет зависеть от природы ОО и самого процесса поставки. В дополнение к исследованию собственно процедур оценщику необходимо получить и определенную уверенность в их действительном применении. Некоторые возможные подходы перечислены ниже.

a) Посещение объекта (объектов) распространения, где можно наблюдать практическое применение процедур.

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

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

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

Для только что разработанного ОО возможно, что процедуры поставки еще необходимо отработать. В подобных случаях оценщику придется удовлетвориться тем, что имеются соответствующие процедуры и средства выполнения предстоящих поставок и что весь привлекаемый персонал знает свои обязанности. Оценщик может запросить «пробный прогон» поставки, если это практически осуществимо. Если разработчик производит другие подобные продукты, то для приобретения доверия может быть полезно исследование процедур при их применении.

13.5.2 Оценка установки, генерации и запуска (ADO_IGS.1)

13.5.2.1 Цели

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

13.5.2.2 Исходные данные

Свидетельства оценки для этого подвида деятельности:

a) руководство администратора;

b) процедуры безопасной установки, генерации и запуска;

c) ОО, пригодный для тестирования.

13.5.2.3 Замечания по применению

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

13.5.2.4 Действие ADO_IGS.1.1E

13.5.2.4.1 Шаг оценивания 4:ADO_IGS.1-1

ИСО/МЭК 15408-3 ADO_IGS.1.1C: *Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.*

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

Если не ожидается, что процедуры установки, генерации и запуска будут или могут быть повторно применены (например, если ОО поставлен в рабочем состоянии), то данный шаг оценивания (или отдельные его части) не применяют и поэтому считают удовлетворенным.

13.5.2.5 Действие ADO_IGS.1.2E

13.5.2.5.1 Шаг оценивания 4:ADO_IGS.1-2

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

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

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

a) изменения задаваемых при инсталляции характеристик безопасности сущностей, находящихся под управлением ФБО;

b) обработки исключительных ситуаций и проблем;

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

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

13.6 Вид деятельности «Разработка»

Вид деятельности «Разработка» предназначен для оценки проектной документации на предмет ее достаточности для понимания того, каким образом ФБО предоставляют функции безопасности ОО. Это понимание должно быть достигнуто путем экспертизы все более уточненных описаний в проектной документации ФБО. Проектная документация состоит из функциональной спецификации (которая описывает внешние интерфейсы ОО), проекта верхнего уровня (который описывает архитектуру ОО в терминах внутренних подсистем) и проекта нижнего уровня (который описывает архитектуру ОО в терминах внутренних модулей). Дополнительно имеются описание представления реализации (описание на уровне исходных текстов), модель политики безопасности (которая описывает политику безопасности, реализуемую ОО) и описание соответствия представлений (которое отображает представления ОО друг на друга, чтобы продемонстрировать их согласованность).

13.6.1 Замечания по применению

Требования ИСО/МЭК 15408 к проектной документации ранжированы по уровню формализации. В ИСО/МЭК 15408 рассмотрены следующие иерархические степени формализации документа: неформальный, полуформальный, формальный. Неформальный документ — это документ, который составлен на естественном языке. Методология не предписывает использовать какой-либо конкретный язык; этот вопрос остается за системой оценки. Ниже дифференцировано содержание различных неформальных документов.

Неформальная функциональная спецификация включает в себя описание функций безопасности (на уровне, подобном уровню представления краткой спецификации ОО) и описание внешне видимых интерфейсов ФБО. Например, если операционная система предоставляет пользователю средства идентификации пользователя, создания, модификации или удаления файлов, установления разрешения другим пользователям на доступ к файлам и взаимодействия с удаленными машинами, то ее функциональная спецификация, как правило, содержит описание каждой из этих функций. Если имеются также функции аудита, связанные с обнаружением и регистрацией таких событий, то описание указанных функций аудита также обычно включают в состав функциональной спецификации; и хотя пользователь формально не обращается к этим функциям непосредственно через внешний интерфейс, на них определенно влияет все то, что происходит на уровне внешнего пользовательского интерфейса.

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

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

В модели описаны политики, осуществляемые теми функциями и сервисами безопасности, которые приведены в функциональной спецификации. Неформальная модель — это описание политик безопасности, осуществляемых сервисами или функциями безопасности, доступными через внешний интерфейс.

Например, политики управления доступом обычно описывают защищаемые ресурсы и условия, которые должны быть обеспечены для предоставления доступа; политики аудита обычно описывают потенциально подвергаемые аудиту события ОО, идентифицируя как те, которые выбираются администратором, так и те, которые всегда подвергаются аудиту; политики идентификации и аутентификации обычно описывают, как идентифицируются пользователи, как аутентифицируется заявленная идентификационная информация, а также любые правила, влияющие на то, каким образом аутентифицируется идентификационная информация (например, для пользователей корпоративной внутренней сети аутентификация не требуется, в то время как внешние пользователи аутентифицируются на основе одноразовых паролей).

Необязательно, чтобы неформальная демонстрация соответствия была в повествовательной форме; может быть достаточно простого двухмерного отображения. Например, матрица с перечисленными по одной оси модулями и перечисленными по другой оси подсистемами, в которой ячейки указывают на соответствие модулей и подсистем, была бы полезна для представления адекватного неформального соответствия между проектом верхнего уровня и проектом нижнего уровня.

13.6.2 Оценка функциональной спецификации (ADV_FSP.2)

13.6.2.1 Цели

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

13.6.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора.

13.6.2.3 Действие ADV_FSP.2.1E

13.6.2.3.1 Шаг оценивания 4:ADV_FSP.2-1

ИСО/МЭК 15408-3 ADV_FSP.2.1C: *Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.*

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

Если вся функциональная спецификация является неформальной, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

13.6.2.3.2 Шаг оценивания 4:ADV_FSP.2-2

ИСО/МЭК 15408-3 ADV_FSP.2.2C: *Функциональная спецификация должна быть внутренне непротиворечивой.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о ее внутренней непротиворечивости.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.6.2.3.3 Шаг оценивания 4:ADV_FSP.2-3

ИСО/МЭК 15408-3 ADV_FSP.2.3C: *Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.*

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

Термин «внешний» относится к тому интерфейсу, который является видимым для пользователя. Внешние интерфейсы ОО — это либо непосредственно интерфейсы ФБО, либо интерфейсы не-ФБО-частей ОО. Однако и через не-ФБО-интерфейсы возможен доступ к ФБО. Эти внешние интерфейсы, которые прямо или косвенно обращаются к ФБО, совместно составляют интерфейс функций безопасности ОО (ИФБО). На рисунке 12 показан ОО, включающий в себя ФБО-части (заштрихованы) и не-ФБО-части (не заштри-

хованы). Данный ОО имеет три внешних интерфейса: интерфейс **c** — непосредственный интерфейс ФБО; интерфейс **b** — косвенный интерфейс ФБО; интерфейс **a** — интерфейс не-ФБО-частей ОО. Таким образом, интерфейсы **b** и **c** составляют ИФБО.

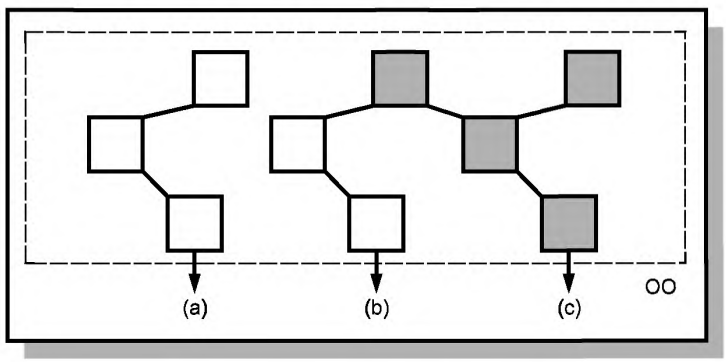


Рисунок 12 — Интерфейсы ФБО

Следует отметить, что все функции безопасности, отраженные в функциональных требованиях из ИСО/МЭК 15408-2 (или в компонентах, дополнительных по отношению к ИСО/МЭК 15408-2), будут иметь своего рода внешне видимые проявления. И хотя не обязательно все из них являются интерфейсами, через которые могут быть протестированы функции безопасности, все они до некоторой степени являются внешне видимыми, а поэтому должны быть включены в функциональную спецификацию.

Руководство по определению границ ОО см. в А.6 «Границы ОО» (приложение А).

13.6.2.3.4 Шаг оценивания 4:ADV_FSP.2-4

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

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

С другой стороны, если по отношению к ОО имеются угрозы, связанные с действиями злонамеренных пользователей или обходом (т.е. в его ЗБ включены компоненты требований из семейств FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена»), то в функциональной спецификации должны быть описаны все внешние интерфейсы , но только в объеме, достаточном для понимания их влияния на ФБО: интерфейсы функций безопасности (т.е. интерфейсы **b** и **c** на рисунке 12) должны быть описаны полностью, в то время как другие интерфейсы описывают только в объеме, достаточном для понимания того, что ФБО являются недоступными через рассматриваемый интерфейс (т.е. что интерфейс относится к типу **a**, а не типу **b** на рисунке 12). Включение компонентов требований из семейств FPT_PHP, FPT_RVM и FPT_SEP предполагает возможность некоторого влияния всех интерфейсов на ФБО. Поскольку каждый внешний интерфейс — это потенциальный интерфейс ФБО, функциональная спецификация должна содержать описание каждого интерфейса с детализацией, достаточной для того, чтобы оценщик мог сделать заключение, является ли интерфейс значимым с точки зрения безопасности.

Некоторые архитектуры позволяют без особого труда предоставить такое описание интерфейсов с достаточной степенью детализации для групп внешних интерфейсов. Например, архитектура на основе ядра такова, что все вызовы операционной системы обрабатываются программами ядра; любые вызовы, которые могли бы нарушить ПБО, запрашиваются программой, у которой есть соответствующие привилегии. Все программы, выполняемые в привилегированном режиме, должны быть включены в функциональную спецификацию. Все программы, внешние по отношению к ядру и выполняемые в непривилегированном режиме, не способны влиять на ПБО (т.е. такие программы являются интерфейсами типа **a**, а не **b** на

рисунке 12), а следовательно, могут не быть включены в функциональную спецификацию. Несмотря на то, что архитектура на основе ядра может ускорить понимание оценщиком описания интерфейсов, такая архитектура не является обязательной.

13.6.2.3.5 Шаг оценивания 4:ADV_FSP.2-5

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

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

a) все ли относящиеся к безопасности, вводимые пользователем параметры (или характеристики этих параметров) определены. Для полноты необходимо, чтобы были определены параметры, которыми пользователь не управляет непосредственно, если они могут быть использованы администраторами;

b) все ли относящиеся к безопасности режимы функционирования ОО, описанные в рассматриваемых руководствах, отражены при описании семантики в функциональной спецификации. Данное описание включает в себя идентификацию режима функционирования ОО в терминах событий и влияния каждого события. Например, если операционная система имеет развитой интерфейс файловой системы и предусматривает различные коды ошибок для разных причин неоткрытия файла по запросу (например, доступ запрещен, такого файла не существует, файл используется другим пользователем, пользователю не разрешено открывать файл после 5 ч вечера и т.д.), то в функциональной спецификации должно быть пояснено, когда файл открывается по запросу, а когда возвращается код ошибки. Недостаточно, чтобы в функциональной спецификации было указано, что файл либо открывается по запросу, либо возвращается код ошибки. В описание семантики должно быть включено описание того, каким образом требования безопасности применены к интерфейсам (например, является ли использование интерфейса потенциально подвергаемым аудиту событием, и, если да, то какая информация может быть зафиксирована);

c) все ли интерфейсы описаны для всех возможных режимов работы. Если для ФБО предусмотрено понятие привилегии, то в описании интерфейса необходимо пояснение режимов его функционирования при наличии или отсутствии привилегии;

d) вся ли информация, содержащаяся в описании относящихся к безопасности параметров, и синтаксис интерфейса непротиворечивы во всей документации.

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

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

13.6.2.3.6 Шаг оценивания 4:ADV_FSP.2-6

ИСО/МЭК 15408-3 ADV_FSP.2.4C: *Функциональная спецификация должна полностью представить ФБО.*

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение о полноте представления ФБО.

Для того чтобы оценить полноту представления ФБО, оценщик принимает во внимание краткую спецификацию ОО из ЗБ, руководства пользователя и администратора. Ни в одном из этих документов не должны быть описаны функции безопасности, которые отсутствуют в представлении ФБО в функциональной спецификации.

13.6.2.3.7 Шаг оценивания 4:ADV_FSP.2-7

ИСО/МЭК 15408-3 ADV_FSP.2.5C: *Функциональная спецификация должна включать в себя обоснование, что ФБО полностью представлены.*

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

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

13.6.2.4 Действие ADV_FSP.2.2E

13.6.2.4.1 Шаг оценивания 4:ADV_FSP.2-8

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она полным отображением функциональных требований безопасности ОО.

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

13.6.2.4.2 Шаг оценивания 4:ADV_FSP.2-9

Оценщик должен исследовать функциональную спецификацию, чтобы сделать заключение, является ли она точным отображением функциональных требований безопасности ОО.

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

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

13.6.3 Оценка проекта верхнего уровня (ADV_HLD.2)

13.6.3.1 Цели

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

13.6.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня.

13.6.3.3 Действие ADV_HLD.2.1E

13.6.3.3.1 Шаг оценивания 4:ADV_HLD.2-1

ИСО/МЭК 15408-3 ADV_HLD.2.1C: *Представление проекта верхнего уровня должно быть неформальным.*

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

Если весь проект верхнего уровня является неформальным, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

13.6.3.3.2 Шаг оценивания 4:ADV_HLD.2-2

ИСО/МЭК 15408-3 ADV_HLD.2.2C: *Проект верхнего уровня должен быть внутренне непротиворечивым.*

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

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

13.6.3.3.3 Шаг оценивания 4:ADV_HLD.2-3

ИСО/МЭК 15408-3 ADV_HLD.2.3C: *Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.*

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах подсистем.

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

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

Подсистемы, используемые для описания проекта верхнего уровня, не обязательно называются «подсистемами», но необходимо, чтобы они представляли подобный уровень декомпозиции. Например, при декомпозиции проекта могут использоваться понятия «слои» или «менеджеры».

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

13.6.3.3.4 Шаг оценивания 4:ADV_HLD.2-4

ИСО/МЭК 15408-3 ADV_HLD.2.4C: *Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.*

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

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

13.6.3.3.5 Шаг оценивания 4:ADV_HLD.2-5

ИСО/МЭК 15408-3 ADV_HLD.2.5C: *Проект верхнего уровня должен идентифицировать любые базовые аппаратные, программно-аппаратные и/или программные средства, требуемые ФБО, с представлением функций, обеспечиваемых поддерживающими механизмами защиты, реализованными в этих аппаратных, программно-аппаратных и/или программных средствах.*

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

Если проект верхнего уровня включает в себя требования безопасности для среды ИТ, которые не включены в ЗБ, или если они отличаются от требований, включенных в ЗБ, такая несогласованность должна быть учтена оценщиком при выполнении действия ADV_HLD.2.2E.

13.6.3.3.6 Шаг оценивания 4:ADV_HLD.2-6

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

Если ЗБ не содержит требования безопасности для среды ИТ, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

13.6.3.3.7 Шаг оценивания 4:ADV_HLD.2-7

ИСО/МЭК 15408-3 ADV_HLD.2.6C: *Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.*

Оценщик должен проверить, идентифицированы ли в проекте верхнего уровня интерфейсы подсистем ФБО.

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

13.6.3.3.8 Шаг оценивания 4:ADV_HLD.2-8

ИСО/МЭК 15408-3 ADV_HLD.2.7C: *Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.*

Оценщик должен проверить, идентифицировано ли в проекте верхнего уровня, какие интерфейсы подсистем ФБО являются внешне видимыми.

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

13.6.3.3.9 Шаг оценивания 4:ADV_HLD.2-9

ИСО/МЭК 15408-3 ADV_HLD.2.8C: *Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, содержится ли в нем описание назначения и методов использования всех интерфейсов каждой подсистемы, и дается ли, при необходимости, подробное описание результатов, нештатных ситуаций и сообщений об ошибках.

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

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

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

13.6.3.3.10 Шаг оценивания 4:ADV_HLD.2-10

ИСО/МЭК 15408-3 ADV_HLD.2.9C: *Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.*

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

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

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

13.6.3.4 Действие ADV_HLD.2.2E

13.6.3.4.1 Шаг оценивания 4:ADV_HLD.2-11

Оценщик должен исследовать проект верхнего уровня, чтобы сделать заключение, является ли он точным отображением функциональных требований безопасности ОО.

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

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

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

13.6.3.4.2 Шаг оценивания 4:ADV_HLD.2-12

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

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

13.6.4 Оценка представления реализации (ADV_IMP.1)

13.6.4.1 Цели

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

13.6.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) проект нижнего уровня;

c) подмножество представления реализации.

13.6.4.3 Действие ADV_IMP.1.1E

13.6.4.3.1 Шаг оценивания 4:ADV_IMP.1-1

ИСО/МЭК 15408-3 ADV_IMP.1.1C: *Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.*

Оценщик должен исследовать представление реализации, чтобы сделать заключение, определены ли однозначно в нем ФБО на таком уровне детализации, что ФБО могут быть сгенерированы без каких бы то ни было дальнейших проектных решений.

Данный шаг оценивания требует от оценщика подтвердить, что представление реализации пригодно для анализа. Оценщику следует рассмотреть процесс, необходимый для генерации ФБО из предоставленного представления реализации. Если процесс полностью определен и не требует дальнейших проектных решений (например, требуется только компиляция исходного кода или построение аппаратных средств на основе чертежей аппаратных средств), то представление реализации можно считать пригодным для анализа.

Любые используемые языки программирования должны быть полностью определены, включая однозначное определение всех операторов, а также опций компилятора, используемых для генерации объектного кода. Заключение об этом может уже быть сделано как часть подвида деятельности ALC_TAT.1 «Полностью определенные инструментальные средства разработки».

13.6.4.3.2 Шаг оценивания 4:ADV_IMP.1-2

Оценщик должен исследовать представление реализации, предоставленное разработчиком, чтобы сделать заключение, является ли оно достаточно репрезентативным.

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

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

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Делая заключение о приемлемости подмножества ФБО, оценщик решает, позволяет ли оно понять и подтвердить правильность реализации механизмов ФБО. Делая данное заключение, оценщику следует рассмотреть различные способы представления, используемые разработчиком, чтобы быть удовлетворенным репрезентативностью выбранного подмножества.

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

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

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

a) сложность проекта (если сложность проекта в рамках одного ОО варьируется, то в подмножество представления реализации следует включить какие-либо части высокой сложности);

b) требования системы оценки;

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

d) суждение оценщика относительно частей представления реализации, которые могут быть полезными для проводимого оценщиком независимого анализа уязвимостей (подвид деятельности AVA_VLA.2 «Независимый анализ уязвимостей»).

13.6.4.3.3 Шаг оценивания 4:ADV_IMP.1-3

ИСО/МЭК 15408-3 ADV_IMP.1.2C: *Представление реализации должно быть внутренне непротиворечивым.*

Оценщик должен исследовать представление реализации, чтобы сделать заключение о его внутренней непротиворечивости.

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.6.4.4 Действие ADV_IMP.1.2E

13.6.4.4.1 Шаг оценивания 4:ADV_IMP.1-4

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

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

Остальные части подмножества представления реализации, если таковые имеются, могут быть проигнорированы, потому что они не связаны с какими-либо функциональными требованиями безопасности ОО, поддерживаемыми подмножеством представления реализации. Тем не менее, оценщик не должен пропустить какие-нибудь части, которые играют косвенную роль, неважно насколько малую, в поддержке функций безопасности ОО. Например, в типичных операционных системах исходный код для частей ядра может не играть непосредственно какую-либо роль в поддержке функции безопасности ОО, но способен помешать правильному функционированию тех частей ядра, которые играют такую роль непосредственно. Если в подмножестве предоставленного представления реализации такие части обнаружены, они должны быть оценены на предмет отсутствия с их стороны вмешательства в функционирование тех частей, для которых в ЗБ требуется отсутствие вмешательства. Данная оценка не потребует того же уровня детализации исследования, что и для тех частей представления реализации, которые играют более непосредственную роль в поддержке функций безопасности ОО.

13.6.5 Оценка проекта нижнего уровня (ADV_LLD.1)

13.6.5.1 Цели

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

13.6.5.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) проект нижнего уровня.

13.6.5.3 Действие ADV_LLD.1.1E

13.6.5.3.1 Шаг оценивания 4:ADV_LLD.1-1

ИСО/МЭК 15408-3 ADV_LLD.1.1C: *Представление проекта нижнего уровня должно быть неформальным.*

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

Если весь проект нижнего уровня является неформальным, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

13.6.5.3.2 Шаг оценивания 4:ADV_LLD.1-2

ИСО/МЭК 15408-3 ADV_LLD.1.2C: *Проект нижнего уровня должен быть внутренне непротиворечивым.*

Оценщик должен исследовать представление проекта нижнего уровня, чтобы сделать заключение о его внутренней непротиворечивости.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.6.5.3.3 Шаг оценивания 4:ADV_LLD.1-3

ИСО/МЭК 15408-3 ADV_LLD.1.3C: *Проект нижнего уровня должен содержать описание ФБО в терминах модулей.*

Оценщик должен исследовать проект нижнего уровня, чтобы сделать заключение, описана ли структура ФБО в терминах модулей.

Применительно к проекту нижнего уровня термин «модуль» использован в соответствующем ИСО/МЭК 15408 для обозначения менее абстрактной сущности, чем подсистема. Это означает, что проект нижнего уровня содержит больше подробностей относительно не только цели каждого модуля, но также и относительно способа достижения модулем своей цели. В идеале в проекте нижнего уровня должна быть представлена вся информация, необходимая для реализации описанных в нем модулей. Последующие шаги оценивания в этом подвиде деятельности требуют проведения конкретного анализа, чтобы сделать заключение, достаточен ли уровень детализации проекта нижнего уровня. На данном шаге оценивания оценщику достаточно верифицировать четкость и однозначность идентификации каждого модуля.

13.6.5.3.4 Шаг оценивания 4:ADV_LLD.1-4

ИСО/МЭК 15408-3 ADV_LLD.1.4C: *Проект нижнего уровня должен содержать описание назначения каждого модуля.*

Оценщик должен исследовать проект нижнего уровня, чтобы сделать заключение, содержит ли он описание назначения каждого модуля.

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

13.6.5.3.5 Шаг оценивания 4:ADV_LLD.1-5

ИСО/МЭК 15408-3 ADV_LLD.1.5C: *Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.*

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

В целях проведения такого анализа рассматривают два способа взаимодействия модулей:

a) предоставление услуг друг другу;

b) совместную работу для поддержки функций безопасности.

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

13.6.5.3.6 Шаг оценивания 4:ADV_LLD.1-6

ИСО/МЭК 15408-3 ADV_LLD.1.6C: *Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.*

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

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

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

13.6.5.3.7 Шаг оценивания 4:ADV_LLD.1-7

ИСО/МЭК 15408-3 ADV_LLD.1.7C: *Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.*

Оценщик должен проверить, идентифицированы ли в проекте нижнего уровня интерфейсы модулей ФБО.

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

13.6.5.3.8 Шаг оценивания 4:ADV_LLD.1-8

ИСО/МЭК 15408-3 ADV_LLD.1.8C: *Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.*

Оценщик должен проверить, идентифицировано ли в проекте нижнего уровня, какие интерфейсы модулей ФБО являются внешне видимыми.

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

13.6.5.3.9 Шаг оценивания 4:ADV_LLD.1-9

ИСО/МЭК 15408-3 ADV_LLD.1.9C: *Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.*

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

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

Данный шаг оценивания может быть выполнен совместно с проведением оценщиком независимого анализа уязвимостей (подвид деятельности AVA_VLA.2).

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

13.6.5.3.10 Шаг оценивания 4:ADV_LLD.1-10

ИСО/МЭК 15408-3 ADV_LLD.1.10C: *Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.*

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

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

13.6.5.4 Действие ADV_LLD.1.2E

13.6.5.4.1 Шаг оценивания 4:ADV_LLD.1-11

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

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

a) спецификации интерфейсов согласованы с описанием назначения модуля;

b) спецификации интерфейсов согласованы с их использованием другими модулями;

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

13.6.5.4.2 Шаг оценивания 4:ADV_LLD.1-12

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

Оценщик удостоверяется, что все функциональные требования из ЗБ отображаются на соответствующие разделы проекта нижнего уровня. Соответствующее заключение следует сделать совместно с выполнением подвида деятельности ADV_RCR.1 «Неформальная демонстрация соответствия».

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

13.6.6 Оценка соответствия представлений (ADV_RCR.1)

13.6.6.1 Цели

Цель данного подвида деятельности — сделать заключение, правильно ли и полностью ли разработчик реализовал требования ЗБ, функциональной спецификации, проекта верхнего уровня и проекта нижнего уровня в представлении реализации.

13.6.6.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) проект нижнего уровня;

e) подмножество представления реализации;

f) материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией;

g) материалы анализа соответствия между функциональной спецификацией и проектом верхнего уровня;

h) материалы анализа соответствия между проектом верхнего уровня и проектом нижнего уровня;

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

13.6.6.3 Действие ADV_RCR.1.1E

13.6.6.3.1 Шаг оценивания 4:ADV_RCR.1-1

ИСО/МЭК 15408-3 ADV_RCR.1.1C: *Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.*

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

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

Оценщик анализирует соответствие между функциями безопасности ОО в краткой спецификации ОО и в функциональной спецификации. Оценщик проверяет непротиворечивость и точность данного соответствия. Там, где материалы анализа соответствия указывают на связь между описанием функции безопасности в краткой спецификации ОО и описанием интерфейса в функциональной спецификации, оценщик верифицирует, что описанные функциональные возможности безопасности являются одними и теми же. Если функции безопасности, описанные в краткой спецификации ОО, точно и полно представлены в описаниях соответствующих интерфейсов, рассматриваемый шаг оценивания считают выполненным.

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

13.6.6.3.2 Шаг оценивания 4:ADV_RCR.1-2

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

Оценщик использует материалы анализа соответствия, функциональную спецификацию и проект верхнего уровня, чтобы удостовериться в возможности отобразить каждую функцию безопасности, идентифицированную в функциональной спецификации, на какую-либо подсистему ФБО, описанную в проекте верхнего уровня. Для каждой функции безопасности материалы соответствия указывают, какие подсистемы ФБО предполагают поддержку данной функции безопасности. Оценщик верифицирует, что проект верхнего уровня содержит описание корректной реализации каждой функции безопасности.

13.6.6.3.3 Шаг оценивания 4:ADV_RCR.1-3

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

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

13.6.6.3.4 Шаг оценивания 4:ADV_RCR.1-4

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

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

13.6.7 Оценка моделирования политики безопасности ОО (ADV_SPM.1)

13.6.7.1 Цели

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

13.6.7.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) модель политики безопасности ОО;

d) руководство пользователя;

e) руководство администратора.

13.6.7.3 Действие ADV_SPM.1.1E

13.6.7.3.1 Шаг оценивания 4:ADV_SPM.1-1

ИСО/МЭК 15408-3 ADV_SPM.1.1C: *Модель ПБО должна быть неформальной.*

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

Если вся модель политики безопасности ОО является неформальной, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

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

13.6.7.3.2 Шаг оценивания 4:ADV_SPM.1-2

ИСО/МЭК 15408-3 ADV_SPM.1.2C: *Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.*

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

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

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

Если ЗБ не содержит явных политик ФБ (вследствие того, что компоненты требований ни из семейства FDP_ACC, ни из семейства FDP_IFC не включены в ЗБ), то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

13.6.7.3.3 Шаг оценивания 4:ADV_SPM.1-3

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

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

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

Если ЗБ не содержит таких подразумеваемых правил, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

13.6.7.3.4 Шаг оценивания 4:ADV_SPM.1-4

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

Правила и характеристики модели политики безопасности ОО описывают состояние безопасности ОО. Вероятно, что такое описание содержится в оцененном ЗБ сертифицированного ОО. Для того чтобы

данное описание было признано четко сформулированным, в нем должны быть определено понятие безопасности для рассматриваемого ОО, идентифицированы атрибуты безопасности сущностей, находящихся под управлением ОО, а также идентифицированы действия ОО, которые изменяют значения этих атрибутов. Например, если в политике безопасности предпринята попытка учесть вопросы целостности данных, то в модели политики безопасности ОО должны быть:

a) определено понятие целостности для рассматриваемого ОО;

b) идентифицированы типы данных, для которых ОО поддерживает целостность;

c) идентифицированы сущности, которые могут модифицировать данные указанных типов;

d) идентифицированы правила, которые должны быть выполнены при модификации данных.

13.6.7.3.5 Шаг оценивания 4:ADV_SPM.1-5

ИСО/МЭК 15408-3 ADV_SPM.1.3C: *Модель ПБО должна включать в себя обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.*

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

Делая заключение о непротиворечивости, оценщик верифицирует, что согласно обоснованию описание каждого правила или характеристики в модели политики безопасности ОО точно отражает предназначение политик ФБ. Например, если политикой безопасности установлено, что управление доступом необходимо на уровне отдельных пользователей, то модель политики безопасности ОО, описывающая безопасный режим функционирования ОО применительно к управлению группами пользователей, не будет признана согласованной с политикой безопасности. Аналогично, если политикой безопасности установлено, что управление доступом необходимо на уровне групп пользователей, то модель политики безопасности ОО, описывающая безопасный режим функционирования ОО применительно к управлению отдельными пользователями, также не будет считаться согласованной с политикой безопасности.

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

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.6.7.3.6 Шаг оценивания 4:ADV_SPM.1-6

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

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

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

13.6.7.3.7 Шаг оценивания 4:ADV_SPM.1-7

ИСО/МЭК 15408-3 ADV_SPM.1.4C: *Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.*

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

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

13.6.7.3.8 Шаг оценивания 4:ADV_SPM.1-8

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

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.7 Вид деятельности «Руководства»

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

13.7.1 Замечания по применению

Вид деятельности «Руководства» применяют к тем функциям и интерфейсам, которые связаны с безопасностью ОО. Безопасная конфигурация ОО должна быть описана в ЗБ.

13.7.2 Оценка руководства администратора (AGD_ADM.1)

13.7.2.1 Цели

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

13.7.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска;

g) документация определения жизненного цикла.

13.7.2.3 Замечания по применению

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

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

13.7.2.4 Действие AGD_ADM.1.1E

13.7.2.4.1 Шаг оценивания 4:AGD_ADM.1-1

ИСО/МЭК 15408-3 AGD_ADM.1.1C: *Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описаны ли в нем относящиеся к администрированию функции безопасности и интерфейсы, доступные администратору ОО.

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

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

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

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

b) параметры, устанавливаемые администратором, их допустимые значения и значения по умолчанию;

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

13.7.2.4.2 Шаг оценивания 4:AGD_ADM.1-2

ИСО/МЭК 15408-3 AGD_ADM.1.2C: *Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, описан ли в нем безопасный способ администрирования ОО.

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

13.7.2.4.3 Шаг оценивания 4:AGD_ADM.1-3

ИСО/МЭК 15408-3 AGD_ADM.1.3C: *Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство администратора, чтобы сделать заключение, содержит ли оно предупреждения относительно функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

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

13.7.2.4.4 Шаг оценивания 4:AGD_ADM.1-4

ИСО/МЭК 15408-3 AGD_ADM.1.4C: *Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство администратора должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

13.7.2.4.5 Шаг оценивания 4:AGD_ADM.1-5

ИСО/МЭК 15408-3 AGD_ADM.1.5C: *Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.*

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

Для каждого параметра безопасности в руководстве администратора должны быть описаны предназначение параметра, допустимые значения параметра и его значение по умолчанию, а также безопасные и небезопасные настройки этих параметров как по отдельности, так и в сочетании.

13.7.2.4.6 Шаг оценивания 4:AGD_ADM.1-6

ИСО/МЭК 15408-3 AGD_ADM.1.6C: *Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.*

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

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

13.7.2.4.7 Шаг оценивания 4:AGD_ADM.1-7

ИСО/МЭК 15408-3 AGD_ADM.1.7C: *Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.7.2.4.8 Шаг оценивания 4:AGD_ADM.1-8

ИСО/МЭК 15408-3 AGD_ADM.1.8C: *Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

13.7.3 Оценка руководства пользователя (AGD_USR.1)

13.7.3.1 Цели

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

13.7.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) руководство пользователя;

e) руководство администратора;

f) процедуры безопасной установки, генерации и запуска.

13.7.3.3 Замечания по применению

В ЗБ могут быть определены несколько различных ролей или групп пользователей, опознаваемых объектом оценки и взаимодействующих с ФБО. Возможности этих ролей и связанные с ними привилегии описывают в ЗБ в классе FMT «Управление безопасностью». Различные роли и группы пользователей должны быть рассмотрены в руководстве пользователя.

13.7.3.4 Действие AGD_USR.1.1E

13.7.3.4.1 Шаг оценивания 4:AGD_USR.1-1

ИСО/МЭК 15408-3 AGD_USR.1.1C: *Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.*

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

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

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

13.7.3.4.2 Шаг оценивания 4:AGD_USR.1-2

ИСО/МЭК 15408-3 AGD_USR.1.2C: *Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.*

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

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

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

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

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

b) параметры, устанавливаемые пользователем, их допустимые значения и значения по умолчанию;

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

13.7.3.4.3 Шаг оценивания 4:AGD_USR.1-3

ИСО/МЭК 15408-3 AGD_USR.1.3C: *Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.*

Оценщик должен исследовать руководство пользователя, чтобы сделать заключение, содержит ли оно предупреждения относительно доступных пользователю функций и привилегий, которые необходимо контролировать в безопасной среде эксплуатации.

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

В руководстве пользователя должны быть идентифицированы функции и привилегии, которые могут быть применены, требуемые для них типы команд и объяснения таких команд. В руководстве пользователя должны быть приведены предупреждающие сообщения относительно использования функций и привилегий, подлежащих контролю. Предупреждающие сообщения должны быть связаны с ожидаемыми последствиями, возможными побочными эффектами и возможным взаимодействием с другими функциями и привилегиями.

13.7.3.4.4 Шаг оценивания 4:AGD_USR.1-4

ИСО/МЭК 15408-3 AGD_USR.1.4C: *Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.*

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

Предположения относительно действий пользователя могут быть описаны более подробно при изложении среды безопасности ОО в ЗБ. Однако в руководство пользователя должна быть включена только та информация, которая относится к безопасной эксплуатации ОО.

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

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

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

13.7.3.4.5 Шаг оценивания 4:AGD_USR.1-5

ИСО/МЭК 15408-3 AGD_USR.1.5C: *Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.*

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

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

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.7.3.4.6 Шаг оценивания 4:AGD_USR.1-6

ИСО/МЭК 15408-3 AGD_USR.1.6C: *Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.*

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

Если ЗБ не содержит требования безопасности ИТ для среды ИТ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

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

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

13.8 Вид деятельности «Поддержка жизненного цикла»

Вид деятельности «Поддержка жизненного цикла» предназначен для определения достаточности процедур, применяемых разработчиком во время разработки и сопровождения ОО. Эти процедуры включают в себя меры безопасности во время разработки ОО, модель жизненного цикла, применяемую разработчиком, и инструментальные средства, используемые разработчиком на протяжении жизненного цикла ОО.

Процедуры безопасности разработки предназначены для защиты ОО и связанной с ним информации о проекте от вмешательства или раскрытия. Вмешательство в процесс разработки может позволить преднамеренно внести уязвимости в ОО. Раскрытие информации о проекте может облегчить использование уязвимостей. Адекватность рассматриваемых процедур будет зависеть от свойств ОО и процесса его разработки.

Плохое управление разработкой и сопровождением ОО может привести к уязвимостям в реализации. Соответствие определенной модели жизненного цикла может способствовать улучшению мер управления в этих областях.

Использование полностью определенных инструментальных средств разработки помогает удостовериться в том, что уязвимости не были непреднамеренно внесены в процессе уточнения ФБО.

13.8.1 Оценка безопасности разработки (ALC_DVS.1)

13.8.1.1 Цели

Цель данного подвида деятельности — сделать заключение, являются ли меры и средства контроля безопасности в среде разработки достаточными для обеспечения конфиденциальности и целостности проекта и реализации ОО. Это необходимо для обеспечения того, чтобы безопасная эксплуатация ОО не была скомпрометирована.

13.8.1.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация по безопасности разработки.

Кроме того, оценщику может понадобиться исследование других поставок, чтобы сделать заключение о том, что меры и средства контроля безопасности полностью определены и их применяют. В частности, оценщику может понадобиться исследование документации разработчика по управлению конфигурацией (исходные данные подвидов деятельности ACM_CAP.4 «Поддержка генерации, процедуры приемки» и ACM_SCP.2 «Охват УК отслеживания проблем»). Также требуется свидетельство применения процедур.

13.8.1.3 Действие ALC_DVS.1.1E

13.8.1.3.1 Шаг оценивания 4:ALC_DVS.1-1

ИСО/МЭК 15408-3 ALC_DVS.1.1C: *Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.*

Оценщик должен исследовать документацию по безопасности разработки, чтобы сделать заключение, содержит ли она подробное описание всех используемых в среде разработки мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта и реализации ОО.

Оценщик определяет, какая информация из ЗБ требуется в первую очередь при вынесении заключения о необходимой защите, особенно из разделов ЗБ об угрозах, политике безопасности организации и предположениях, хотя такая информация может и не быть представлена в явном виде. Изложение в ЗБ целей безопасности для среды также может быть полезно в этом отношении.

Если в ЗБ не имеется такой информации в явном виде, оценщик должен принять решение о необходимых мерах, основываясь на рассмотрении предполагаемой среды для ОО. В тех случаях, когда меры

разработчика признаны недостаточными, необходимо, чтобы было представлено четкое и логическое обоснование для оценки уязвимостей, потенциально пригодных для использования.

При исследовании документации оценщик рассматривает следующие типы мер безопасности:

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

b) процедурные, например распространяющиеся:

- на предоставление доступа к среде разработки или к конкретным объектам среды, таким как оборудование разработки,
- на отмену прав доступа лиц при их исключении из состава разработчиков,
- на передачу защищаемого материала из среды разработки,
- на встречу и сопровождение посетителей среды разработки,
- на роли и обязанности по обеспечению непрерывного применения мер безопасности и обнаружения нарушений безопасности;

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

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

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

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

13.8.1.3.2 Шаг оценивания 4:ALC_DVS.1-2

Оценщик должен исследовать политики обеспечения конфиденциальности и целостности при разработке, чтобы сделать заключение о достаточности применяемых мер безопасности.

При рассмотрении политик учитывают следующее:

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

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

Оценщику следует сделать заключение, описаны ли эти политики в документации по безопасности разработки, совместимы ли применяемые меры безопасности с политиками, являются ли они достаточно полными.

Необходимо отметить, что процедуры управления конфигурацией способствуют защите целостности ОО, и оценщику следует избегать частичного перекрытия с шагами оценивания, проводимыми в рамках подвида деятельности ACM_CAP «Возможности УК». Например, документация УК может описывать процедуры безопасности, необходимые для контроля ролей или лиц, которым следует предоставить доступ к среде разработки и которые могут модифицировать ОО.

Тогда как требования ACM_CAP зафиксированы, требования для ALC_DVS «Безопасность разработки», предписывающие только необходимые меры, зависят от типа ОО и от информации, которая может быть представлена в разделе ЗБ «Среда безопасности». Например, ЗБ может идентифицировать политику безопасности организации, в которой требуется наличие формы допуска у персонала разработчиков ОО. Тогда оценщику в ходе выполнения данного подвида деятельности необходимо сделать заключение, была ли применена такая политика.

13.8.1.3.3 Шаг оценивания 4:ALC_DVS.1-3

ИСО/МЭК 15408-3 ALC_DVS.1.2C: *Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.*

Оценщик должен проверить документацию по безопасности разработки, чтобы сделать заключение, сформировано ли документальное свидетельство в результате применения процедур.

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

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.8.1.4 Действие ALC_DVS.1.2E

13.8.1.4.1 Шаг оценивания 4:ALC_DVS.1-4

Оценщик должен исследовать документацию по безопасности разработки и связанные с ней свидетельства, чтобы сделать заключение, применены ли меры безопасности.

На этом шаге оценивания от оценщика требуется сделать заключение, применены ли меры безопасности, описанные в документации по безопасности разработки, таким образом, при котором целостность ОО и конфиденциальность связанной с ним документации адекватно защищены. Например, данное заключение могло бы быть сделано по результатам исследования представленных документальных свидетельств. Документальные свидетельства следует дополнить непосредственным ознакомлением со средой разработки. Непосредственное ознакомление со средой разработки предоставит оценщику возможность:

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

b) исследовать документальные свидетельства применения процедур;

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

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

Руководство по посещению объектов см. в А.5 «Посещение объектов» (приложение А).

13.8.2 Оценка определения жизненного цикла (ALC_LCD.1)

13.8.2.1 Цели

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

13.8.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) документация определения жизненного цикла.

13.8.2.3 Действие ALC_LCD.1.1E

13.8.2.3.1 Шаг оценивания 4:ALC_LCD.1-1

ИСО/МЭК 15408-3 ALC_LCD.1.1C: *Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.*

Оценщик должен исследовать документированное описание используемой модели жизненного цикла, чтобы сделать заключение, распространяется ли она на процессы разработки и сопровождения ОО.

Модель жизненного цикла должна распространяться на процедуры, инструментальные средства и методы, используемые при разработке и сопровождении ОО. Описание модели жизненного цикла должно включать в себя информацию о процедурах, инструментальных средствах и методах, используемых разработчиком (например, при проектировании, кодировании, тестировании, исправлении ошибок). В ней должно содержаться описание общей структуры управления применением процедур (например, идентификация и описание персональной ответственности за каждую из процедур, требуемых в процессе разработки и сопровождения ОО согласно модели жизненного цикла). ALC_LCD.1 «Определение модели жизненного цикла разработчиком» не содержит требования соответствия используемой модели какой-либо стандартизованной модели жизненного цикла.

13.8.2.3.2 Шаг оценивания 4:ALC_LCD.1-2

ИСО/МЭК 15408-3 ALC_LCD.1.2C: *Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.*

Оценщик должен исследовать модель жизненного цикла, чтобы сделать заключение, будет ли использование процедур, инструментальных средств и методов, описанных в модели жизненного цикла, оказывать необходимое положительное влияние на разработку и сопровождение ОО.

Информация, представленная в модели жизненного цикла, дает оценщику определенную уверенность в том, что принятые процедуры разработки и сопровождения минимизируют вероятность недостатков безопасности. Например, если в модели жизненного цикла содержится описание процесса проверки, но не

предусмотрено протоколирование внесения изменений в компоненты, то оценщик будет менее уверен, что в ОО не будут внесены ошибки. Оценщик может достичь большей уверенности, сравнивая описание модели со своим пониманием процесса разработки, полученным при выполнении других своих действий, относящихся к анализу процесса разработки ОО (например, тех действий, на которые распространяется вид деятельности АСМ). Выявленным недостаткам в модели жизненного цикла следует уделить особое внимание, если можно ожидать, что они приведут к случайному или преднамеренному внесению ошибок в ОО.

ИСО/МЭК 15408 не предписывает какой-либо конкретный подход к разработке; следует оценить каждый подход по существу. Например, такие подходы к проектированию, как спиральный, быстрого макетирования или каскадный, могут быть использованы для создания высококачественного ОО, если они применимы в контролируемой среде.

13.8.3 Оценка инструментальных средств и методов (ALC_TAT.1)

13.8.3.1 Цели

Цель данного подвида деятельности — сделать заключение, использовал ли разработчик полностью определенные инструментальные средства разработки [например, языки программирования или системы автоматизированного проектирования (САПР)], которые дают непротиворечивые и предсказуемые результаты.

13.8.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация инструментальных средств разработки;

b) подмножество представления реализации.

13.8.3.3 Замечания по применению

Эта работа может быть выполнена в сочетании с подвидом деятельности ADV_IMP.1 «Подмножество реализации ФБО», а именно, в части, касающейся определения используемых характеристик инструментальных средств, которые влияют на объектный код (например, опции компиляции).

13.8.3.4 Действие ALC_TAT.1.1E

13.8.3.4.1 Шаг оценивания 4:ALC_TAT.1-1

ИСО/МЭК 15408-3 ALC_TAT.1.1C: *Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.*

Оценщик должен исследовать представленную документацию инструментальных средств разработки, чтобы сделать заключение, все ли инструментальные средства разработки полностью определены.

Например, полностью определенными можно считать те языки, компиляторы или САПР, которые соответствуют общепризнанным стандартам, таким как стандарты ИСО. Полностью определенным языком является тот, для которого имеется четкое и полное описание его синтаксиса и детальное описание семантики каждой из его конструкций.

13.8.3.4.2 Шаг оценивания 4:ALC_TAT.1-2

ИСО/МЭК 15408-3 ALC_TAT.1.2C: *Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.*

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

В документации инструментальных средств разработки (например, в спецификациях языка программирования и в руководствах пользователя) должны быть охвачены все конструкции, используемые в представлении реализации ОО, и для каждой такой конструкции предоставлено четкое и однозначное определение предназначения и результата выполнения этой конструкции. Эта работа может быть выполнена в сочетании с исследованием оценщиком представления реализации, выполняемого в рамках подвида деятельности ADV_IMP.1 «Подмножество реализации ФБО». Главные усилия оценщика должны быть направлены на выяснение того, действительно ли документация достаточно ясна для понимания представления реализации. Например, в документации не следует предполагать, что пользователь является экспертом по примененному языку программирования.

Ссылка на использование документированного стандарта — приемлемый подход для удовлетворения этого требования при условии, что данный стандарт доступен для оценщика. Любые отклонения от этого стандарта должны быть задокументированы.

Важная проверка состоит в том, может ли оценщик понять исходный код ОО при выполнении анализа исходного кода, включенного в подвид деятельности «Представление реализации» (ADV_IMP).

Несмотря на это, для поиска проблемных областей может быть использован следующий проверочный список:

a) на естественном языке такие фразы, как «цель данной конструкции не определена» и такие термины, как «зависит от реализации» или «ошибочный» могут указывать на плохо определенные области;

b) псевдонимы (позволяют ссылаться на одну и ту же часть памяти различными способами) — общий источник проблем неоднозначности;

c) обработка исключительных событий (например, что должно происходить после исчерпания свободной памяти или переполнения стека) часто плохо определена.

Большинство широко используемых языков, как бы хорошо они ни были разработаны, могут иметь некоторые проблематичные конструкции. Если язык реализации в целом хорошо определен, но все же существуют некоторые проблематичные конструкции, то до окончания экспертизы исходных текстов следует вынести неокончательный вердикт.

Оценщику в процессе экспертизы исходных кодов следует верифицировать, что любое использование проблематичных конструкций не вносит уязвимости. Оценщику следует также удостовериться, что конструкции, не предусмотренные соответствующим стандартом, не используются.

13.8.3.4.3 Шаг оценивания 4:ALC_TAT.1-3

ИСО/МЭК 15408-3 ALC_TAT.1.3C: *Документация инструментальных средств разработки должна однозначно определить значения всех опций, обусловленных реализацией.*

Оценщик должен исследовать документацию инструментальных средств, чтобы сделать заключение, однозначно ли определены в ней значения всех опций, обусловленных реализацией.

В документацию инструментальных средств разработки программного обеспечения должны быть включены определения опций, обусловленных реализацией, которые могут повлиять на содержание выполняемого кода, и тех, которые отличаются от стандарта используемого языка. В случаях, когда оценщику предоставлен исходный код, ему также должна быть предоставлена информация по используемым опциям компиляции и сборки.

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

13.9 Вид деятельности «Тестирование»

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

13.9.1.Замечания по применению

Объем и состав подмножества тестов оценщика зависят от нескольких факторов, рассматриваемых в подвидах деятельности, связанных с независимым тестированием (ATE_IND.2 «Выборочное независимое тестирование»). Один из таких факторов, оказывающих влияние на состав подмножества тестов, — это известные из общедоступных источников слабые места, к информации о которых оценщику необходимо получить доступ (например, в рамках системы оценки).

В ИСО/МЭК 15408 для повышения гибкости применения компонентов семейств вопросы покрытия тестами и глубины тестирования рассмотрены отдельно от функциональных тестов. Тем не менее, требования соответствующих семейств предназначены для совместного применения в целях подтверждения, что ФБО выполняются согласно их спецификации. Такая тесная связь семейств привела к некоторому дублированию работы оценщика по подвидам деятельности. Настоящие замечания по применению позволяют минимизировать повторения текста при описании подвидов деятельности одного и того же вида деятельности и ОУД.

13.9.1.1 Понимание ожидаемого режима функционирования ОО

Прежде чем адекватность тестовой документации может быть надлежащим образом оценена и прежде чем могут быть созданы новые тесты, оценщику необходимо понять желательный ожидаемый режим выполнения функций безопасности применительно к требованиям, которым они должны удовлетворять.

Оценщик может предпочесть анализировать функции безопасности ФБО поочередно. Для каждой функции безопасности оценщик исследует конкретное требование ЗБ и соответствующие части функциональной спецификации, проекта верхнего уровня и руководств для понимания ожидаемого режима функционирования ОО.

Понимая ожидаемый режим функционирования ОО, оценщик исследует план тестирования, чтобы определить подход к тестированию. В большинстве случаев подход к тестированию будет предусматривать инициирование выполнения некоторой функции безопасности через внешние или внутренние интерфейсы и наблюдение ее реакции. Тем не менее, в некоторых случаях функция безопасности не может быть адекватно протестирована через интерфейс (как, например, в случае с тестированием функциональных возможностей защиты остаточной информации); в подобных случаях необходимо использовать другой способ.

13.9.1.2 Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности

В тех случаях, когда практически нецелесообразно или несоразмерно осуществлять тестирование через интерфейс, в плане тестирования следует определить альтернативный подход к верификации ожидаемого режима выполнения. Сделать заключение о пригодности альтернативного подхода — обязанность оценщика. Оценивая пригодность альтернативных подходов, следует учесть, что:

a) приемлемым альтернативным подходом является анализ представления реализации для заключения, что требуемый режим функционирования будет демонстрироваться ОО. Это может означать экспертизу кода для программного ОО или, возможно, экспертизу фотошаблона (маски) микросхем для аппаратного ОО;

b) приемлемым является использование свидетельства помодульного или интегрированного тестирования разработчиком, даже если это несоизмеримо с представленным на оценку проектом нижнего уровня или реализацией. Если при верификации ожидаемого режима выполнения функции безопасности используется свидетельство помодульного или интегрированного тестирования разработчиком, следует внимательно отнестись к подтверждению того, что данное свидетельство тестирования отражает текущую реализацию ОО. Если конкретная подсистема или модули подверглись изменению после проведения тестирования, то обычно потребуется свидетельство, что изменения были отслежены и учтены в ходе анализа или проведения последующего тестирования.

Дополнительные по отношению к тестированию усилия с использованием альтернативных подходов следует предпринять только тогда, когда и разработчик, и оценщик сделают заключение, что не существует других практичных способов проведения тестирования ожидаемого режима выполнения некоторой функции безопасности. Такая альтернатива позволяет разработчику минимизировать затраты (времени и/или денег) на тестирование при описанных выше обстоятельствах; она не предназначена для того, чтобы дать оценщику большую свободу требовать произвольную дополнительную информацию относительно ОО, а также для того, чтобы заменить тестирование.

13.9.1.3 Верификация адекватности тестов

Для тестов необходимо заранее установить требуемые начальные условия их выполнения. Они могут быть определены через параметры, которые должны быть установлены, или через упорядочение тестов в тех случаях, когда завершение одного теста устанавливает необходимые предварительные условия выполнения другого теста. Оценщик должен сделать заключение о полноте предварительных условий выполнения тестов и их приемлемости с точки зрения того, что они не приведут к смещению наблюдаемых результатов тестирования по отношению к ожидаемым результатам тестирования.

Шаги тестирования и ожидаемые результаты тестирования определяют действия и параметры, относящиеся к интерфейсам, а также способ верификации ожидаемых результатов и что они собой представляют. Оценщик должен сделать заключение о согласованности шагов тестирования и ожидаемых результатов тестирования с функциональной спецификацией и проектом верхнего уровня. Тесты должны верифицировать задокументированный в этих спецификациях режим выполнения. Это означает, что для каждой характеристики режима выполнения функции безопасности, явным образом описанной в функциональной спецификации и проекте верхнего уровня, должны быть тесты и описание ожидаемых результатов тестирования, чтобы верифицировать данный режим выполнения.

Несмотря на то, что все ФБО должны быть протестированы разработчиком, исчерпывающее тестирование их интерфейсов не требуется. Основная цель данного вида деятельности состоит в том, чтобы сделать заключение о достаточности тестирования каждой функции безопасности на соответствие заявленным в функциональной спецификации и проекте верхнего уровня режимам выполнения. Процедуры тестирования обеспечат понимание того, каким образом разработчиком в ходе тестирования были опробованы функции безопасности. Оценщик будет использовать данную информацию при разработке дополнительных тестов для независимого тестирования ОО.

13.9.2 Оценка покрытия (ATE_COV.2)

13.9.2.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли тестирование (как это документально зафиксировано) достаточным, чтобы установить, что ФБО были систематическим методом протестированы на соответствие функциональной спецификации.

13.9.2.2 Исходные данные

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) материалы анализа покрытия тестами.

13.9.2.3 Действие ATE_COV.2.1E

13.9.2.3.1 Шаг оценивания 4:ATE_COV.2-1

ИСО/МЭК 15408-3 ATE_COV.2.1C: *Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.*

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение, является ли точным соответствие между тестами, идентифицированными в тестовой документации, и функциональной спецификацией.

Демонстрация соответствия может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов, достаточно наличия такого отображения. В других случаях может потребоваться некоторое обоснование (на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

На рисунке 13 отражена концептуальная структура соответствия между функциями безопасности, описанными в функциональной спецификации, и тестами, выделенными в тестовой документации для тестирования этих функций. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями тестов или общей целью выполняемого теста.

Идентификация тестов и функций безопасности, представленных в материалах анализа покрытия тестами, должна быть однозначной. Материалы анализа покрытия тестами позволят оценщику сопоставить идентифицированные тесты с тестовой документацией, а тестируемые функции безопасности — с функциональной спецификацией.

13.9.2.3.2 Шаг оценивания 4:ATE_COV.2-2

Оценщик должен исследовать план тестирования, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих замечаниях по применению:

a) «Понимание ожидаемого режима функционирования ОО»;

b) «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

13.9.2.3.3 Шаг оценивания 4:ATE_COV.2-3

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к функциональной спецификации, можно найти в замечаниях по применению «Верификация адекватности тестов».

13.9.2.3.4 Шаг оценивания 4:ATE_COV.2-4

ИСО/МЭК 15408-3 ATE_COV.2.2C: *Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.*

Оценщик должен исследовать материалы анализа покрытия тестами, чтобы сделать заключение о полноте соответствия между ФБО, описанными в функциональной спецификации, и тестами, идентифицированными в тестовой документации.

Все функции безопасности и интерфейсы, которые описаны в функциональной спецификации, должны быть представлены в материалах анализа покрытия тестами и сопоставлены с тестами для утверждения о

полноте, хотя исчерпывающее тестирование интерфейсов спецификации не требуется. Как показано на рисунке 13, для всех функций безопасности имеются относящиеся к ним тесты, а следовательно, в данном примере продемонстрировано полное покрытие тестами. Неполнота покрытия была бы очевидна, если бы некоторая функция безопасности была идентифицирована в материалах анализа покрытия тестами, но никакие тесты не могли быть к ней отнесены.

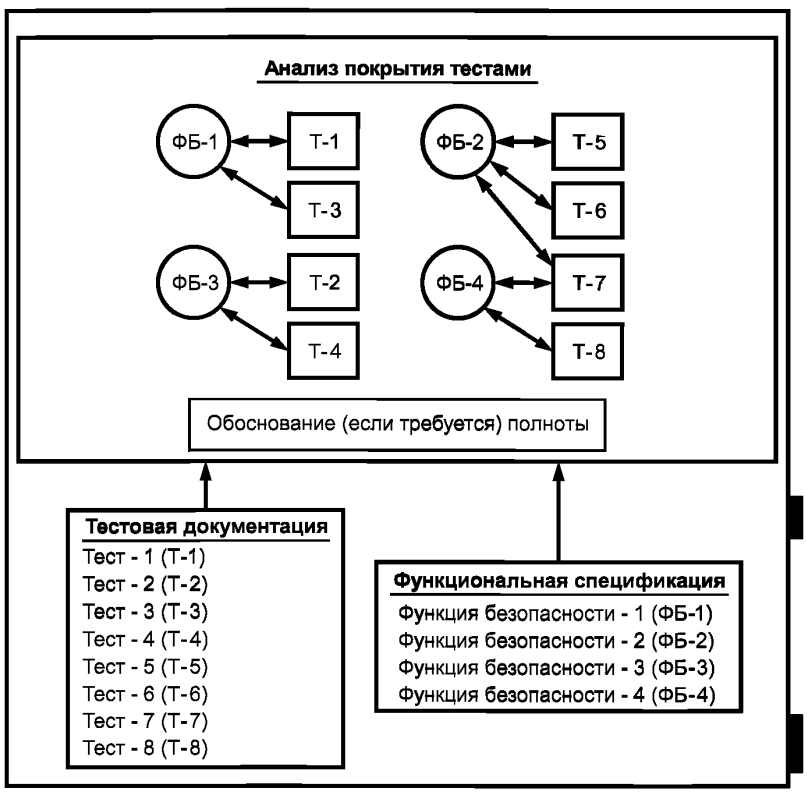


Рисунок 13 — Концептуальная структура анализа покрытия тестами

13.9.3 Оценка глубины (ATE_DPT.1)

13.9.3.1 Цели

Цель данного подвида деятельности — сделать заключение, тестировал ли разработчик ФБО на соответствие проекту верхнего уровня.

13.9.3.2 Исходные данные

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) тестовая документация;

e) материалы анализа глубины тестирования.

13.9.3.3 Действие ATE_DPT.1.1E

13.9.3.3.1 Шаг оценивания 4:ATE_DPT.1-1

ИСО/МЭК 15408-3 ATE_DPT.1.1C: *Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.*

Оценщик должен исследовать материалы анализа глубины тестирования на предмет сопоставления тестов, идентифицированных в тестовой документации, и проекта верхнего уровня.

В материалах анализа глубины тестирования должны быть идентифицированы все подсистемы, описанные в проекте верхнего уровня, и представлено сопоставление тестов с этими подсистемами. Соответствие может принимать форму таблицы или матрицы. В некоторых случаях, чтобы показать соответствие тестов, достаточно наличия такого отображения. В других случаях может потребоваться некоторое обоснование (обычно на естественном языке) для того, чтобы дополнить материалы анализа соответствия, представленные разработчиком.

Все детали проекта, специфицированные в проекте верхнего уровня, сопоставленные с требованиями безопасности ОО и удовлетворяющие им, являются предметом тестирования, а следовательно, должны быть сопоставлены с тестовой документацией. На рисунке 14 отражена концептуальная структура сопоставления подсистем, описанных в проекте верхнего уровня, и тестов, изложенных в тестовой документации ОО и используемых для их тестирования. Тесты могут затрагивать одну или несколько функций безопасности, что может быть обусловлено зависимостями между тестами или общей целью выполняемого теста.

13.9.3.3.2 Шаг оценивания 4:ATE_DPT.1-2

Оценщик должен исследовать план тестирования разработчика, чтобы сделать заключение, является ли подход к тестированию каждой функции безопасности ФБО пригодным для демонстрации ожидаемого режима ее выполнения.

Руководство по выполнению этого шага оценивания можно найти в следующих замечаниях по применению:

a) «Понимание ожидаемого режима функционирования ОО»;

b) «Альтернативные тестированию подходы к верификации ожидаемого режима выполнения функции безопасности».

Тестирование ФБО может быть выполнено с использованием внешних интерфейсов, внутренних интерфейсов или комбинации тех и других. Независимо от того, какая стратегия используется, оценщик будет рассматривать ее пригодность для адекватного тестирования функций безопасности. В частности, оценщик делает заключение, является ли тестирование с использованием внутренних интерфейсов функций безопасности необходимым или эти внутренние интерфейсы могут быть надлежащим образом протестированы (хотя и неявным образом) с использованием внешних интерфейсов. Это решение, как и его логическое обоснование, остается за оценщиком.

13.9.3.3.3 Шаг оценивания 4:ATE_DPT.1-3

Оценщик должен исследовать процедуры тестирования, чтобы сделать заключение, адекватно ли описание предварительных условий тестирования, шагов тестирования и ожидаемого результата (ожидаемых результатов) для тестирования каждой функции безопасности.

Руководство по выполнению этого шага оценивания, который относится к проекту верхнего уровня, можно найти в замечаниях по применению «Верификация адекватности тестов».

13.9.3.3.4 Шаг оценивания 4:ATE_DPT.1-4

Оценщик должен проверить материалы анализа глубины тестирования, чтобы удостовериться, что ФБО в том виде, в котором они определены в проекте верхнего уровня, полностью сопоставлены с тестами, представленными в тестовой документации.

Материалы анализа глубины тестирования обеспечивают полное изложение соответствия между проектом верхнего уровня, планом и процедурами тестирования. Все подсистемы и внутренние интерфейсы, описанные в проекте верхнего уровня, должны быть представлены в материалах анализа глубины тестирования. Для всех подсистем и внутренних интерфейсов, представленных в материалах анализа глубины тестирования, должны иметься сопоставленные с ними тесты для того, чтобы можно было утверждать о полноте. Как показано на рисунке 14, для всех подсистем и внутренних интерфейсов имеются относящиеся к ним тесты, а следовательно, в данном примере продемонстрирована полнота глубины тестирования. Неполнота тестирования была бы очевидна, если бы подсистема или внутренний интерфейс были идентифицированы в материалах анализа глубины тестирования, но никакие тесты не могли быть к ним отнесены.

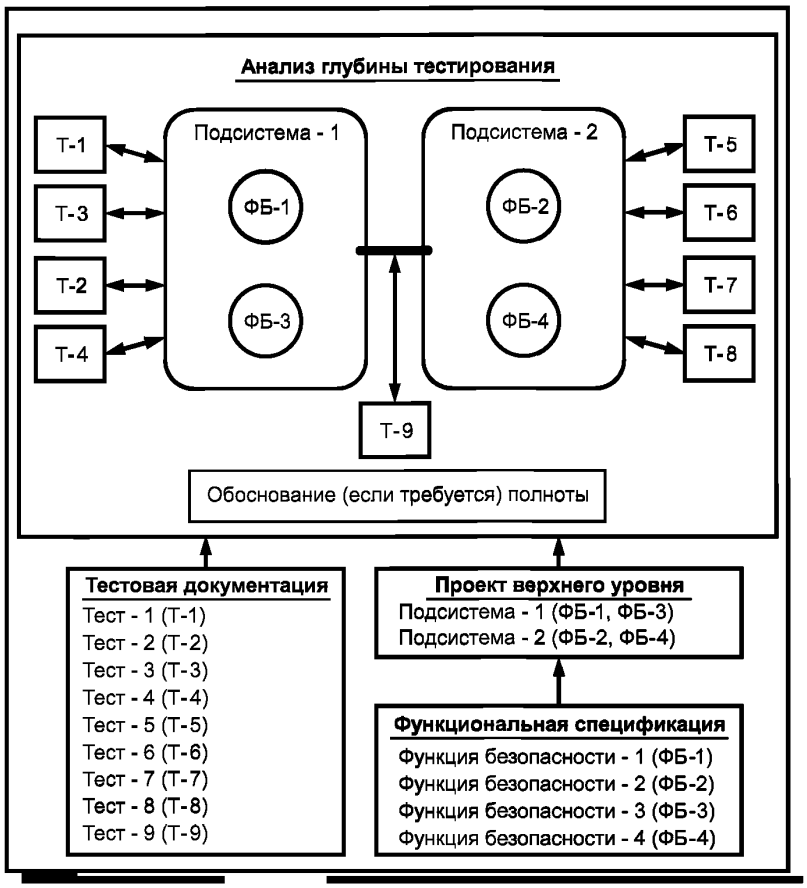


Рисунок 14 — Концептуальная структура анализа глубины тестирования

13.9.4 Оценка функциональных тестов (ATE_FUN.1)

13.9.4.1 Цели

Цель данного подвида деятельности — сделать заключение, является ли документация функциональных тестов разработчика достаточной для демонстрации того, что функции безопасности выполняются в соответствии со спецификациями.

13.9.4.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) тестовая документация;

d) процедуры тестирования.

13.9.4.3 Замечания по применению

Степень требуемого покрытия ФБО тестовой документацией зависит от соответствующего компонента доверия, связанного с покрытием тестами.

Для представленных тестов разработчика оценщик делает заключение, являются ли тесты повторимыми, и определяет степень возможности использования тестов разработчика при проведении оценщиком независимого тестирования. Любую функцию безопасности, для которой результаты тестирования разработчиком указывают, что она может быть не выполнена в соответствии со спецификациями, оценщику следует подвергнуть независимому тестированию, чтобы сделать заключение, выполнена ли она в соответствии со спецификациями или нет.

Тестовая документация должна идентифицировать все случаи использования привилегированных режимов для установления/отмены условий тестирования для последующих тестов. Тестовая документа-

ция должна описывать, почему было необходимо использовать привилегированные режимы для достижения необходимых условий (например, для обеспечения генерации средствами тестирования определенных объектов, необходимых для выполнения некоторого теста, которые не могут быть созданы непривилегированными пользователями), а также – каким образом осуществляется выход из привилегированных режимов до проведения шагов по тестированию, демонстрирующих функциональные возможности безопасности ОО. Следовательно, несмотря на то, что тестовая конфигурация может не соответствовать описанию ОО в ЗБ, в процессе установления условий тестирования тестовая документация должна содержать описание, каким образом конфигурацию можно вернуть в состояние, которое соответствует конфигурации, описанной в ЗБ, для выполнения шагов по тестированию.

13.9.4.4 Действие ATE_FUN.1.1E

13.9.4.4.1 Шаг оценивания 4:ATE_FUN.1-1

ИСО/МЭК 15408-3 ATE_FUN.1.1C: *Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.*

Оценщик должен проверить, что тестовая документация включает в себя планы тестирования, описание процедур тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

13.9.4.4.2 Шаг оценивания 4:ATE_FUN.1-2

ИСО/МЭК 15408-3 ATE_FUN.1.2C: *Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей проводимых тестов.*

Оценщик должен проверить, что в плане тестирования идентифицированы подлежащие тестированию функции безопасности.

Одним из методов, который может быть использован для идентификации проверяемой функции безопасности, является ссылка на соответствующую часть (части) функциональной спецификации, в которой определена конкретная функция безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.3 Шаг оценивания 4:ATE_FUN.1-3

Оценщик должен исследовать план тестирования, чтобы сделать заключение, содержит ли он описание целей выполняемых тестов.

План тестирования предоставляет информацию о том, каким образом тестируются функции безопасности, а также информацию о тестируемой конфигурации ОО, используемой при проведении тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.4 Шаг оценивания 4:ATE_FUN.1-4

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласована ли тестируемая конфигурация ОО с той конфигурацией, которая идентифицирована для оценки в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ. Оценщик верифицирует, что в тестовой документации разработчика определены тестируемые конфигурации и они согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

13.9.4.4.5 Шаг оценивания 4:ATE_FUN.1-5

Оценщик должен исследовать план тестирования, чтобы сделать заключение, согласован ли он с описанием процедур тестирования.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.9.4.4.6 Шаг оценивания 4:ATE_FUN.1-6

ИСО/МЭК 15408-3 ATE_FUN.1.3C: *Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функ-*

ции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

Оценщик должен проверить, что в описании процедур тестирования идентифицирован каждый из подлежащих тестированию режимов выполнения функций безопасности.

Одним из методов, который может быть использован для идентификации подлежащего тестированию режима выполнения функции безопасности, является ссылка на соответствующую часть (части) спецификации проекта, которая определяет конкретный подлежащий тестированию режим выполнения функции безопасности.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.7 Шаг оценивания 4:ATE_FUN.1-7

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции для того, чтобы установить воспроизводимые начальные условия выполнения тестов, включая зависимости, связанные с порядком следования, при их наличии.

Для того чтобы установить начальные условия выполнения тестов, возможно, потребуется выполнить некоторые шаги. Например, необходимо добавить учетные записи пользователей прежде, чем их можно будет удалить. Пример зависимостей, связанных с порядком следования тестов, от результатов других тестов — необходимо тестирование функции аудита прежде, чем можно будет полагаться на нее при создании записей аудита для другого механизма безопасности, такого как управления доступом. Другой пример зависимости, связанной с порядком следования тестов, — при выполнении одного набора тестов генерируется файл данных, используемых в качестве исходных данных для другого набора тестов.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.8 Шаг оценивания 4:ATE_FUN.1-8

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение, представлены ли достаточные инструкции для того, чтобы иметь воспроизводимый способ инициирования выполнения функций безопасности и наблюдения за режимом их выполнения.

Инициирующее воздействие обычно обеспечивается внешним по отношению к функции безопасности способом через ИФБО. После того как входные данные (инициирующее воздействие) предоставлены ИФБО, через ИФБО можно наблюдать режим выполнения функции безопасности. Воспроизводимость не обеспечивается, если процедуры тестирования не содержат достаточных подробностей для однозначного описания инициирующего воздействия и режима выполнения, ожидаемого в результате инициирующего воздействия.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.9 Шаг оценивания 4:ATE_FUN.1-9

Оценщик должен исследовать описание процедур тестирования, чтобы сделать заключение об их согласованности с процедурами тестирования.

Если описание процедур тестирования — это собственно процедуры тестирования, то рассматриваемый шаг оценивания не применяют и поэтому считают удовлетворенным.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А). Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.9.4.4.10 Шаг оценивания 4:ATE_FUN.1-10

ИСО/МЭК 15408-3 ATE_FUN.1.4C: *Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.*

Оценщик должен исследовать тестовую документацию, чтобы сделать заключение о достаточности включенных в нее ожидаемых результатов выполнения тестов.

Ожидаемые результаты тестирования необходимы, чтобы сделать заключение, действительно ли тест был успешно выполнен. Описание ожидаемых результатов тестирования достаточно, если оно однозначно и согласуется с ожидаемым режимом выполнения ФБО, обусловленным подходом к тестированию.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.4.4.11 Шаг оценивания 4:ATE_FUN.1-11

ИСО/МЭК 15408-3 ATE_FUN.1.5C: *Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.*

Оценщик должен проверить, что ожидаемые результаты тестирования в тестовой документации согласуются с представленными фактическими результатами тестирования.

Сравнение представленных разработчиком фактических и ожидаемых результатов тестирования выявит какие бы то ни было несоответствия результатов.

Возможно, что непосредственное сравнение фактических результатов не может быть выполнено до того, как будет выполнено некоторое преобразование или синтез данных. В подобных случаях в тестовой документации разработчика должен быть описан процесс преобразования или синтеза фактических данных.

Например, разработчику может потребоваться проверить содержимое буфера сообщений после того, как имело место сетевое соединение, чтобы определить содержимое буфера. Буфер сообщения будет содержать бинарную последовательность. Эту бинарную последовательность, как правило, преобразуют в другую форму представления данных, чтобы сделать тест более содержательным. Преобразование этого бинарного представления данных в представление более высокого уровня должно быть достаточно подробно описано разработчиком, чтобы позволить оценщику выполнить процесс преобразования (т.е. необходимо описать, используется ли синхронный или асинхронный метод передачи данных, число стоповых битов, битов четности и т.д.).

Следует отметить, что описание процесса преобразования или синтеза фактических данных оценщик использует не для того, чтобы фактически исполнить необходимую модификацию, а для того, чтобы оценить корректность этого процесса. Преобразование ожидаемых результатов тестирования в формат, позволяющий их легко сравнивать с фактическими результатами тестов, возложено на разработчика.

Для выполнения данного шага оценивания оценщик может избрать стратегию выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

Если ожидаемые и фактические результаты тестирования для какого-либо из тестов не совпадают, то правильность выполнения функции безопасности не продемонстрирована. Такая ситуация окажет влияние на усилия оценщика по независимому тестированию, выражающееся в необходимости тестирования соответствующей функции безопасности. Оценщику также следует рассмотреть вопрос об увеличении выборки свидетельств, на основе которых должен быть выполнен рассматриваемый шаг оценивания.

13.9.4.4.12 Шаг оценивания 4:ATE_FUN.1-12

Оценщик должен привести в отчете информацию об усилиях разработчика по тестированию, выделив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании разработчиком, зафиксированная в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные разработчиком на тестирование ОО. Смысл предоставления данной информации состоит в том, чтобы привести краткий содержательный обзор усилий разработчика по тестированию. Не обязательно, чтобы информация о тестировании разработчиком в ТОО была точной копией конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, позволяющие другим оценщикам и сотрудникам органов оценки понять подход разработчика к тестированию, объем выполненного тестирования, тестируемые конфигураций ОО и общий результат тестирования разработчиком.

Информация об усилиях разработчика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, подвергнутые тестированию;

b) подход к тестированию. Описание общей стратегии тестирования, которую применил разработчик;

c) объем тестирования, выполненного разработчиком. Описание степени покрытия тестами и глубины тестирования разработчиком;

d) результаты тестирования. Описание общих результатов тестирования разработчиком.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, связанной с усилиями разработчика по тестированию, которую следует привести в ТОО.

13.9.5 Оценка путем независимого тестирования (ATE_IND.2)

13.9.5.1 Цели

Цель данного подвида деятельности состоит в том, чтобы путем независимого тестирования некоторого подмножества ФБО сделать заключение, соответствуют ли спецификациям режимы функционирования ОО, и повысить уверенность в результатах тестирования разработчиком путем выполнения выборки тестов разработчика.

13.9.5.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) руководство пользователя;

d) руководство администратора;

e) процедуры безопасной установки, генерации и запуска;

f) тестовая документация;

g) материалы анализа покрытия тестами;

h) материалы анализа глубины тестирования;

i) ОО, пригодный для тестирования.

13.9.5.3 Действие ATE_IND.2.1E

13.9.5.3.1 Шаг оценивания 4:ATE_IND.2-1

ИСО/МЭК 15408-3 ATE_IND.2.1C: *ОО должен быть пригоден для тестирования.*

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, используемый оценщиком для тестирования, должен иметь ту же самую уникальную маркировку, которая установлена в соответствии с подвидом деятельности ACM_CAP.* «Возможности УК».

В ЗБ может быть определено более одной подлежащей оценке конфигурации. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию в соответствии с ЗБ. Тестируемые оценщиком конфигурации ОО должны быть согласованы соответственно с каждой из оцениваемых конфигураций, описанных в ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не относятся к среде тестирования. Например, предположение относительно допусков пользователей не относится к среде тестирования, а предположение относительно единой точки подключения к сети относится к среде тестирования.

При использовании любых средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика.

13.9.5.3.2 Шаг оценивания 4:ATE_IND.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности ADO_IGS.1 «Процедуры установки, генерации и запуска» позволит считать выполненным данный шаг оценивания, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику необходимо выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данный шаг оценивания мог бы удовлетворить шаг оценивания ADO_IGS.1-2.

13.9.5.3.3 Шаг оценивания 4:ATE_IND.2-3

ИСО/МЭК 15408-3 ATE_IND.2.2C: *Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.*

Оценщик должен исследовать набор ресурсов, предоставленных разработчиком, чтобы сделать заключение, эквивалентны ли они набору ресурсов, использованных разработчиком для функционального тестирования ФБО.

Данный набор ресурсов может, кроме всего прочего, включать в себя доступное лабораториям и специальное испытательное оборудование. Ресурсы, которые не являются идентичными ресурсам, использованным разработчиком, должны быть эквивалентны им с точки зрения любого влияния, которое они могут оказать на результаты тестирования.

13.9.5.4 Действие ATE_IND.2.2E

13.9.5.4.1 Шаг оценивания 4:ATE_IND.2-4

Оценщик должен определить тестируемое подмножество ФБО.

Оценщик выбирает тестируемое подмножество и стратегию тестирования, которая является приемлемой для ОО. Одна, крайняя, стратегия тестирования предусматривает наличие тестируемого подмноже-

ства ФБО, содержащего как можно большее число функций безопасности, тестируемых с небольшой строгостью. Другая стратегия тестирования предусматривает наличие тестируемого подмножества, содержащего небольшое число функций безопасности, исходя из их осознанной значимости, и строгое тестирование этих функций.

Как правило, стратегия тестирования, принятая оценщиком, должна находиться где-то между этими двумя крайностями. Оценщику следует проверить выполнение большинства определенных в ЗБ функциональных требований безопасности, используя, по крайней мере, один тест для каждого требования, но при этом нет необходимости, чтобы тестирование продемонстрировало исчерпывающую проверку спецификаций.

При выборе подмножества тестируемых ФБО оценщику необходимо рассмотреть следующие факторы:

a) свидетельства тестирования разработчиком. Свидетельства тестирования разработчиком включают в себя: анализ покрытия тестами, анализ глубины тестирования и тестовую документацию. Свидетельства тестирования разработчиком будут обеспечивать понимание того, каким образом разработчиком в ходе тестирования были проверены функции безопасности. Оценщик будет использовать данную информацию при разработке новых тестов для независимого тестирования ОО. Оценщику следует, в особенности, рассмотреть:

1) усиление тестирования, выполненного разработчиком, для определенной функции (функций) безопасности. Оценщик может выполнить большее число тестов того же самого типа, чтобы путем изменения параметров более строго протестировать функцию безопасности;

2) дополнение стратегии тестирования, примененной разработчиком, для определенной функции (функций) безопасности. Оценщик может изменить подход к тестированию определенной функции безопасности, тестируя ее с использованием другой стратегии тестирования;

b) число функций безопасности, из которых необходимо сформировать тестируемое подмножество. В тех случаях, когда у ОО только небольшое число функций безопасности, может быть практичным строгое тестирование всех функций безопасности. Для ОО с большим числом функций безопасности это будет нерентабельно и потребуется осуществление выборки;

c) поддержание некоторого баланса между видами деятельности по оценке. Усилия оценщика, затраченные на вид деятельности по тестированию, должны быть соразмерны с усилиями, затраченными на любой другой вид деятельности по оценке.

Оценщик выбирает определенные функции безопасности для формирования соответствующего подмножества. Этот выбор будет зависеть от ряда факторов, и рассмотрение этих факторов также может влиять на выбор размера тестируемого подмножества ФБО:

a) строгость тестирования разработчиком функций безопасности. Все функции безопасности, идентифицированные в функциональной спецификации, должны иметь относящиеся к ним свидетельства тестирования разработчиком, как это требуется в ATE_COV.2 «Анализ покрытия». Те функции безопасности, которые оценщик определил как требующие дополнительного тестирования, следует включить в тестируемое подмножество ФБО;

b) результаты тестирования разработчиком. Если результаты тестов разработчика заставляют оценщика сомневаться в том, что функция безопасности или ее аспект выполняется в соответствии со спецификациями, то оценщику следует включить подобные функции безопасности в тестируемое подмножество;

c) известные из общедоступных источников слабые места безопасности, обычно ассоциируемые с конкретным типом ОО (например, с операционной системой, межсетевым экраном). Известные из общедоступных источников слабые места, ассоциируемые с конкретным типом ОО, будут влиять на процесс выбора тестируемого подмножества. Оценщику следует включить в тестируемое подмножество те функции безопасности, которые связаны с известными из общедоступных источников слабыми местами для данного типа ОО (известные из общедоступных источников слабые места в данном случае относятся не к уязвимостям как таковым, а к несоответствиям или проблемным вопросам, которые были обнаружены для данного конкретного типа ОО). Если такие слабые места неизвестны, то может быть более приемлемым более общий подход, связанный с выбором широкого диапазона функций безопасности;

d) значимость функций безопасности. Те функции безопасности, которые более значимы, чем другие, с точки зрения целей безопасности для ОО, следует включить в тестируемое подмножество;

e) утверждение о СФБ, сделанное в ЗБ. Все функции безопасности, для которых было сделано конкретное утверждение о СФБ, следует включить в тестируемое подмножество ФБО;

f) сложность функции безопасности. Для сложных функций безопасности может потребоваться выполнение сложных тестов, налагающих обременительные требования на разработчика или оценщика, что,

в свою очередь, не будет способствовать экономичным оценкам. С другой стороны, сложные функции безопасности — это вероятная область поиска ошибок и подходящие кандидаты для включения в подмножество. Оценщику необходимо достигнуть баланса между этими соображениями;

g) неявное тестирование. Тестирование некоторых функций безопасности может зачастую сопровождаться неявным тестированием других функций безопасности, и их включение в подмножество может максимизировать (хотя и не в явном виде) число тестируемых функций безопасности. Некоторые интерфейсы могут обеспечивать несколько функциональных возможностей безопасности, и их следует сделать объектом эффективного подхода к тестированию;

h) типы интерфейсов ОО (например, программный интерфейс, командная строка, протокол). Оценщику следует рассмотреть возможность включения тестов для всех различных типов интерфейсов, которые поддерживает данный ОО;

i) инновационные или необычные функции. В тех случаях, когда в ОО включены инновационные или необычные функции безопасности, которые могут быть широко представлены в маркетинговой литературе, они должны быть прямыми кандидатами на тестирование.

Выше сформулированы факторы, которые необходимо рассмотреть в процессе выбора приемлемого тестируемого подмножества ФБО, но они ни в коем случае не являются исчерпывающими.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.5.4.2 Шаг оценивания 4:ATE_IND.2-5

Оценщик должен разработать тестовую документацию для тестируемого подмножества ФБО, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов.

Установив из ЗБ и функциональной спецификации ожидаемый режим выполнения функции безопасности, оценщик должен определить наиболее подходящий способ тестирования данной функции. Оценщик, в особенности, рассматривает:

a) подход, который будет использован, например, будет ли функция безопасности протестирована через внешний интерфейс, внутренний интерфейс с использованием каких-либо средств автономного тестирования или будет применен альтернативный тестированию подход (например, в исключительных обстоятельствах — экспертиза кода);

b) интерфейс(ы) функции безопасности, который(е) будет(ут) использован(ы) для инициирования выполнения функции безопасности и наблюдения ее реакции;

c) начальные условия, которые будут необходимы для выполнения теста (т.е. любые конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

d) специальное оборудование для тестирования, которое потребуется либо для инициирования выполнения функции безопасности (например, генераторы пакетов), либо для наблюдения за функцией безопасности (например, сетевые анализаторы).

Оценщик может посчитать практичным тестировать каждую функцию безопасности с помощью ряда наборов тестов, где каждый набор тестов будет использован для тестирования конкретного режима выполнения функции безопасности.

В тестовой документации оценщика следует определить происхождение каждого теста, прослеживая его к соответствующей спецификации проекта и, если необходимо, к ЗБ.

13.9.5.4.3 Шаг оценивания 4:ATE_IND.2-6

Оценщик должен провести тестирование.

Оценщик использует разработанную тестовую документацию как основу для тестирования ОО, но это не мешает ему выполнить дополнительные специальные тесты. Оценщик может разработать новые тесты исходя из режима функционирования ОО, обнаруженного в процессе тестирования. Эти новые тесты должны быть внесены в тестовую документацию.

13.9.5.4.4 Шаг оценивания 4:ATE_IND.2-7

Оценщик должен зафиксировать следующую информацию о тестах, которые составляют подмножество тестов:

a) идентификационную информацию тестируемого режима выполнения функции безопасности;

b) инструкции по подключению и настройке всего необходимого оборудования для тестирования, как это требуется для проведения конкретного теста;

c) инструкции по установке всех предварительных условий выполнения теста;

d) инструкции по инициированию функции безопасности;

e) инструкции по наблюдению режима выполнения функции безопасности;

f) описание всех ожидаемых результатов и необходимого анализа, проводимого по отношению к наблюдаемому режиму выполнения для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО;

h) фактические результаты тестирования.

Уровень детализации должен быть таким, чтобы другой оценщик мог повторить тесты и получить эквивалентный результат. Хотя некоторые специфические детали результатов выполнения теста могут различаться (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными.

Возможны случаи, когда нет необходимости предоставлять всю информацию, приведенную на этом шаге оценивания (например, фактические результаты тестирования могут не требовать какого бы то ни было анализа до их сравнения с ожидаемыми результатами). Решение опустить эту информацию, как и его логическое обоснование, остается за оценщиком.

13.9.5.4.5 Шаг оценивания 4:ATE_IND.2-8

Оценщик должен проверить, что все фактические результаты тестирования соответствуют ожидаемым результатам тестирования.

Любые различия в фактических и ожидаемых результатах тестирования могут свидетельствовать либо о том, что ОО не функционирует в соответствии со спецификацией, либо о том, что тестовая документация оценщика может быть некорректной. Не соответствующие ожидаемым фактические результаты тестирования могут потребовать внесения корректив в ОО или тестовую документацию, а также, возможно, повторного выполнения вызвавших коллизию тестов, модификации размера и состава выборки тестов. Это решение, как и его логическое обоснование, остается за оценщиком.

13.9.5.5 Действие ATE_IND.2.3E

13.9.5.5.1 Шаг оценивания 4:ATE_IND.2-9

Оценщик должен провести тестирование, используя выборку тестов, предусмотренных в плане и процедурах тестирования разработчика.

Общая цель данного шага оценивания состоит в выполнении тестов разработчика в количестве, достаточном для подтверждения правильности результатов тестирования разработчиком. Оценщик должен определить размер выборки и тесты разработчика, которые составят данную выборку.

С учетом общих усилий оценщика по виду деятельности, связанному с тестированием, обычно следует выполнить около 20 % тестов разработчика, хотя этот процент может варьироваться в зависимости от характера ОО и представленных свидетельств тестирования.

Все тесты разработчика могут быть сопоставлены с конкретными функциями безопасности. Следовательно, факторы, которые необходимо рассмотреть при выборе тестов для включения в выборку, подобны тем, которые перечислены на шаге оценивания ATE_IND.2-4 для выбора тестируемого подмножества ФБО. Дополнительно, для выбора тестов разработчика, включаемых в выборку, оценщик может избрать метод случайной выборки.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.9.5.5.2 Шаг оценивания 4:ATE_IND.2-10

Оценщик должен проверить, что все фактические результаты тестирования согласуются с ожидаемыми результатами тестирования.

Противоречия между ожидаемыми результатами тестирования разработчиком и фактическими результатами тестирования заставляют оценщика разрешать эти несоответствия. Противоречия, с которыми столкнулся оценщик, могут быть разрешены разработчиком путем убедительного объяснения и устранения противоречий.

Если удовлетворительное объяснение или устранение противоречий не может быть достигнуто, то уверенность оценщика в результатах тестирования разработчиком может уменьшиться; у оценщика даже может возникнуть необходимость в увеличении объема выборки, чтобы восстановить уверенность в результатах тестирования разработчиком. Если увеличение объема выборки не оправдает ожиданий оценщика, может потребоваться повторение всей совокупности тестов разработчика. В конечном счете, для адекватного тестирования подмножества ФБО, идентифицированного на шаге оценивания ATE_IND.2-4, недостаточность тестов разработчика приведет к необходимости корректировки тестов разработчика или разработки оценщиком новых тестов.

13.9.5.5.3 Шаг оценивания 4:ATE_IND.2-11

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

Информация оценщика о тестировании, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию и усилия, затраченные в течение оценки на вид деятельности по тестированию.

Смысл предоставления данной информации состоит в том, чтобы привести содержательный краткий обзор усилий по тестированию. Не имеется в виду, чтобы информация о тестировании в ТОО была точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию, объем выполненного оценщиком тестирования, объем выполненного разработчиком тестирования, тестируемые конфигурации ОО и общий результат вида деятельности по тестированию.

Информация, относящаяся к усилиям оценщика по тестированию, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были протестированы;

b) выбранный размер подмножества. Число протестированных в течение оценки функций безопасности и логическое обоснование этого размера;

c) критерии выбора для функций безопасности, которые составляют тестируемое подмножество. Краткое изложение факторов, рассмотренных при отборе функций безопасности для включения в подмножество;

d) протестированные функции безопасности. Краткий перечень функций безопасности, обоснованно включенных в подмножество;

e) выполненные тесты разработчика. Число выполненных тестов разработчика и краткое описание критериев, использованных для выбора данных тестов;

f) вердикт по виду деятельности. Общий вывод по результатам тестирования, проведенного в течение оценки.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования, выполненного оценщиком в течение оценки, которую следует привести в ТОО.

13.10 Вид деятельности «Оценка уязвимостей»

Вид деятельности «Оценка уязвимостей» предназначен для того, чтобы сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО. Это заключение должно быть основано на анализе, выполненном разработчиком и оценщиком, и поддержано тестированием, выполненным оценщиком.

13.10.1 Оценка неправильного применения (AVA_MSU.2)

13.10.1.1 Цели

Цель данного подвида деятельности — сделать заключение, не являются ли руководства вводящими в заблуждение, необоснованными или противоречивыми, были ли учтены процедуры безопасности для всех режимов функционирования и будет ли использование руководств способствовать предотвращению и обнаружению небезопасных состояний ОО.

13.10.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) проект нижнего уровня;

e) подмножество представления реализации;

f) модель политики безопасности ОО;

g) руководство пользователя;

h) руководство администратора;

i) процедуры безопасной установки, генерации и запуска;

j) материалы анализа неправильного применения руководств;

k) тестовая документация;

l) ОО, пригодный для тестирования.

13.10.1.3 Замечания по применению

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной установки, генерации и запуска. Здесь к процедурам установки, генерации и запуска относятся все процедуры перевода ОО из состояния при поставке в состояние функционирования, ответственным за выполнение которых является администратор.

Этот компонент включает в себя требование к анализу, выполняемому разработчиком, которое не присутствует в AVA_MSU.1 «Экспертиза руководств». Проверку правильности этого анализа не следует

использовать как замену собственного исследования оценщиком руководств, но следует использовать, чтобы предоставить свидетельство, что разработчик также явным образом учел проблему неправильного применения.

13.10.1.4 Действие AVA_MSU.2.1E

13.10.1.4.1 Шаг оценивания 4:AVA_MSU.2-1

ИСО/МЭК 15408-3 AVA_MSU.2.1C: *Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.*

Оценщик должен исследовать руководства и другие свидетельства оценки, чтобы сделать заключение, идентифицированы ли в руководствах все возможные режимы эксплуатации ОО (включая, если применимо, функционирование после сбоя или ошибки в работе), их последствия и значение для поддержания безопасной эксплуатации.

Другие свидетельства оценки, в особенности функциональная спецификация и тестовая документация, представляют собой источник информации, который оценщику следует использовать, чтобы сделать заключение, содержат ли руководства достаточную руководящую информацию.

Оценщик может предпочесть анализировать функции безопасности ФБО поочередно, сопоставляя руководство для безопасного использования данной функции безопасности с другими свидетельствами оценки, чтобы сделать заключение, достаточны ли руководства в части, относящейся к данной функции безопасности, для ее безопасного использования (т.е. согласовано ли оно с ПБО). Оценщику следует также рассмотреть соотношения между функциями, осуществляя поиск потенциальных конфликтов.

13.10.1.4.2 Шаг оценивания 4:AVA_MSU.2-2

ИСО/МЭК 15408-3 AVA_MSU.2.2C: *Руководства должны быть полны, понятны, непротиворечивы и обоснованны.*

Оценщик должен исследовать руководства, чтобы сделать заключение, являются ли они понятными и внутренне непротиворечивыми.

Руководства являются непонятными, если они так или иначе могут быть неправильно истолкованы администратором или пользователем и использованы путем, причиняющим ущерб ОО или безопасности, обеспечиваемой ОО.

Руководство по анализу непротиворечивости см. в А.3 «Анализ непротиворечивости» (приложение А).

13.10.1.4.3 Шаг оценивания 4:AVA_MSU.2-3

Оценщик должен исследовать руководства и другие свидетельства оценки, чтобы сделать заключение, являются ли руководства полными и обоснованными.

Оценщику следует использовать знание ОО, приобретенное при выполнении других видов деятельности по оценке, чтобы сделать заключение, являются ли руководства полными.

В частности, оценщику следует рассмотреть функциональную спецификацию и краткую спецификацию ОО. Предполагается, что все функции безопасности, описание которых содержится в этих документах, описаны в руководствах надлежащим образом, чтобы дать возможность их безопасного администрирования и использования. Оценщик может в качестве вспомогательного средства подготовить неформальное отображение между руководствами и этими документами. Какие-либо пропуски в этом отображении могут указывать на неполноту.

Руководства являются необоснованными, если они содержат требования к использованию ОО или среде функционирования, которые противоречат ЗБ или являются чрезмерно обременительными для поддержания безопасности.

Оценщику следует учесть, что результаты, полученные в процессе выполнения шагов оценивания подвида деятельности AGD_ADM, предоставят полезные исходные данные для данного исследования.

13.10.1.4.4 Шаг оценивания 4:AVA_MSU.2-4

ИСО/МЭК 15408-3 AVA_MSU.2.3C: *Руководства должны содержать список всех предположений относительно среды эксплуатации.*

Оценщик должен исследовать руководства, чтобы сделать заключение, все ли предположения относительно предопределенной среды четко сформулированы.

Оценщик анализирует предположения ЗБ относительно предопределенной среды безопасности ОО и сравнивает их с руководствами, чтобы удостовериться, все ли предположения из ЗБ относительно предопределенной среды безопасности ОО, которые имеют отношение к администратору или пользователю, соответствующим образом описаны в руководствах.

13.10.1.4.5 Шаг оценивания 4:AVA_MSU.2-5

ИСО/МЭК 15408-3 AVA_MSU.2.4C: *Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).*

Оценщик должен исследовать руководства, чтобы сделать заключение, все ли требования для внешних мер безопасности четко сформулированы.

Оценщик анализирует руководства, чтобы удостовериться, перечислены ли в нем все внешние процедурные меры, меры физической защиты, управления персоналом и связностью. Цели безопасности в ЗБ для не-ИТ среды указывают на то, что требуется.

13.10.1.4.6 Шаг оценивания 4:AVA_MSU.2-6

ИСО/МЭК 15408-3 AVA_MSU.2.5C: *Документация анализа должна демонстрировать, что руководства полны.*

Оценщик должен исследовать материалы анализа, выполненного разработчиком, чтобы сделать заключение, предпринял ли разработчик соответствующие меры для обеспечения полноты руководств.

Материалы анализа, выполненного разработчиком, могут включать в себя отображения ЗБ или функциональной спецификации на руководства, чтобы продемонстрировать, что руководства являются полными. Какие бы ни были предоставлены разработчиком свидетельства для демонстрации полноты, оценщику следует оценить материалы анализа, выполненного разработчиком, с учетом любых недостатков, обнаруженных при выполнении шагов оценивания с AVA_MSU.2-1 по AVA_MSU.2-5, а также AVA_MSU.2-7.

13.10.1.5 Действие AVA_MSU.2.2E

13.10.1.5.1 Шаг оценивания 4:AVA_MSU.2-7

Оценщик должен выполнить все процедуры администратора и пользователя (если применимо), необходимые для конфигурирования и установки ОО, чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Конфигурация и инсталляция требуют, чтобы оценщик перевел ОО из состояния при поставке в состояние, в котором ОО функционирует и осуществляет ПБО, согласованную с целями безопасности, специфицированными в ЗБ.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя и администратора, обычно поставляемых потребителю ОО. Любые встретившиеся трудности в процессе такого применения процедур могут указывать на неполноту, непонятность, противоречивость или необоснованность руководств.

Работа, выполненная для удовлетворения данного шага оценивания, может также способствовать удовлетворению действия оценщика ADO_IGS.1.2E.

13.10.1.5.2 Шаг оценивания 4:AVA_MSU.2-8

Оценщик должен выполнить другие относящиеся к безопасности процедуры, специфицированные в руководствах, чтобы сделать заключение, может ли ОО быть безопасно сконфигурирован и использован с применением только представленных руководств.

Оценщику необходимо следовать только процедурам разработчика, задокументированным в руководствах пользователя и администратора, обычно поставляемых потребителю ОО.

Оценщику следует осуществить выборку при выполнении данного шага оценивания. При осуществлении выборки оценщику следует принять во внимание:

a) ясность руководства. Любое потенциально непонятное руководство следует включить в выборку;

b) руководство, которое будет использоваться наиболее часто. Редко используемое руководство обычно не следует включать в выборку;

c) сложность руководства. Сложное руководство следует включать в выборку;

d) серьезность ошибки. Процедуры, для которых ошибка влияет очень серьезным образом на безопасность, следует включать в выборку;

e) характер ОО. Руководство, связанное с нормальным или наиболее вероятным использованием ОО, следует включать в выборку.

Руководство по выборке см. в А.2 «Выборка» (приложение А).

13.10.1.6 Действие AVA_MSU.2.3E

13.10.1.6.1 Шаг оценивания 4:AVA_MSU.2-9

Оценщик должен исследовать руководства, чтобы сделать заключение, предоставлены ли потребителю руководства, достаточные, чтобы эффективно администрировать и использовать функции безопасности ОО, а также обнаруживать небезопасные состояния.

ОО могут использовать разнообразные способы содействия потребителю в эффективном с точки зрения безопасности использовании ОО. Один ОО может использовать функциональные возможности (характеристики), чтобы предупредить потребителя, когда ОО находится в небезопасном состоянии, в то время как другие ОО могут быть поставлены с расширенными руководствами, содержащими предложения, советы, процедуры и т.д. по наиболее эффективному использованию существующих характеристик безопасности, например, с руководством по использованию аудита как вспомогательного средства при обнаружении небезопасных состояний.

Чтобы вынести вердикт для этого шага оценивания, оценщик рассматривает функциональные возможности ОО, его назначение и предопределенную среду, а также предположения о его использовании или о пользователях. Оценщику следует прийти к заключению, что если возможен переход ОО в небезопасное состояние, то имеется ли обоснованное ожидание, что использование руководства позволит своевременно обнаружить небезопасное состояние. Заключение о потенциальной возможности перехода ОО в небезопасные состояния может быть сделано с использованием поставляемых для оценки материалов, таких как ЗБ, функциональная спецификация и проект верхнего уровня ФБО.

13.10.1.7 Действие AVA_MSU.2.4E

13.10.1.7.1 Шаг оценивания 4:AVA_MSU.2-10

Оценщик должен исследовать материалы анализа руководств, выполненного разработчиком, чтобы сделать заключение, предоставлено ли руководство по безопасному функционированию во всех режимах функционирования ОО.

Результаты действия по оценке AVA_MSU.2.1E обеспечивают основу для оценки материалов анализа, выполненного разработчиком. Оценивая возможность неправильного применения руководств, оценщик должен сделать заключение, отвечает ли анализ неправильного применения, выполненный разработчиком, целям этого подвида деятельности.

13.10.2 Оценка стойкости функций безопасности ОО (AVA_SOF.1)

13.10.2.1 Цели

Цель данного подвида деятельности — сделать заключение, приведены ли в ЗБ утверждения о СФБ для всех вероятностных или перестановочных механизмов и поддержаны ли утверждения о СФБ, приведенные разработчиком в ЗБ, корректным анализом.

13.10.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) проект нижнего уровня;

e) подмножество представления реализации;

f) руководство пользователя;

g) руководство администратора;

h) материалы анализа стойкости функций безопасности ОО.

13.10.2.3 Замечания по применению

Анализ СФБ выполняют для механизмов, которые по своей природе являются вероятностными или перестановочными, таких как механизм пароля или биометрия. Хотя криптографические механизмы также являются вероятностными и зачастую описываются в терминах стойкости, AVA_SOF.1 «Оценка стойкости функции безопасности» не применим к криптографическим механизмам. Для таких механизмов оценщику следует руководствоваться указаниями системы оценки.

Хотя анализ СФБ выполняют на базе отдельных механизмов, общее заключение о СФБ базируется на функциях. Если для обеспечения некоторой функции безопасности применяют более одного вероятностного или перестановочного механизма, проанализирован должен быть каждый отдельный механизм. Способ объединения этих механизмов для обеспечения функции безопасности определит общий уровень СФБ для этой функции. Оценщику необходима информация о проекте, чтобы понять, как механизмы работают вместе, чтобы обеспечить функцию, и минимальный уровень для такой информации предоставляют через зависимость от ADV_HLD.1 «Описательный проект верхнего уровня». Фактическая проектная информация, доступная оценщику, определяется ОУД, и эту доступную информацию, когда требуется, следует использовать для поддержки анализа, выполняемого оценщиком.

О СФБ в отношении многодоменных ОО см. в 9.3.6 «Оценка раздела «Требования безопасности ИТ» (ASE_REQ.1).

13.10.2.4 Действие AVA_SOF.1.1E

13.10.2.4.1 Шаг оценивания 4:AVA_SOF.1-1

ИСО/МЭК 15408-3 AVA_SOF.1.1C: *Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого в ЗБ имеется утверждение о СФБ, выраженное как уровень СФБ.

Если утверждения о СФБ выражены исключительно в метрике СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Уровень СФБ выражают как базовую СФБ, среднюю СФБ или высокую СФБ, которые определены в терминах потенциала нападения — см. ИСО/МЭК 15408-1, раздел 2. Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ как некотором уровне, который превышает общее требование СФБ.

Руководство по определению потенциала нападения, необходимого для осуществления нападения, и, следовательно, определению СФБ как некоторого уровня см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

Материалы анализа СФБ включают в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

13.10.2.4.2 Шаг оценивания 4:AVA_SOF.1-2

ИСО/МЭК 15408-3 AVA_SOF.1.2C: *Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.*

Оценщик должен проверить, предоставил ли разработчик материалы анализа СФБ для каждого механизма безопасности, в отношении которого имеется утверждение о СФБ в ЗБ, выраженное в некоторой метрике.

Если утверждения о СФБ выражены исключительно как уровни СФБ, то данный шаг оценивания не применяют и поэтому считают удовлетворенным.

Минимальное общее требование СФБ, выраженное как некоторый уровень, применяют ко всем некриптографическим вероятностным или перестановочным механизмам безопасности. Однако для отдельных механизмов может иметься утверждение о СФБ в метрике, которая удовлетворяет или превосходит общее требование СФБ.

Анализ СФБ включает в себя логическое обоснование утверждения о СФБ, приведенного в ЗБ.

13.10.2.4.3 Шаг оценивания 4:AVA_SOF.1-3

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, являются ли обоснованными любые утверждения или предположения, поддерживающие анализ.

Например, может быть неверным предположение, что конкретная реализация генератора псевдослучайных чисел будет обладать энтропией, необходимой для отбора данного механизма безопасности в число тех, для которых уместен анализ СФБ.

Ожидается, что предположения, сопровождающие анализ СФБ, отражают самый плохой случай, за исключением случая, являющегося в соответствии с ЗБ несостоятельным. Когда существует ряд различных возможных сценариев, зависящих от поведения человека-пользователя или нарушителя, следует предположить сценарий, который представляет самую низкую стойкость, если этот сценарий не был признан ранее несостоятельным.

Например, утверждение о стойкости, основанное на максимальной теоретически возможной области значений пароля (т.е. комбинаций всех печатных символов ASCII), обычно не является самым плохим случаем, потому что человеку свойственно использовать пароли на естественном языке, существенно уменьшая область значений пароля и ассоциированную с ней стойкость. Однако такое предположение может быть приемлемым, если в конкретном ОО применены меры ИТ, идентифицированные в ЗБ, такие как фильтры паролей, с целью минимизировать использование паролей на естественном языке.

13.10.2.4.4 Шаг оценивания 4:AVA_SOF.1-4

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, корректны ли любые алгоритмы, принципы, характеристики и вычисления, поддерживающие анализ.

Характер данного шага оценивания сильно зависит от типа рассматриваемого механизма. В А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А) представлен пример анализа СФБ для

функции идентификации и аутентификации, которая реализована с использованием механизма пароля; при анализе рассмотрена максимальная область значений пароля, чтобы, в конечном счете, прийти к некоторому уровню СФБ. Для биометрии при анализе рассматривают разрешающую способность и другие факторы, влияющие на чувствительность механизма к обману.

СФБ, выраженная как некоторый уровень, основана на минимальном потенциале нападения, требуемом, чтобы нанести поражение механизму безопасности. Уровни СФБ определены в терминах потенциала нападения в ИСО/МЭК 15408-1, раздел 2.

Руководство по определению потенциала нападения см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

13.10.2.4.5 Шаг оценивания 4:AVA_SOF.1-5

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, каждое ли утверждение о СФБ удовлетворено или превышено.

Руководство по ранжированию утверждений о СФБ см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

13.10.2.4.6 Шаг оценивания 4:AVA_SOF.1-6

Оценщик должен исследовать материалы анализа СФБ, чтобы сделать заключение, все ли функции с заявленной СФБ удовлетворяют минимальному уровню стойкости, определенному в ЗБ.

13.10.2.5 Действие AVA_SOF.1.2E

13.10.2.5.1 Шаг оценивания 4:AVA_SOF.1-7

Оценщик должен исследовать функциональную спецификацию, проект верхнего уровня, проект нижнего уровня, руководство пользователя и руководство администратора, чтобы сделать заключение, для всех ли вероятностных или перестановочных механизмов имеется утверждение о СФБ.

Идентификация разработчиком функций безопасности, которые реализованы вероятностными или перестановочными механизмами, должна быть верифицирована в процессе оценки ЗБ. Однако, поскольку краткая спецификация ОО может быть единственным свидетельством, доступным при выполнении этих действий, идентификация таких механизмов может быть неполной. Дополнительные свидетельства оценки, требуемые в качестве исходных данных для этого подвида деятельности, могут идентифицировать дополнительные вероятностные или перестановочные механизмы, ранее не идентифицированные в ЗБ. Если это так, то ЗБ должно быть соответствующим образом обновлено, чтобы отразить дополнительные утверждения о СФБ, а разработчику будет необходимо представить материалы дополнительного анализа, в которых должны быть логически обоснованы утверждения о СФБ, в качестве исходных данных для действия оценщика AVA_SOF.1.1E.

13.10.2.5.2 Шаг оценивания 4:AVA_SOF.1-8

Оценщик должен исследовать утверждения о СФБ, чтобы сделать заключение, являются ли они корректными.

Если материалы анализа СФБ включают в себя утверждения или предположения (например, о возможном числе попыток аутентификации в минуту), оценщику следует независимо подтвердить, что они корректны. Это может быть достигнуто путем тестирования или независимого анализа.

13.10.3 Оценка анализа уязвимостей (AVA_VLA.2)

13.10.3.1 Цели

Цель данного подвида деятельности — сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, уязвимости, пригодные для использования нарушителями, обладающими низким потенциалом нападения.

13.10.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

a) ЗБ;

b) функциональная спецификация;

c) проект верхнего уровня;

d) проект нижнего уровня;

e) подмножество представления реализации;

f) модель политики безопасности ОО;

g) руководство пользователя;

h) руководство администратора;

i) процедуры безопасной установки, генерации и запуска;

j) материалы анализа уязвимостей;

k) материалы анализа стойкости функций безопасности ОО;

l) ОО, пригодный для тестирования.

Дополнительным исходным материалом для данного подвида деятельности является:

a) текущая информация о явных уязвимостях (например, от органа оценки).

13.10.3.3 Замечания по применению

Использование термина «руководства» в этом подвиде деятельности относится к руководству пользователя, руководству администратора и процедурам безопасной установки, генерации и запуска.

Рассмотрение пригодных для использования уязвимостей определяется целями безопасности и функциональными требованиями в ЗБ. Например, если меры по предотвращению обхода функций безопасности не требуются в ЗБ (FPT_PHP «Физическая защита ФБО», FPT_RVM «Посредничество при обращениях» и FPT_SEP «Разделение домена» отсутствуют), то уязвимости, на которых базируется обход, рассматривать не следует.

Уязвимости могут быть или не быть идентифицированы в общедоступных источниках и могут требовать или не требовать навыка для их использования. Эти два фактора являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована только потому, что она идентифицирована в общедоступных источниках.

Следующие термины использованы в данном руководстве с конкретным значением:

a) уязвимость — слабость в ОО, которая может быть использована, чтобы нарушить политику безопасности в некоторой среде;

b) анализ уязвимостей — систематический поиск уязвимостей в ОО и оценка найденных уязвимостей, чтобы сделать заключение об их значимости для предопределенной среды ОО;

c) явная уязвимость — уязвимость, которая является открытой для использования, требующего минимума понимания ОО, технических познаний и ресурсов;

d) потенциальная уязвимость — уязвимость, существование которой в ОО предположено (на основании теоретически допускаемого маршрута нападения), но не подтверждено;

e) пригодная для использования уязвимость — уязвимость, которая может быть использована в предопределенной среде ОО;

f) непригодная для использования уязвимость — уязвимость, которая не может быть использована в предопределенной среде ОО;

g) остаточная уязвимость — непригодная для использования уязвимость, которая могла бы быть использована нарушителем с более высоким потенциалом нападения, чем ожидается в предопределенной среде ОО;

h) тестирование проникновения — тестирование, выполняемое с целью сделать заключение о пригодности к использованию в предопределенной среде ОО идентифицированных потенциальных уязвимостей ОО.

13.10.3.4 Действие AVA_VLA.2.1E

13.10.3.4.1 Шаг оценивания 4:AVA_VLA.2-1

ИСО/МЭК 15408-3 AVA_VLA.2.1C: *Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска способов, которыми пользователь может нарушить ПБО.*

ИСО/МЭК 15408-3 AVA_VLA.2.2C: *Документация анализа уязвимостей должна содержать описание решения в отношении идентифицированных уязвимостей.*

ИСО/МЭК 15408-3 AVA_VLA.2.3C: *Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.*

ИСО/МЭК 15408-3 AVA_VLA.2.4C: *Документация анализа уязвимостей должна содержать логическое обоснование, что ОО с идентифицированными уязвимостями устойчив по отношению к очевидным атакам проникновения.*

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

Предполагается, что анализ уязвимостей, выполненный разработчиком, охватывает поиск разработчиком уязвимостей, по меньшей мере, во всех поставляемых для оценки материалах и общедоступных источниках информации.

Информация в общедоступных источниках является высокодинамичной. Поэтому возможно, что о новых уязвимостях будет сообщено в общедоступных источниках в период между временем, когда

разработчик выполняет анализ уязвимостей, и временем завершения оценки. Моментом прекращения мониторинга информации в общедоступных источниках является выпуск органом оценки результатов оценки; поэтому за указаниями следует обращаться к органу оценки.

13.10.3.4.2 Шаг оценивания 4:AVA_VLA.2-2

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

Уязвимость считают непригодной для использования, если выполнено одно или более условие из следующих условий:

a) функции или меры безопасности в (ИТ или не-ИТ) среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования;

b) уязвимость является пригодной для использования, но только нарушителями, обладающими умеренным или высоким потенциалом нападения. Например, уязвимость распределенного ОО к нападениям, связанным с перехватом сеанса, требует потенциала нападения выше, чем низкий. Такие уязвимости должны быть приведены в ТОО в качестве остаточных уязвимостей;

c) в ЗБ либо не утверждается о противостоянии соответствующей угрозе, либо не утверждается о следовании политике безопасности организации, которая может быть нарушена. Например, для межсетевого экрана, в ЗБ которого не заявлена политика доступности и который уязвим к TCP SYN-атакам (нападение на общепринятый протокол Интернета, которое лишает хосты способности обслуживания запросов на соединение), не следует делать отрицательного заключения по данному действию оценщика только на основе одной этой уязвимости.

Руководство по определению потенциала нападения, необходимого для использования уязвимости, см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

13.10.3.4.3 Шаг оценивания 4:AVA_VLA.2-3

Оценщик должен исследовать материалы анализа уязвимостей, выполненного разработчиком, чтобы сделать заключение, согласуются ли они с ЗБ и руководствами.

Анализ уязвимостей разработчиком может быть направлен на некоторую уязвимость с предложением конкретных конфигураций или настроек функций ОО. Если такие ограничения применения считают действенными и согласованными с ЗБ, то предполагают, что все такие конфигурации/настройки адекватно описаны в руководствах, чтобы их мог применить потребитель.

13.10.3.5 Действие AVA_VLA.2.2E

13.10.3.5.1 Шаг оценивания 4:AVA_VLA.2-4

Оценщик должен подготовить тесты проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик готовит к тестированию проникновения:

a) то, что необходимо, чтобы попытаться опровергнуть анализ разработчика в случаях, когда обоснование разработчиком непригодности уязвимости для использования является, по мнению оценщика, сомнительным;

b) то, что необходимо, чтобы сделать заключение о восприимчивости ОО, находящегося в своей предопределенной среде, к уязвимости, не рассмотренной разработчиком. Оценщику необходимо иметь доступ к текущей информации (например, от органа оценки) о явных уязвимостях из общедоступных источников, которые могли быть не рассмотрены разработчиком; необходимо, чтобы оценщик также мог идентифицировать потенциальные уязвимости в результате выполнения других действий по оценке.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Если в результате исследований в ходе оценки оценщик обнаружит уязвимость, пригодную для использования только нарушителем с большим, чем низкий, потенциалом нападения, то она должна быть приведена в ТОО как остаточная уязвимость.

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности, оценщик рассматривает:

a) интерфейсы функций безопасности, которые будут использованы для инициирования выполнения ФБО и наблюдения их реакции;

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использован для тестирования конкретной уязвимости.

13.10.3.5.2 Шаг оценивания 4:AVA_VLA.2-5

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на материалах анализа уязвимостей, выполненного разработчиком, детализация которой достаточна, чтобы обеспечить воспроизводимость тестов. Тестовая документация должна включать в себя:

a) идентификацию тестируемой уязвимости ОО;

b) инструкции по подключению и настройке всего необходимого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и анализа, который следует проводить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО.

Цель установления данного уровня детализации в тестовой документации — предоставить возможность другому оценщику повторить тесты и получить эквивалентный результат.

13.10.3.5.3 Шаг оценивания 4:AVA_VLA.2-6

Оценщик должен провести тестирование проникновения, основываясь на материалах анализа уязвимостей, выполненного разработчиком.

Оценщик использует документацию для тестов проникновения, подготовленных на шаге оценивания AVA_VLA.2-4, как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может подготовить специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, должны быть внесены в документацию для тестов проникновения. Такие тесты могут быть необходимы, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

13.10.3.5.4 Шаг оценивания 4:AVA_VLA.2-7

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными. Любые различия следует логически обосновать.

13.10.3.5.5 Шаг оценивания 4:AVA_VLA.2-8

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы привести краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки понять выбранный подход к тестированию проникновения, объем выполненного тестирования проникновения, тестируемые конфигурации ОО и общий результат действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были подвергнуты тестированию проникновения;

b) функции безопасности, подвергнутые тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

13.10.3.6 Действие AVA_VLA.2.3E

13.10.3.6.1 Шаг оценивания 4:AVA_VLA.2-9

Оценщик должен исследовать все исходные данные для данного подвида деятельности, чтобы сделать заключение о возможных уязвимостях безопасности, не учтенных ранее при анализе уязвимостей разработчиком.

Следует использовать методологию гипотез о недостатках, посредством которой анализируют спецификации и документацию ОО, а после этого делают предположения об уязвимостях в ОО. Затем перечень предполагаемых уязвимостей упорядочивают по приоритетам на основе оцененной вероятности существования уязвимости, потенциала нападения, требуемого для ее использования, а также возможностей, предоставляющихся нарушителю, или предполагаемого ущерба, который обусловлен конкретной уязвимостью. Упорядоченный по приоритетам перечень потенциальных уязвимостей используют для руководства тестированием проникновения в ОО.

Руководство по определению потенциала нападения, необходимого для использования уязвимости, см. в А.8 «Стойкость функций безопасности и анализ уязвимостей» (приложение А).

Уязвимости, предположительно пригодные для использования только нарушителями, обладающими умеренным или высоким потенциалом нападения, не приводят к отрицательному результату по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то соответствующие уязвимости в дальнейшем не рассматривают в качестве исходных данных для тестирования проникновения. Такие уязвимости приводят в ТОО в качестве остаточных уязвимостей.

Уязвимости, предположительно пригодные для использования нарушителем, обладающим низким потенциалом нападения, которые не вызывают нарушения целей безопасности, указанных в ЗБ, не приводят к отрицательному результату по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то нет необходимости рассматривать соответствующие уязвимости в дальнейшем в качестве исходных данных для тестирования проникновения.

Уязвимости, предполагаемые как потенциально пригодные для использования нарушителем, обладающим низким потенциалом нападения, и приводящие к нарушению целей безопасности, следует отнести к самым высокоприоритетным потенциальным уязвимостям, содержащимся в перечне, используемом непосредственно для тестирования проникновения в ОО.

Исходя из конкретных угроз, присутствующих в предопределенной среде, оценщику при независимом анализе уязвимостей следует рассмотреть характерные уязвимости под каждой из следующих рубрик:

a) уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом оценки;

b) обход;

c) вмешательство;

d) прямые нападения;

e) неправильное применение.

Перечисления b) — e) далее объяснены более детально.

13.10.3.6.1.1 Обход

Обход предполагает любой способ, посредством которого нарушитель мог бы избежать осуществления мер безопасности путем:

a) использования возможностей интерфейсов ОО или утилит, взаимодействующих с ОО;

b) наследования привилегий или других возможностей, которые, наоборот, следовало бы запретить;

c) (когда важна конфиденциальность) чтения чувствительных данных, сохраненных или скопированных в недостаточно защищенные области.

При независимом анализе уязвимостей, выполняемом оценщиком, следует рассмотреть (когда это уместно) каждый из следующих факторов:

a) нападения, основанные на возможностях интерфейсов или утилит, обычно используют в своих целях отсутствие требуемых мер безопасности для этих интерфейсов. Например, получение доступа

к функциональным возможностям, которые реализованы на более низком уровне, чем тот, на котором осуществляется управление доступом. Возможные варианты:

1) изменение предопределенной последовательности вызова функций;

2) выполнение дополнительной функции;

3) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

4) использование подробностей реализации, приведенных в менее абстрактных представлениях;

5) использование задержки между временем проверки доступа и временем использования;

b) изменение предопределенной последовательности вызова компонентов следует рассматривать, когда имеется предопределенный порядок вызова интерфейсов ОО (например, команд пользователя) для выполнения некоторой функции безопасности (например, открытия файла для доступа и затем чтения данных из него). Если функция безопасности вызывается на одном из интерфейсов ОО (например, проверка управления доступом), то оценщику следует рассмотреть, возможен ли обход функции безопасности путем выполнения соответствующего вызова в более поздней точке последовательности или пропуска ее целиком;

c) выполнение дополнительного компонента (в предопределенной последовательности) является формой нападения, похожей на вышеописанную, но включает в себя вызов некоторого другого интерфейса ОО в некоторой точке последовательности. Оно может также включать в себя нападения, основанные на перехвате передаваемых по сети чувствительных данных путем использования анализаторов сетевого трафика (дополнительным компонентом здесь является анализатор сетевого трафика);

d) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает в себя использование для обхода функции безопасности не связанного с ней интерфейса ОО для достижения цели, которая для него не планировалась или не предполагалась. Скрытые каналы являются примером этого типа нападения. Использование недокументированных интерфейсов (которые могут быть небезопасными) также попадает в эту категорию (в том числе и недокументированные возможности по поддержке и помощи);

e) использование подробностей реализации, приведенных в менее абстрактных представлениях, также включает в себя использование скрытых каналов, через которые нарушитель использует в своих целях дополнительные функции, ресурсы или атрибуты, представленные в ОО как последствия процесса усовершенствования (например, использование переменной, обеспечивающей блокировку, в качестве скрытого канала). Дополнительные функциональные возможности также могут быть обеспечены тестовыми фрагментами кода, содержащимися в программных модулях ОО;

f) использование задержки между временем проверки доступа и временем использования включает в себя сценарии, в которых выполняется проверка управления доступом и предоставляется доступ, а нарушитель впоследствии способен создать условия, при которых во время выполнения проверки доступа мог бы произойти сбой проверки доступа. Примером является пользователь, порождающий фоновый процесс для чтения и отправки высокочувствительных данных на терминал пользователя и затем осуществляющий выход из системы и повторный вход в систему на более низком уровне чувствительности. Если фоновый процесс не завершается при выходе пользователя из системы, то проверки в соответствии с мандатным управлением доступом могут быть фактически обойдены;

g) нападения, основанные на наследовании привилегий, базируются главным образом на незаконном приобретении привилегий или возможностей некоторого привилегированного компонента, обычно путем выхода из него неконтролируемым или непредусмотренным способом. Возможные варианты:

1) выполнение данных, не предназначенных для выполнения, или преобразование их в возможные для выполнения;

2) генерация непредусмотренных исходных данных для некоторого компонента;

3) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня;

h) выполнение данных, не предназначенных для выполнения, или преобразование их в возможные для выполнения включает в себя нападения с использованием вирусов (например, помещение в некоторый файл выполняемого кода или команд, автоматически выполняемых при редактировании данного файла или получении доступа к нему, и наследование таким образом привилегий, которые имеет владелец файла);

i) генерация непредусмотренных исходных данных для некоторого компонента может приводить к непредусмотренным результатам, которыми может воспользоваться нарушитель. Например, если ОО является приложением, реализующим функции безопасности, которые можно обойти при получении пользо-

вателем доступа к базовой операционной системе, то возможно получить такой доступ сразу после выполнения входной последовательности, изучая, пока пароль аутентифицируется, результаты ввода различных управляющих или перебираемых последовательностей;

j) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает в себя нападения, основанные на выходе из-под действия ограничений приложения для получения доступа к базовой операционной системе, чтобы обойти функции безопасности, реализуемые приложением. В этом случае предположение, которое нарушается, состоит в том, что для пользователя приложения невозможно получить такой доступ. Подобное нападение можно предвидеть, если функции безопасности реализуются приложением, работающим под управлением системы управления базами данных: при этом есть возможность обхода функций безопасности, если нарушитель сможет выйти из-под действия ограничений приложения;

k) нападения, основанные на чтении чувствительных данных, сохраненных в недостаточно защищенных областях (применимо, когда важна конфиденциальность), включают в себя следующие варианты, рассматриваемые как возможные способы получения доступа к чувствительным данным:

1) сбор «мусора» на диске;

2) доступ к незащищенной памяти;

3) использование доступа к совместно используемым по записи файлам или другим совместно используемым ресурсам (например, к файлам подкачки);

l) активация восстановления после ошибок, чтобы определить, какой доступ пользователи могут получить. Например, после отказа автоматическая система восстановления файлов для файлов без заголовков может использовать каталог для потерянных и найденных файлов, которые присутствуют на диске без меток. Если ОО реализует мандатное управление доступом, то важно исследовать, какой уровень безопасности поддерживается для этого каталога (например, наивысший для системы) и кто имеет доступ к этому каталогу.

13.10.3.6.1.2 Вмешательство

Вмешательство включает в себя любое нападение, основанное на попытке нарушителя повлиять на режим выполнения функции безопасности или механизма (т. е. искажение или блокировка), например, путем:

a) доступа к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности;

b) вынуждения ОО функционировать в необычных или непредусмотренных условиях;

c) отключения или задержки обеспечения безопасности.

В ходе независимого анализа уязвимостей оценщику следует рассмотреть (когда это уместно) каждый из следующих факторов:

a) нападения, основанные на доступе к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности, в том числе:

1) чтение, запись или модификация внутренних данных прямо или косвенно;

2) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

3) использование взаимного влияния компонентов, которые невидимы на более высоком уровне абстракции;

b) чтение, запись или модификация внутренних данных прямо или косвенно охватывает следующие типы нападений, которые необходимо рассмотреть:

1) чтение «секретов», хранимых внутри ОО, таких как пароли пользователей;

2) подмена внутренних данных, на которые полагаются механизмы, обеспечивающие безопасность;

3) изменение переменных среды (например, логических имен) или данных в файлах конфигурации или временных файлах;

c) возможно обмануть доверенный процесс для модификации защищенного файла, к которому этот процесс штатно не должен обращаться;

d) оценщику необходимо также рассмотреть следующие «опасные характеристики»:

1) исходный код вместе с компилятором, постоянно имеющиеся в наличии в ОО (например, возможно изменение исходного кода, связанного с входом в систему);

2) интерактивный отладчик и средства внесения изменений (например, возможно изменение исполняемого образа);

3) возможность внесения изменений на уровне контроллеров устройств, на котором файловой защиты не существует;

4) диагностический код, который присутствует в исходном коде и может быть опционально включен;

5) инструментальные средства разработчика, оставленные в ОО;

e) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает в себя (например) случай, когда ОО является приложением, полагающимся на операционную систему, а пользователи используют знания пакета текстового процессора или другого редактора, чтобы изменить свой собственный командный файл (например, чтобы приобрести большие привилегии);

f) использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, включает в себя нападения, предусматривающие совместный доступ к ресурсам, когда модификация ресурса одним компонентом может влиять на режим выполнения другого (доверенного) компонента, например, на уровне исходного кода, через использование глобальных данных или косвенных механизмов, таких как совместно используемая память или семафоры;

g) следует всегда учитывать нападения, основанные на принуждении ОО функционировать в необычных или непредусмотренных обстоятельствах. Возможные варианты:

1) генерация непредусмотренных исходных данных для некоторого компонента;

2) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня;

h) генерация непредусмотренных исходных данных для компонента включает в себя исследование режима функционирования ОО, когда имеет место:

1) переполнение буферов ввода команд (возможно «разрушение стека» или перезапись другой области хранения, которыми нарушитель может воспользоваться в своих интересах, или принудительная выдача аварийного «дампа», который может содержать чувствительную информацию, такую как открытый текст паролей);

2) ввод неправильных команд или параметров (включая установку параметра в состояние «только для чтения» для интерфейса, который предполагает выдачу данных через этот параметр);

3) вставка маркера конца файла (например, CTRL/Z или CTRL/D) или нулевого символа в журнал аудита;

i) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает в себя нападения, использующие ошибки в исходном коде, где предполагается (явно или неявно), что относящиеся к безопасности данные находятся в конкретном формате или имеют конкретный диапазон значений. В таких случаях оценщику следует, формируя данные в другом формате или присваивая им другие значения, сделать заключение, могут ли нападения привести к нарушению таких предположений и, если это так, может ли это дать преимущества нарушителю;

j) корректный режим выполнения функций безопасности может зависеть от предположений, которые нарушаются в критических обстоятельствах, когда исчерпываются лимиты ресурсов или параметры достигают своего максимального значения. Оценщику следует рассмотреть (если это целесообразно) режим функционирования ОО, когда эти пределы достигнуты, например:

1) изменение дат (например, исследования, как ведет себя ОО при переходе датой критического порога);

2) переполнение дисков;

3) превышение максимального числа пользователей;

4) заполнение журнала аудита;

5) переполнение очередей сигналов безопасности, выдаваемых на консоль;

6) перегрузка различных частей многопользовательского ОО, который сильно зависит от компонентов связи;

7) забивание сети или отдельных хостов трафиком;

8) заполнение буферов или полей;

k) нападения, основанные на отключении или задержке обеспечения безопасности, включают в себя:

1) использование прерываний или функций составления расписаний, чтобы нарушить последовательное выполнение операций;

2) нарушения при параллельном выполнении;

3) использование взаимного влияния между компонентами, которое невидимо на более высоком уровне абстракции;

l) использование прерываний или функций составления расписаний, чтобы нарушить последовательность выполнения операций, включает в себя исследование режима функционирования ОО при:

1) прерывании команды (по CTRL/C, CTRL/Y и т.п.);

2) порождении второго прерывания до того, как будет распознано первое;

m) необходимо исследовать результаты завершения процессов, критических для безопасности (например, демона аудита). Аналогично, возможна такая задержка регистрации записей аудита или выдачи/получения предупреждающих сигналов, что они становятся бесполезными для администратора (так как нападение может уже достичь цели);

n) нарушения при параллельном выполнении предполагают исследование режима функционирования ОО, когда два или более субъекта предпринимают попытку одновременного доступа. Возможно, ОО и справится с блокировкой, необходимой, когда два субъекта предпринимают попытку одновременного доступа, но при этом его поведение станет не полностью определенным при наличии дополнительных субъектов. Например, критичный по безопасности процесс может быть переведен в состояние ожидания получения ресурса, если два других процесса осуществляют доступ к ресурсу, который ему требуется;

o) использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, может обеспечить способ задержки критического по времени доверенного процесса.

13.10.3.6.1.3 Прямые нападения

Прямое нападение включает в себя идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения заявленной минимальной стойкости функций безопасности. При идентификации тестов проникновения оценщику следует учитывать возможность существования уязвимостей вследствие наличия механизмов безопасности, восприимчивых к прямым нападениям.

13.10.3.6.1.4 Неправильное применение

Неправильное применение включает в себя идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения материалов анализа неправильного применения. Факторы, подлежащие рассмотрению:

a) режим функционирования ОО при активации запуска, завершения работы или восстановления после ошибок;

b) режим функционирования ОО в экстремальных условиях (иногда называемых перегрузкой или асимптотическим режимом), в частности, когда это могло бы привести к деактивации или отключению некоторой функции или механизма, направленного на обеспечение безопасности;

c) любая потенциальная возможность неумышленной ошибки в конфигурации или небезопасного использования ОО в результате нападений, указанных выше под рубрикой «Вмешательство».

13.10.3.7 Действие AVA_VLA.2.4E

13.10.3.7.1 Шаг оценивания 4:AVA_VLA.2-10

Оценщик должен подготовить тесты проникновения, основанные на независимом анализе уязвимостей.

Оценщик готовится к тестированию проникновения, основываясь на упорядоченном по приоритетам перечне уязвимостей, предположения о существовании которых были сделаны при выполнении действия оценщика AVA_VLA.2.3E.

Не предполагается тестирования оценщиком уязвимостей, помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости.

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности, оценщик рассматривает:

a) интерфейсы функций безопасности, которые будут использованы для инициирования выполнения ФБО и наблюдения их реакции;

b) начальные условия, которые будут необходимы для выполнения теста (т.е. какие-либо конкретные объекты или субъекты и атрибуты безопасности, которые им необходимо будет иметь);

c) специальное оборудование для тестирования, которое потребуется либо для инициирования функции безопасности, либо для наблюдения за функцией безопасности.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения с помощью ряда наборов тестов, где каждый набор тестов будет использован для тестирования конкретной уязвимости.

13.10.3.7.2 Шаг оценивания 4:AVA_VLA.2-11

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на независимом анализе уязвимостей, детализация которой достаточна, чтобы обеспечить повторяемость тестов. Тестовая документация должна включать в себя:

a) идентификацию явной уязвимости, на предмет которой тестируется ОО;

b) инструкции по подключению и настройке всего необходимого тестового оборудования, как требуется для проведения конкретного теста проникновения;

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

d) инструкции по инициированию ФБО;

e) инструкции по наблюдению режима выполнения ФБО;

f) описание всех ожидаемых результатов и анализа, который следует проводить по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

g) инструкции по завершению теста и установке необходимого посттестового состояния ОО.

Цель данного уровня детализации в тестовой документации — обеспечить возможность другому оценщику повторить тесты и получить эквивалентный результат.

13.10.3.7.3 Шаг оценивания 4:AVA_VLA.2-12

Оценщик должен провести тестирование проникновения, основываясь на независимом анализе уязвимостей.

Оценщик использует документацию для тестов проникновения, подготовленных на шаге оценивания AVA_VLA.2-10, как основу для выполнения тестов проникновения по отношению к ОО, но это не мешает оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может подготовить новые тесты в результате изучения информации в процессе тестирования проникновения, которые, если были выполнены оценщиком, необходимо зафиксировать в документации для тестов проникновения. Такие тесты могут потребоваться, чтобы исследовать непредвиденные результаты или наблюдения, а также потенциальные уязвимости, существование которых оценщик предположил во время предварительно запланированного тестирования.

Если тестирование проникновения показывает, что предполагавшаяся уязвимость не существует, то оценщику следует сделать заключение, был ли или не был корректным собственный анализ оценщика, или не являются ли предоставленные для оценки материалы некорректными или неполными.

13.10.3.7.4 Шаг оценивания 4:AVA_VLA.2-13

Оценщик должен зафиксировать фактические результаты выполнения тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общие результаты должны быть идентичными. Любые различия следует логически обосновать.

13.10.3.7.5 Шаг оценивания 4:AVA_VLA.2-14

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

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления данной информации состоит в том, чтобы дать содержательный краткий обзор усилий оценщика по тестированию проникновения. Это не значит, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных шагов тестирования или результатов отдельных тестов. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органов оценки получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает в себя:

a) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые были подвергнуты тестированию проникновения;

b) функции безопасности, подвергнутые тестированию проникновения. Краткий перечень функций безопасности, на которых было сосредоточено тестирование проникновения;

c) вердикт по данному подвиду деятельности. Общий вывод по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует привести в ТОО.

13.10.3.8 Действие AVA_VLA.2.5E

13.10.3.8.1 Шаг оценивания 4:AVA_VLA.2-15

Оценщик должен исследовать результаты всего тестирования проникновения и выводы по всему анализу уязвимостей, чтобы сделать заключение, является ли ОО, находящийся в своей предопределенной среде, стойким к нарушителю, обладающему низким потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей предопределенной среде, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по этому действию оценщиком должно быть сделано отрицательное заключение.

13.10.3.8.2 Шаг оценивания 4:AVA_VLA.2-16

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

a) ее источник (например, стала известна при выполнении действий ОМО, известна оценщику, прочитана в публикации);

b) связанную с ней функцию (функции) безопасности, недостигнутую цель (цели), нарушенную политику (политики) безопасности организации, реализованную угрозу (угрозы);

c) описание;

d) пригодна ли она для использования в предопределенной среде или нет (т.е. пригодная ли для использования или является остаточной уязвимостью);

e) идентификацию участника оценки (например, разработчик, оценщик), который ее идентифицировал.

14 Подвид деятельности «Устранение недостатков»

14.1 Оценка устранения недостатков (ALC_FLR.1)

14.1.1 Цели

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

14.1.2 Исходные данные

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

14.1.3 Действие ALC_FLR.1.1E

14.1.3.1 Шаг оценивания ALC_FLR.1-1

ИСО/МЭК 15408-3 ALC_FLR.1.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, предпринимаемые разработчиком с момента сообщения о каждом предполагаемом недостатке безопасности до момента реализации решения по нему. Это предполагает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков») процедуры устранения недостатка для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

Хотя эти требования не обязательно определяют способ широкого оповещения пользователей ОО о недостатках безопасности, они обязывают, чтобы все недостатки безопасности, о которых уже имеется сообщение, были отслежены. Таким образом, недостаток безопасности, о котором имеется сообщение, не может быть проигнорирован только потому, что оно поступило не из организации разработчика.

14.1.3.2 Шаг оценивания ALC_FLR.1-2

ИСО/МЭК 15408-3 ALC_FLR.1.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также статуса процесса исправления этого недостатка.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют конкретные действия, которые приняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т.д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙВХОД».

14.1.3.3 Шаг оценивания ALC_FLR.1-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает в себя: предполагаемые недостатки безопасности, о которых выпущено сообщение; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, о которых сообщено, но они еще не были исследованы; недостатки, которые исследуют в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

14.1.3.4 Шаг оценивания ALC_FLR.1-4

ИСО/МЭК 15408-3 ALC_FLR.1.3С: *Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.*

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

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

Если источником недостатка безопасности является ошибка в документации, то действие по исправлению сводят к обновлению соответствующего руководства ОО. Если действие по исправлению является процедурной мерой, то данная мера будет включать в себя обновление соответствующего руководства ОО для отражения этих процедур.

14.1.3.5 Шаг оценивания ALC_FLR.1-5

ИСО/МЭК 15408-3 ALC_FLR.1.4С: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусмотрено на шаге оценивания ALC_FLR.1-2), предписанного действия по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменения документации для обновлений могут быть предоставлены пользователям ОО любым способом, таким как размещение их на веб-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по поиску такой информации.

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

14.2 Оценка устранения недостатков (ALC_FLR.2)

14.2.1 Цели

Цель данного подвида деятельности — сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по их исправлению и доведение информации об этих действиях до пользователей ОО. Дополнительно, по этому подвиду деятельности должно быть сделано заключение, предусматривают ли процедуры разработчика исправление недостатков безопасности, получение сообщений о недостатках от пользователей ОО и обеспечение уверенности, что исправления не приведут ни к каким новым недостаткам безопасности.

Для того чтобы разработчики имели возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представлять сообщения о недостатках безопасности разработчикам, а разработчикам необходимо знать, каким образом получать эти сообщения. Руководство по устранению недостатков, предназначенное для пользователя ОО, обеспечивает осведомленность пользователей ОО о том, как установить связь с разработчиком, а процедуры устранения недостатков описывают роль разработчика при таком взаимодействии.

14.2.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация процедур устранения недостатков;

b) документация руководств по устранению недостатков.

14.2.3 Действие ALC_FLR.2.1E

14.2.3.1 Шаг оценивания ALC_FLR.2-1

ИСО/МЭК 15408-3 ALC_FLR.2.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, предпринимаемые разработчиком с момента сообщения о каждом предполагаемом недостатке безопасности до момента реализации решения по нему. Это предполагает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков») процедуры устранения недостатка для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

14.2.3.2 Шаг оценивания ALC_FLR.2-2

ИСО/МЭК 15408-3 ALC_FLR.2.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также статуса процесса исправления этого недостатка.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют конкретные действия, которые приняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т.д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты

воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙВХОД».

14.2.3.3 Шаг оценивания ALC_FLR.2-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает в себя: предполагаемые недостатки безопасности, о которых выпущено сообщение; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, о которых сообщено, но они еще не были исследованы; недостатки, которые исследуют в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

14.2.3.4 Шаг оценивания ALC_FLR.2-4

ИСО/МЭК 15408-3 ALC_FLR.2.3С: *Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.*

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

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

Если источником недостатка безопасности является ошибка в документации, то действие по исправлению сводят к обновлению соответствующего руководства ОО. Если действие по исправлению является процедурной мерой, то данная мера будет включать в себя обновление соответствующего руководства ОО для отражения этих процедур.

14.2.3.5 Шаг оценивания ALC_FLR.2-5

ИСО/МЭК 15408-3 ALC_FLR.2.4С: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусмотрено на шаге оценивания ALC_FLR.2-2), предписанного действия по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменения документации для обновлений могут быть предоставлены пользователям ОО любым способом, таким как размещение их на веб-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по поиску такой информации.

Наиболее подходящая метрика оценки достаточности метода, используемого для предоставления информации, материалов по исправлению и руководств, — та, которая позволяет надеяться, что пользователи ОО смогут достать или получить их. Для примера рассмотрен метод распространения, при котором необходимые данные размещают на веб-сайте на один месяц, а пользователи ОО осведомлены о том, что это произойдет и когда это произойдет. Он может быть не настолько приемлем или эффективен (как, например, при постоянном размещении на веб-сайте), но все же позволяет пользователю ОО получить необходимую информацию. С другой стороны, если бы информация была размещена на веб-сайте всего лишь на

один час, причем пользователи ОО никак не были оповещены об этом и не знали заранее о времени размещения, то получение ими необходимой информации было бы практически невозможно.

14.2.3.6 Шаг оценивания ALC_FLR.2-6

ИСО/МЭК 15408-3 ALC_FLR.2.5C: *Процедуры устранения недостатков должны описывать средства, с помощью которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, описан ли в них порядок получения разработчиком от пользователей ОО сообщений о предполагаемых недостатках безопасности или запросов на исправление таких недостатков.

Процедуры обеспечивают наличие у пользователей ОО способа связи с разработчиком ОО. Располагая таким способом, пользователь может сообщить о недостатках безопасности, узнать о статусе недостатков безопасности или запросить материалы по исправлению недостатков. Этот способ связи может быть в общем случае частью общих услуг связи для сообщения о проблемах, не относящихся к безопасности.

Использование этих процедур не ограничивается пользователями ОО; однако только пользователям ОО данные процедуры должны быть доведены во всех подробностях. Другие лица из числа имеющих доступ к ОО или возможность ознакомиться с ним могут использовать эти же процедуры представления сообщений разработчику для их предполагаемой последующей обработки. Любые способы представления сообщений разработчику, кроме идентифицированных им, выходят за рамки этого шага оценивания, поэтому нет необходимости рассматривать сообщения, созданные другими способами.

14.2.3.7 Шаг оценивания ALC_FLR.2-7

ИСО/МЭК 15408-3 ALC_FLR.2.6C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены исправления.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить исправление каждого недостатка, о котором получено сообщение.

Процедуры устранения недостатков распространяются на те недостатки безопасности, которые обнаружены и о которых получено сообщение как от участников разработки, так и от пользователей ОО. Процедуры должны быть детализированы в достаточной степени для описания того, как обеспечивается исправление каждого недостатка, о котором получено сообщение. Процедуры содержат обоснованные шаги, которые показывают прогресс в получении окончательного решения.

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

14.2.3.8 Шаг оценивания ALC_FLR.2-8

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить доведение до пользователей ОО действий по исправлению для каждого недостатка безопасности.

Эти процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления действия по исправлению. Процедуры для поставки действий по исправлению должны быть согласованы с целями безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ADO_DEL при включении компонента этого семейства в требования доверия. Например, если аппаратная часть ОО была изначально доставлена курьерской связью, то при обновлении аппаратных средств для устранения недостатков по аналогии ожидалось бы их распределение курьерской связью. Обновления, не связанные с устранением недостатков, выполнялись бы согласно процедурам, сформулированным в документации, удовлетворяющей требованиям ADO_DEL «Поставка».

14.2.3.9 Шаг оценивания ALC_FLR.2-9

ИСО/МЭК 15408-3 ALC_FLR.2.7C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур такие защитные меры, что предполагаемые исправления не приведут к нежелательным последствиям.

Применяя анализ, тестирование или их сочетание, разработчик может уменьшить вероятность того, что исправление недостатка безопасности повлечет за собой нежелательные последствия. Оценщик

определяет, предусматривают ли процедуры во всех деталях, как для данного исправления устанавливается необходимое сочетание анализа и действий по тестированию.

Для случая, когда источником недостатка безопасности является ошибка в документации, оценщик делает также заключение, включают ли в себя процедуры защитные меры по предотвращению противоречий с остальной документацией.

14.2.3.10 Шаг оценивания ALC_FLR.2-10

ИСО/МЭК 15408-3 ALC_FLR.2.8C: *Руководство по устранению недостатков должно описывать средства, с помощью которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.*

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

Данное руководство предоставляет пользователям ОО описание способа связи с разработчиком ОО. Располагая таким способом связи, пользователь может сообщить о недостатках безопасности, узнать о статусе недостатков безопасности или запросить материалы по исправлению недостатков.

14.3 Оценка устранения недостатков (ALC_FLR.3)

14.3.1 Цели

Цель данного подвида деятельности — сделать заключение, установил ли разработчик процедуры устранения недостатков, которые описывают отслеживание недостатков безопасности, идентификацию действий по их устранению и доведение информации об этих действиях до пользователей ОО. Дополнительно, по этому подвиду деятельности должно быть сделано заключение, предусматривают ли процедуры разработчика исправление недостатков безопасности, получение сообщений о недостатках от пользователей ОО, обеспечение уверенности, что исправления не приведут ни к каким новым недостаткам безопасности, определение контактных данных каждого пользователя ОО и своевременное доведение до пользователей ОО действий по их исправлению.

Для того чтобы разработчики имели возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности, пользователям ОО необходимо понимать, как представлять сообщения о недостатках безопасности разработчикам, а разработчикам необходимо знать, каким образом получать эти сообщения. Руководство по устранению недостатков, предназначенное для пользователя ОО, обеспечивает, что пользователи ОО осведомлены о том, как установить связь с разработчиком, а процедуры устранения недостатков описывают роль разработчика при таком взаимодействии.

14.3.2 Исходные данные

Свидетельствами оценки для этого подвида деятельности являются:

a) документация процедур устранения недостатков;

b) документация руководств по устранению недостатков.

14.3.3 Действие ALC_FLR.3.1E

14.3.3.1 Шаг оценивания ALC_FLR.3-1

ИСО/МЭК 15408-3 ALC_FLR.3.1C: *Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, описывает ли она процедуры отслеживания всех ставших известными недостатков безопасности в каждом релизе ОО.

Эти процедуры описывают действия, предпринимаемые разработчиком с момента сообщения о каждом предполагаемом недостатке безопасности до момента реализации решения по нему. Это предполагает временные рамки всей деятельности, связанной с отдельным недостатком, начиная от его обнаружения, включая выяснение, что недостаток является недостатком безопасности, и заканчивая реализацией решения по нему.

Если выявленный недостаток не влияет на безопасность, то не понадобится выполнять (согласно требованиям ALC_FLR «Устранение недостатков») процедуры устранения недостатка для его дальнейшего отслеживания; только при этом необходимо объяснение, почему недостаток не влияет на безопасность.

14.3.3.2 Шаг оценивания ALC_FLR.3-2

ИСО/МЭК 15408-3 ALC_FLR.3.2C: *Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также статуса процесса исправления этого недостатка.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, сопровождается ли применение этих процедур описанием каждого недостатка безопасности с точки зрения его сути и последствий.

Процедуры идентифицируют действия, которые предприняты разработчиком для достаточно детального описания сути и последствий каждого недостатка безопасности, дающего возможность его воспроизведения. Описание сути недостатка безопасности раскрывает, является ли он ошибкой в документации, недостатком в проекте ФБО, недостатком в реализации ФБО и т.д. Описание последствий недостатка безопасности идентифицирует фрагменты реализации ФБО, подвергаемые воздействию, и результаты воздействия на эти фрагменты. Например, недостаток безопасности в реализации может быть в том, что он влияет на идентификацию и аутентификацию, осуществляемую ФБО, разрешая аутентификацию с паролем «ТАЙНЫЙВХОД».

14.3.3.3 Шаг оценивания ALC_FLR.3-3

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, будет ли идентифицировано при применении этих процедур состояние процесса исправления каждого недостатка безопасности.

Процедуры устранения недостатков идентифицируют различные стадии недостатков безопасности. Эта дифференциация, по крайней мере, включает в себя: предполагаемые недостатки безопасности, о которых выпущено сообщение; предполагаемые недостатки безопасности, для которых подтверждено, что они на самом деле являются недостатками безопасности; недостатки безопасности, решение по которым реализовано. Допустимо включение дополнительных стадий (например: недостатки, о которых сообщено, но они еще не были исследованы; недостатки, которые исследуются в настоящее время; недостатки безопасности, для которых решение найдено, но пока не реализовано).

14.3.3.4 Шаг оценивания ALC_FLR.3-4

ИСО/МЭК 15408-3 ALC_FLR.3.3С: *Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.*

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

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

Если источником недостатка безопасности является ошибка в документации, то действие по исправлению сводят к обновлению соответствующего руководства ОО. Если действие по исправлению является процедурной мерой, то данная мера будет включать в себя обновление соответствующего руководства ОО для отражения этих процедур.

14.3.3.5 Шаг оценивания ALC_FLR.3-5

ИСО/МЭК 15408-3 ALC_FLR.3.4С: *Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.*

Оценщик должен исследовать документацию процедур устранения недостатков, чтобы сделать заключение, содержит ли она описание методов, используемых для предоставления пользователям ОО необходимой информации о каждом недостатке безопасности.

Необходимая информация о каждом недостатке безопасности состоит из его описания (не обязательно такого же подробного, как это предусмотрено на шаге оценивания ALC_FLR.3-2), предписанного действия по исправлению и соответствующего руководства по реализации исправления.

Такая информация, материалы по исправлению и изменению документации для обновлений могут быть предоставлены пользователям ОО любым способом, таким как размещение их на веб-сайте, рассылка пользователям ОО или заключение соглашения по инсталляции исправлений разработчиком. В тех случаях, когда способ предоставления этой информации требует действий, инициируемых пользователем ОО, оценщик исследует руководство ОО, чтобы удостовериться, содержит ли оно инструкции по поиску такой информации.

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

Для пользователей ОО, зарегистрированных у разработчика (см. шаг оценивания ALC_FLR.3-12), простого обеспечения доступности этой информации недостаточно. Разработчикам необходимо самим целенаправленно рассылать данную информацию (или уведомление о ее доступности) зарегистрированным пользователям ОО.

14.3.3.6 Шаг оценивания ALC_FLR.3-6

ИСО/МЭК 15408-3 ALC_FLR.3.5C: *Процедуры устранения недостатков должны описывать средства, с помощью которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, описан ли в них порядок получения разработчиком от пользователей ОО сообщений о предполагаемых недостатках безопасности или запросов на исправление таких недостатков.

Процедуры обеспечивают наличие у пользователей ОО способа связи с разработчиком ОО. Располагая таким способом, пользователь может сообщить о недостатках безопасности, узнать о статусе недостатков безопасности или запросить материалы по исправлению недостатков. Этот способ связи может быть в общем случае частью общих услуг связи для сообщения о проблемах, не относящихся к безопасности.

Использование этих процедур не ограничивается пользователями ОО; однако только пользователям ОО данные процедуры должны быть доведены во всех подробностях. Другие лица из числа имеющих доступ к ОО или возможность ознакомиться с ним могут использовать эти же процедуры представления сообщений разработчику для их предполагаемой последующей обработки. Любые способы представления сообщений разработчику, кроме идентифицированных им, выходят за рамки этого шага оценивания, поэтому нет необходимости рассматривать сообщения, созданные другими способами.

14.3.3.7 Шаг оценивания ALC_FLR.3-7

ИСО/МЭК 15408-3 ALC_FLR.3.6C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены исправления.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить исправление каждого недостатка, о котором получено сообщение.

Процедуры устранения недостатков распространяются на те недостатки безопасности, которые обнаружены и о которых получено сообщение как от участников разработки, так и от пользователей ОО. Процедуры детализированы в достаточной степени для описания того, как обеспечивается исправление каждого недостатка, о котором получено сообщение. Процедуры содержат обоснованные шаги, которые показывают прогресс в получении окончательного решения.

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

14.3.3.8 Шаг оценивания ALC_FLR.3-8

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, помогает ли применение этих процедур обеспечить доведение до пользователей ОО действий по исправлению для каждого недостатка безопасности.

Процедуры описывают процесс, выполняемый от момента принятия решения по недостатку безопасности до момента предоставления действия по исправлению. Процедуры для поставки действий по исправлению должны быть согласованы с целями безопасности; они не обязательно идентичны процедурам, используемым для поставки ОО, документированным для удовлетворения ADO_DEL «Поставка» при включении компонента этого семейства в требования доверия. Например, если аппаратная часть ОО была изначально доставлена курьерской связью, то при обновлении аппаратных средств для устранения недостатков по аналогии ожидалось бы их распределение курьерской связью. Обновления, не связанные с

устранением недостатков, выполнялись бы согласно процедурам, сформулированным в документации, удовлетворяющей требованиям ADO_DEL «Поставка».

14.3.3.9 Шаг оценивания ALC_FLR.3-9

ИСО/МЭК 15408-3 ALC_FLR.3.7C: *Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур такие защитные меры, что предполагаемые исправления не приведут к нежелательным последствиям.

Применяя анализ, тестирование или их сочетание, разработчик может уменьшить вероятность того, что исправление недостатка безопасности повлечет за собой нежелательные последствия. Оценщик определяет, предусматривают ли процедуры во всех деталях, как для данного исправления устанавливается необходимое сочетание анализа и действий по тестированию.

Для случая, когда источником недостатка безопасности является ошибка в документации, оценщик делает также заключение, включают ли в себя процедуры защитные меры по предотвращению противоречий с остальной документацией.

14.3.3.10 Шаг оценивания ALC_FLR.3-10

ИСО/МЭК 15408-3 ALC_FLR.3.8C: *Руководство по устранению недостатков должно описывать средства, с помощью которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.*

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

Данное руководство предоставляет пользователям ОО описание способа связи с разработчиком ОО. Располагая таким способом связи, пользователь может сообщить о недостатках безопасности, узнать о статусе недостатков безопасности или запросить материалы по исправлению недостатков.

14.3.3.11 Шаг оценивания ALC_FLR.3-11

ИСО/МЭК 15408-3 ALC_FLR.3.9C: *Процедуры устранения недостатков должны включать в себя процедуру своевременного реагирования для автоматического распространения сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям, для которых эти недостатки могут иметь последствия.*

Оценщик должен исследовать процедуры устранения недостатков, чтобы сделать заключение, предусматривает ли применение этих процедур способ своевременного доведения сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям ОО, для которых эти недостатки могут иметь последствия.

Вопрос своевременности относится к выпуску как сообщений о недостатках безопасности, так и связанных с ними материалов по исправлению. Однако нет необходимости выпускать их одновременно. Считают, что сообщения о недостатках следует формировать и выпускать, как только найдено промежуточное решение, даже если это решение так же радикально, как «Выключить ОО». Аналогично, когда найдено более долговременное (и менее радикальное) решение, его следует издать без лишней задержки.

Нет необходимости в ограничении числа получателей сообщений и исправлений только теми пользователями ОО, для которых данный недостаток безопасности может иметь последствия; допустимо, чтобы до всех пользователей ОО своевременно были доведены такие сообщения и исправления для всех недостатков безопасности.

14.3.3.12 Шаг оценивания ALC_FLR.3-12

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

Автоматическое распространение не подразумевает полного исключения участия человека в распространении. В действительности, метод распространения может состоять полностью из ручных процедур, возможно, с использованием строго контролируемой процедуры, предписывающей усиление мер контроля за выпуском сообщений или материалов по исправлению.

Нет необходимости в ограничении числа получателей сообщений и исправлений только теми пользователями ОО, для которых данный недостаток безопасности может иметь последствия; допустимо, чтобы

до всех пользователей ОО автоматически доводились такие сообщения и исправления для всех недостатков безопасности.

14.3.3.13 Шаг оценивания ALC_FLR.3-13

ИСО/МЭК 15408-3 ALC_FLR.3.10C: *Руководство по устранению недостатков должно описывать средства, с помощью которых пользователи ОО могут регистрироваться у разработчика, чтобы иметь право получать сообщения о недостатках безопасности и исправления.*

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, описан ли в нем способ предоставления пользователям ОО возможности регистрации у разработчика.

Предоставление пользователям ОО возможности регистрации у разработчика означает наличие у каждого пользователя ОО возможности предоставить разработчику свои контактные данные; эти контактные данные используют для обеспечения пользователя ОО информацией, связанной как с недостатками безопасности, которые могли бы иметь последствия для этого пользователя ОО, так и с исправлениями недостатков безопасности. Регистрация пользователя ОО может быть осуществлена как часть стандартных процедур, выполняемых пользователями ОО, чтобы идентифицировать себя у разработчика, зарегистрировать лицензию на программное обеспечение или получать обновления и другую полезную информацию.

Нет необходимости в отдельном зарегистрированном пользователе для каждой инсталляции ОО; в организации вполне достаточно иметь одного зарегистрированного пользователя ОО. Например, корпоративный пользователь ОО может иметь централизованную службу комплектования для всех мест его размещения. В этом случае достаточно осуществлять контакт через службу комплектования для всех мест размещения ОО у корпоративного пользователя и, таким образом, обеспечить для каждой пользовательской инсталляции ОО зарегистрированные контактные данные.

В любом случае необходимо иметь возможность ассоциировать каждый поставленный ОО с конкретной организацией, чтобы обеспечить наличие зарегистрированного пользователя для каждого ОО. Для организаций, имеющих несколько различных адресов, это позволит убедиться в отсутствии пользователей, которых ошибочно будут считать охваченными регистрацией.

Следует отметить, что пользователи ОО не обязаны регистрироваться, но такую возможность им необходимо предоставить. Тем не менее, пользователям, выбравшим регистрацию, необходимо прямо посылать информацию (или уведомление о ее доступности).

14.3.3.14 Шаг оценивания ALC_FLR.3-14

ИСО/МЭК 15408-3 ALC_FLR.3.11C: *В руководстве по устранению недостатков должна быть идентифицирована контактная информация для всех сообщений и запросов по вопросам безопасности, связанных с ОО.*

Оценщик должен исследовать руководство по устранению недостатков, чтобы сделать заключение, идентифицированы ли в нем конкретные контактные данные для всех сообщений и запросов пользователя относительно проблем безопасности, относящихся к ОО.

Руководство включает в себя способ, посредством которого зарегистрированные пользователи ОО могут взаимодействовать с разработчиком, чтобы сообщать ему об обнаруженных недостатках безопасности в ОО или делать запросы относительно обнаруженных недостатков безопасности в ОО.

Приложение А
(обязательное)

Общие указания по оценке

А.1 Цели

Цель настоящего приложения состоит в том, чтобы охватить общие вопросы руководства обеспечением технического подтверждения результатов оценки. Использование такого общего руководства помогает достичь объективности, повторяемости и воспроизводимости работы, выполненной оценщиком.

А.2 Выборка

Настоящий раздел содержит общие указания по осуществлению выборки. Конкретная и подробная информация дана в тех шагах оценивания, соответствующих определенным элементам действий оценщика, где выборку необходимо выполнить.

Выборка — это определенная процедура, выполняемая оценщиком, посредством которой некоторое подмножество требуемой совокупности свидетельств оценки исследуют и полагают репрезентативным (представительным) для совокупности в целом. Это позволяет оценщику получить достаточную уверенность в правильности конкретного свидетельства оценки без его анализа в полном объеме. Выборку проводят для экономии ресурсов при поддержании адекватного уровня доверия. Выборка из свидетельства может приводить к двум результатам:

a) на подмножестве не обнаружено никаких ошибок, что дает оценщику определенную уверенность в том, что совокупность в целом корректна;

b) на подмножестве найдены ошибки, и поэтому правильность совокупности в целом подвергается сомнению. Даже устранение всех обнаруженных ошибок может оказаться недостаточным для получения оценщиком необходимой уверенности, и поэтому оценщику придется либо увеличить размер подмножества, либо прекратить использование выборки для этого конкретного свидетельства.

Выборка — это метод, который может быть использован для получения заслуживающих доверия выводов, когда состав свидетельства относительно однороден по существу, например, если свидетельство является результатом полностью определенного процесса.

В ИСО/МЭК 15408 определены следующие элементы действий оценщика, для которых заведомо применима выборка.

a) ADV_RCR.3.2E: «Оценщик должен сделать независимое заключение о правильности доказательств соответствия, избирательно верифицируя формальный анализ».

b) ATE_IND.*.2E: «Оценщик должен протестировать подмножество ФБО как необходимо, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями».

c) ATE_IND.2.3E: «Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком».

d) AVA_CCA.*.3E: «Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование».

e) AVA_MSU.2.2E и AVA_MSU.3.2E: «Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства».

Кроме того, в ADV_IMP.1.1D содержится требование, чтобы разработчик обеспечил представление реализации только для подмножества ФБО. Выборку подмножества ему следует согласовать с оценщиком. Предоставление разработчиком выборки представления реализации позволяет оценщику как оценить непосредственно предоставленное представление реализации, так и выборочно проверить свидетельство прослеживания требований безопасности в представлениях проекта ОО, чтобы получить уверенность в соответствии между проектом нижнего уровня и представлением реализации.

В дополнение к выборке, предусмотренной в ИСО/МЭК 15408, настоящий стандарт определяет следующие действия, для которых выборка применима:

a) Действие ACM_CAP.*.1E: «Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств».

В этом случае выборка применима для элементов содержания и представления свидетельств ACM_CAP.*.8C и ACM_CAP.*.9C для ОУД3 и ОУД4.

b) Действие ATE_FUN.1.1E: «Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств».

В этом случае выборка применима для элементов содержания и представления свидетельств ATE_FUN.1.3C, ATE_FUN.1.4C и ATE_FUN.1.5C для ОУД2, ОУД3 и ОУД4.

c) Действие ALC_DVS.1.1E: «Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств».

В этом случае выборка применима для элементов содержания и представления свидетельств ALC_DVS.1.2C для ОУД3 и ОУД4.

Выборка в случаях, указанных в ИСО/МЭК 15408 или специально предусмотренных в шагах оценивания методологии, признается как экономичный подход к действиям, выполняемым оценщиком. Выборка в других областях разрешается только в исключительных случаях, там, где выполнение конкретного вида деятельности в целом потребовало бы усилий, непропорциональных другим видам деятельности, и где оно не повысило бы соответственно доверие. В таких случаях потребуется обоснование применения выборки в этой области. Ни тот факт, что ОО является объемным и сложным, ни то, что он имеет много функциональных требований безопасности, не является достаточным обоснованием, так как при оценке объемных и сложных ОО как раз и могут потребоваться большие усилия. Скорее предполагается, что это исключение ограничивается такими случаями, когда подход к разработке ОО дает большое количество материала для конкретного требования ИСО/МЭК 15408, который обычно весь требуется проверить или исследовать, и когда не ожидается, что такое действие повысит соответственно степень доверия.

Выборка нуждается в логическом обосновании, учитывая возможное влияние на цели безопасности и угрозы ОО. Влияние зависит от того, что может быть пропущено в результате выборки. Необходимо также учитывать характер свидетельства, проверяемого выборочно, и требование не игнорировать любые функции безопасности и не снижать их роль.

Следует признать, что выборка из свидетельства, прямо связанного с реализацией ОО (например, результатов теста разработчика), требует подхода, отличного от применяемого при выборке, связанного с вынесением заключения, правильно ли был выполнен процесс. Во многих случаях, когда от оценщика требуется определить, что процесс действительно выполняется, рекомендуется стратегия выборки. Подход здесь отличается от применяемого при выборке результатов тестирования разработчиком, потому что в первом случае речь идет об уверенности в том, что процесс выполняется, а во втором — с определением корректности реализации ОО. Как правило, более объемные выборки должны быть проанализированы в случаях, связанных с правильной реализацией ОО, чем с необходимостью удостовериться, что процесс выполняется.

При выборке рекомендуется соблюдать нижеприведенные принципы:

a) объем выборки следует сопоставить с эффективностью затрат на проведение оценки, он зависит от некоторых характеристик ОО (например, от размеров и сложности ОО, от объема документации), но минимальный объем в 20 % следует принять за норму для выборки из материалов, относящихся к реализации ОО. Там, где выборку осуществляют для получения свидетельства выполнения некоторого процесса (например, контроля посетителей или анализа проекта), задание определенного процента не применяют. Оценщику следует выбрать объем информации, достаточный для получения приемлемой уверенности в выполнении процесса и логически обосновать объем выборки;

b) следует, чтобы выборка была репрезентативна по всем факторам, относящимся к областям применения выборки. В частности, следует, чтобы выборка охватила все разнообразие компонентов, функций безопасности, мест разработки и эксплуатации (если их несколько) и типов аппаратных платформ (если их несколько);

c) заявителя и разработчика не следует заблаговременно информировать о точном составе выборки. При этом следует учитывать необходимость обеспечения своевременности поставки выборки и вспомогательных материалов, например комплексов тестовых программ и оборудования, оценщику в соответствии с графиком проведения оценки;

d) следует, чтобы отбор при выборке по возможности был непредвзятым (не стоит выбирать всегда только первый или последний номер в списке). В идеале отбор следует поручить не оценщику, а кому-то другому.

Ошибки, найденные в выборке, могут быть отнесены к двум категориям — систематическим или случайным. Если ошибка систематическая, следует устранить ее причину и полностью выполнить новую выборку. При надлежащем объяснении разработчика вопрос о случайных ошибках может быть решен без проведения новой выборки, хотя такое объяснение следует подтвердить. Оценщику следует руководствоваться здравым смыслом при определении, увеличить ли объем выборки или использовать другую выборку.

А.3 Анализ непротиворечивости

В настоящем разделе представлено общее руководство по анализу непротиворечивости. Конкретная и подробная информация дана в тех шагах оценивания, соответствующих определенным элементам действий оценщика, где анализ непротиворечивости необходимо выполнить.

Анализ непротиворечивости — это определенная процедура, выполняемая оценщиком, посредством которой выбранную часть одной из поставок для оценки анализируют автономно (на внутреннюю непротиворечивость) или сравнивают с одной или несколькими другими поставками для оценки.

В ИСО/МЭК 15408 различаются несколько типов анализа непротиворечивости.

a) Оценщику необходимо проанализировать внутреннюю непротиворечивость поставки для оценки. Примеры:

- ADV_FSP.1.2C: «Функциональная спецификация должна быть внутренне непротиворечивой»;
- ADV_HLD.1.2C: «Проект верхнего уровня должен быть внутренне непротиворечивым»;
- ADV_IMP.1.2C: «Представление реализации должно быть внутренне непротиворечивым»;
- ADV_LLD.1.2C: «Проект нижнего уровня должен быть внутренне непротиворечивым».

При выполнении анализа внутренней непротиворечивости оценщику необходимо удостовериться, что представленная поставка не содержит неоднозначностей. Поставка для оценки не должна содержать противоречивые формулировки в различных своих составляющих. Например, неформальные, полуформальные или формальные представления одного и того же свидетельства должны быть согласованы между собой.

Оценщику следует учесть, что составляющие поставки для оценки могут быть представлены в нескольких документах (например, процедуры безопасной установки, генерации и запуска могут быть описаны в трех различных документах).

b) Оценщику необходимо проанализировать, согласована ли поставка для оценки с одной или несколькими другими поставками. Примеры:

- AGD_ADM.1.7C: «Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки»;
- AGD_USR.1.5C: «Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки».

При анализе непротиворечивости от оценщика требуется верифицировать согласованность описания функций, параметров безопасности, процедур и событий, относящихся к безопасности, в одном документе с их описанием в других документах, представленных для оценки. Это означает, что оценщику следует учесть возможные противоречия с другими источниками информации. Примерами являются:

- противоречия с другими руководствами по использованию функций безопасности;
- противоречия с ЗБ (например, в части угроз, предположений безопасного использования, не-ИТ-целей безопасности или функций безопасности ИТ);
- применение параметров безопасности, противоречащее их описанию в функциональной спецификации или в проекте нижнего уровня;
- описание событий, относящихся к безопасности, противоречащее информации, содержащейся в проектах верхнего или нижнего уровня;
- несоответствие функций, осуществляющих безопасность, неформальной модели ПБО.

c) Оценщику необходимо проанализировать и то, что поставка для оценки внутренне непротиворечива, и то, что поставка для оценки согласована с другими поставками. Пример:

- AVA_MSU.1.2C: «Руководства должны быть полны, понятны, непротиворечивы и обоснованны».

В этом случае требуется, чтобы руководство в целом удовлетворяло требованию непротиворечивости. Поскольку руководство может содержаться в одном документе или в нескольких отдельных документах, требование относится к непротиворечивости всего руководства как в пределах отдельных документов, так и между ними.

d) Оценщику необходимо проверить результаты анализа, представленные разработчиком и требуемые для демонстрации непротиворечивости. Примеры:

- ADV_SPM.1.3C: «Модель ПБО должна включать в себя обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы»;
- ADV_SPM.1.4C: «Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО».

В указанных случаях свидетельство непротиворечивости представляется разработчиком. Тем не менее, оценщику необходимо уяснить этот анализ и подтвердить его, возможно, даже выполнив, при необходимости, независимый анализ.

Анализ непротиворечивости может быть выполнен исследованием поставки (поставок) для оценки. Оценщику следует принять разумный и структурированный подход к анализу непротиворечивости документов и, возможно, объединить его с другими видами деятельности типа отображения или прослеживания, выполняемых как часть других шагов оценивания. Оценщик может разрешить любые найденные противоречия, обращаясь к формальному описанию при его наличии. Аналогично для уменьшения неоднозначности в поставках возможно использование полуформальной нотации, даже если она не настолько точная, как формальная нотация.

Неоднозначность может возникать явно, например из-за противоречивых формулировок, или неявно, когда формулировки недостаточно точны. При этом пространная формулировка не является, сама по себе, достаточным основанием для принятия отрицательного вердикта по критерию непротиворечивости.

Проверка непротиворечивости поставок для оценки может выявить упущения, из-за которых может потребоваться повторное выполнение завершенных ранее шагов оценивания. Например, проверка непротиворечивости целей безопасности может выявить пропуск одного или нескольких требований безопасности. В этом случае оценщику следует проверить соответствие между целями безопасности и ФБО.

А.4 Зависимости

В общем случае выполнение требуемых видов и подвидов деятельности и действий по оценке возможно в произвольном порядке или параллельно. Тем не менее, имеются различные виды зависимостей, которые необходимо учитывать оценщику. Настоящий подраздел представляет общее руководство по учету зависимостей между различными видами и подвидами деятельности и действиями по оценке.

А.4.1 Зависимости между видами деятельности

В некоторых случаях для различных классов доверия может быть рекомендована или даже потребована определенная последовательность выполнения связанных с ними видов деятельности по оценке. Конкретный пример — вид деятельности по оценке ЗБ. Вид деятельности по оценке ЗБ начинается до выполнения каких-либо видов деятельности по оценке ОО, так как ЗБ обеспечивает основу и контекст их выполнения. Однако сделать итоговое заключение по оценке ЗБ до завершения оценки ОО может оказаться невозможным, так как результаты деятельности по оценке ОО могут привести к изменениям в ЗБ.

А.4.2 Зависимости между подвидами деятельности

Оценщику необходимо учитывать зависимости между компонентами, указанные в ИСО/МЭК 15408-3. Пример такого вида зависимости — AVA_VLA.1 «Анализ уязвимостей разработчиком». В этом компоненте заявлены зависимости от ADV_FSP.1 «Неформальная функциональная спецификация», ADV_HLD.1 «Описательный проект верхнего уровня», AGD_ADM.1 «Руководство администратора» и AGD_USR.1 «Руководство пользователя».

Обычно положительный вердикт по подвиду деятельности можно принять только при успешном завершении всех тех подвидов деятельности, от которых зависит данный подвид деятельности. Например, как правило, положительный вердикт по AVA_VLA.1 может быть принят, если только по подвидам деятельности, относящимся к ADV_FSP.1, ADV_HLD.1, AGD_ADM.1 и AGD_USR.1, также принят положительный вердикт.

Поэтому при определении, будет ли некоторый подвид деятельности влиять на другой подвид деятельности, оценщику следует выяснить, зависит ли этот подвид деятельности от потенциальных результатов оценки любых зависимых подвидов деятельности. Действительно, возможно, что зависимый подвид деятельности сам станет влиять на этот подвид деятельности, требуя выполнить заново ранее завершенные действия.

Существенное влияние приобретают зависимости при обнаружении оценщиком недостатков. Если недостаток идентифицирован в результате проведения одного из подвидов деятельности, положительный вердикт по зависимому подвиду деятельности может оказаться невынесенным до устранения всех недостатков, относящихся к подвиду деятельности, от которого он зависит.

Необходимо отметить, что некоторые компоненты из ИСО/МЭК 15408, например компоненты семейств ASE_INT и ASE_DES, зависимы друг от друга, и поэтому такая ситуация имеет место для каждой последовательности выполнения соответствующих подвидов деятельности.

А.4.3 Зависимости между действиями

Возможно, что результаты, полученные оценщиком во время одного действия, будут использованы при выполнении другого действия. Например, действия по анализу полноты и непротиворечивости не могут быть завершены, пока не завершена проверка содержания и представления свидетельств. Это означает, например, что оценщику рекомендуется оценивать обоснование ПЗ/ЗБ после оценки составляющих частей ПЗ/ЗБ.

А.5 Посещение объектов

В настоящем разделе представлено общее руководство по посещению объектов. Конкретная и подробная информация дана в шагах оценивания тех подвидов деятельности, где предусмотрены такие посещения:

a) «Автоматизация УК» (ACM_AUT);

b) «Возможности УК» (ACM_CAP).*n* (при $n>2$);

c) «Поставка» (ADO_DEL);

d) «Безопасность разработки» (ALC_DVS).

Посещение объектов разработки — полезный способ определения оценщиком, выполняются ли процедуры способом, не противоречащим описанию в документации.

Объекты посещают для того, чтобы ознакомиться:

a) с использованием системы УК, как описано в плане УК;

b) с практическим применением процедур поставки;

c) с применением мер безопасности во время разработки.

Во время оценки часто необходимы несколько встреч оценщика с разработчиком, и один из обычных вопросов рационального планирования — совмещение посещений объектов для уменьшения затрат. Например, можно совмещать посещение объектов для проверки управления конфигурацией, безопасности, обеспечиваемой разработчиком, и выполнения поставок. Могут также оказаться необходимыми несколько посещений одного и того же объекта для проверки всех стадий разработки. Следует учесть, что разработка может происходить в нескольких помещениях одного и того же здания, в нескольких зданиях, расположенных на одной территории, или же в нескольких местах.

Первое посещение объекта следует запланировать на ранних стадиях оценки. Для оценки, которая начинается на стадии разработки ОО, это позволит внести, при необходимости, коррективы. Для оценки, проводимой после завершения разработки ОО, раннее посещение позволит предпринять меры по исправлению, если в применяемых процедурах будут выявлены серьезные неточности, и избежать лишних усилий при оценке.

Интервью также является полезным способом определения, отражают ли задокументированные процедуры то, что делается в действительности. При проведении подобных интервью оценщику следует стремиться к получению более глубокого понимания анализируемых процедур на месте разработки, их практического использования и применения в соответствии с представленными свидетельствами оценки. Такие интервью дополняют, но не заменяют исследование свидетельств оценки.

При подготовке к посещению объекта оценщику следует составить перечень проверок, основанный на представленных свидетельствах оценки. Результаты посещения объекта следует задокументировать.

Посещения объекта необязательны, если, например, место разработки недавно посещалось для другой оценки ОО или ранее было подтверждено следование определенным процедурам согласно ИСО 9000. Тогда следует рассмотреть иные подходы для получения уверенности, предоставляющие эквивалентный уровень доверия (например, проанализировать свидетельства оценки). Любое решение отменить посещение следует принимать после консультации с органом оценки.

А.6 Границы объекта оценки

Идентификатор объекта оценки помещают в ТОО, в сертификат, в ЗБ и в перечень оцененных продуктов. Хотя предметом купли-продажи обычно являются продукты, оценке подвергают ОО.

Нижеследующие материалы были положены в основу определений, используемых в настоящем стандарте, наряду с их взаимосвязями и влиянием на оценку и сертификацию.

А.6.1 Продукт и система

Продукт — это пригодная для использования совокупность аппаратных средств и/или программного обеспечения. Некоторые поставщики имеют возможность объединять совокупность продуктов (например, текстовый процессор, электронную таблицу и графическое приложение), получая, таким образом, уже иной продукт (например, систему автоматизации делопроизводства). Но результирующую совокупность считают продуктом только при условии, что она общедоступна или пригодна для использования либо другими изготовителями, либо ограниченным кругом потребителей.

Система состоит из одного или нескольких продуктов в известной среде эксплуатации. Основное различие между оценкой продукта и оценкой системы заключается в том, что при оценке системы оценщик принимает во внимание реально существующие условия эксплуатации, а не теоретически предполагаемые условия, как это делается при оценке продукта.

А.6.2 Объект оценки

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.

Эта оцениваемая конфигурация идентифицируется достаточно подробно, чтобы различать аппаратные средства, включенные в оцениваемую конфигурацию, от аппаратных средств, которые не включены в нее, несмотря на то, что последние могут являться частью продукта, на котором базируется ОО. Данная идентификация делает очевидным для потенциальных потребителей, какой продукт должен быть приобретен и какие опции конфигурации должны использоваться для того, чтобы ОО работал в безопасном режиме.

А.6.3 Функции безопасности объекта оценки

ФБО представляют собой совокупность тех функций ОО, которые обеспечивают поддержание безопасности ОО в соответствии с ЗБ. Возможно существование таких функций ОО, которые в соответствии с ЗБ не вносят вклада в поддержание безопасности ОО; следовательно, такие функции не являются частью ФБО.

Элементы аппаратных средств ФБО описывают на уровне детализации, соответствующем требованиям доверия, связанным с документацией разработки (функциональная спецификация, проект высокого уровня, проект низкого уровня) и тестовой документацией. Уровень идентификации аппаратных средств определяется влиянием, оказываемым со стороны характеристик данных аппаратных средств на заявленные функции безопасности и меры доверия.

А.6.4 Оценка

Для всех оценок неявно допускается, что ОО является (по определению) продуктом или системой в ее оцениваемой конфигурации; прямое включение этого предположения в перечень предположений при оценке не обязательно. В ходе проведения оценки ОО подвергают тщательному исследованию: анализ выполняют только в рамках оцениваемой конфигурации, тестирование выполняют для этой же оцениваемой конфигурации, пригодные для использования уязвимости выявляют также в рамках оцениваемой конфигурации, а предположения имеют отношение также только к этой же оцениваемой конфигурации. Легкость, с которой конкретная конфигурация ОО может быть нарушена, важна и ее необходимо учитывать при обращении к требованиям семейства AVA_MSU «Неправильное применение». В нем рассматривают стабильность конфигурации ОО и последствия любых случайных или преднамеренных отклонений от нее, которые могут остаться необнаруженными.

Следующий пример представляет три ОО, все они основаны на одном и том же продукте — межсетевом экране виртуальной частной сети (ВЧС), но приводят к различным результатам оценки из-за различий в заданиях по безопасности.

1) Межсетевой экран ВЧС, который конфигурирован таким образом, что функциональные возможности ВЧС отключены. В ЗБ все угрозы связаны с доступом к защищаемой сети из незащищенной сети.

Объектом оценки является межсетевой экран ВЧС, конфигурированный таким образом, что функциональные возможности ВЧС отключены. Если администратор конфигурирует межсетевой экран таким образом, что некоторые или все функции ВЧС будут включены, то продукт окажется не в оцениваемой конфигурации; поэтому его будут считать неоцененным и, таким образом, о его безопасности ничего нельзя будет утверждать.

2) Межсетевой экран ВЧС, в ЗБ которого все угрозы связаны с доступом к защищаемой сети из незащищенной сети.

Объектом оценки является весь межсетевой экран ВЧС целиком. Функции ВЧС являются частью ОО, поэтому одним из вопросов, которые подлежат решению в ходе проведения оценки, является следующий: имеется ли способ получения доступа к защищаемой сети из незащищенной сети через функции ВЧС.

3) Межсетевой экран ВЧС, в ЗБ которого все угрозы связаны либо с доступом к защищаемой сети из незащищенной сети, либо с конфиденциальностью трафика в незащищенной сети.

Объектом оценки является весь межсетевой экран ВЧС целиком. Функции ВЧС являются частью ОО, поэтому одним из вопросов, которые подлежат решению в ходе проведения оценки, является следующий: допускают ли функции ВЧС возможность реализации какой-либо из угроз, описанных в ЗБ.

А.6.5 Сертификация

Из изложенного выше понятно, что оценивание одного и того же продукта с различными ЗБ приводит к различным ОО с различными ФБО. Следовательно, сертификаты, ТОО, ЗБ и элементы перечня оцененных продуктов будут отличаться для таких оценок, чтобы быть полезными потенциальным потребителям.

Для приведенного выше примера трех различных оценок межсетевых экранов видимые различия между соответствующими сертификатами трудноуловимы, поскольку в сертификатах для всех трех межсетевых экранов ВЧС объект оценки будет определен следующим образом:

Продукт — XYZ межсетевой экран в оцененной конфигурации, определенной в задании по безопасности #ABC

с различными идентификаторами ABC для каждого ЗБ.

Поэтому оценщику необходимо удостовериться в адекватном описании ОО в ЗБ в части функциональных возможностей, учитываемых при оценке. Четкое разъяснение жизненно важно, потому что предполагаемые потребители оцененных продуктов будут принимать во внимание ЗБ продуктов, которые они собираются приобрести, чтобы определить, какие функциональные возможности безопасности этих продуктов были оценены.

А.7 Угрозы и требования класса FPT

Автор ПЗ/ЗБ идентифицирует угрозы (не различая при этом угрозы, исходящие от злонамеренных пользователей, и угрозы, проистекающие из некорректностей в реализации, пригодных для использования через внешний интерфейс ФБО) и, исходя из этого, определяет, включать или не включать требования семейств FPT_PHP «Физическая защита ФБО», FPT_SEP «Разделение домена» и/или FPT_RVM «Посредничество при обращениях» в ПЗ/ЗБ. Эти семейства требований предполагают наличие для ОО угрозы физического воздействия, вмешательства пользователей или обхода функций безопасности:

a) требование защиты ФБО непосредственно связано с описанием среды ОО. Там, где явно или неявно присутствует угроза воздействия или обхода, меры противодействия угрозе необходимо обеспечивать с помощью либо ОО, либо его среды;

b) на угрозу воздействия или обхода обычно указывает присутствие в среде ОО недоверенных субъектов (обычно людей-пользователей) при наличии у них мотивации атаки на активы, которые ОО предназначен защищать;

c) при оценивании изложения требований безопасности в ПЗ/ЗБ оценщик определяет потребность в защите ФБО для выполнения целей безопасности и там, где такая потребность установлена, проверяет присутствие функциональных требований для ее удовлетворения. В тех случаях, когда потребность в защите выявлена, но такая защита не обеспечена ни ОО, ни его средой, выносят отрицательный вердикт по подвиду деятельности APE/ASE_REQ по оценке ПЗ/ЗБ.

Необходимо иметь некоторую форму защиты ОО, если он может осуществлять свою политику безопасности. В конечном счете, если ФБО не защищены от искажения, то не имеется никакой гарантии, что функции, осуществляющие его политику, будут выполняться, как ожидается.

Эта защита может быть обеспечена несколькими способами. В операционной системе со многими пользователями, у которых имеется обширный (программный) интерфейс взаимодействия с ОО, ФБО должны быть способны к собственной защите. Однако если ОО имеет ограниченный интерфейс или ограничения при эксплуатации, необходимая защита может быть обеспечена средствами вне ОО.

Автор ПЗ/ЗБ должен выбрать комбинации ФБО, предположений относительно среды ИТ и других предположений, которые обеспечат необходимую собственную защиту ФБО. Оценщик обязан подтвердить, что необходимая защита обеспечивается. В зависимости от ОО и сделанных предположений для необходимой защиты могут быть привлечены функциональные требования безопасности из класса FPT, но при определенных обстоятельствах они могут и не понадобиться.

А.7.1 Объекты оценки, для которых необязательны требования класса FPT

Возможно, что к некоторым ОО (типа встроенного ОО без интерфейса пользователя) рассматриваемые угрозы не относятся. Скорее всего, для ОО, предоставляющего пользователю расширенный интерфейс, будет несостоятельным ПЗ/ЗБ, который/которое содержит эти угрозы, но не имеет требований из семейств FPT_PHP, FPT_RVM и FPT_SEP. ОО, для которых, возможно, нет необходимости в требованиях самозащиты из класса FPT, могут быть разделены на три следующих типа.

А.7.1.1 Объект оценки с ограниченным интерфейсом пользователя

ОО, который предоставляет только ограниченный интерфейс (недоверенному) пользователю, уже этим может установить достаточные ограничения на действия пользователя так, что даже злонамеренный пользователь не будет иметь возможности исказить ОО. Например, прибор, подобный калькулятору или устройству аутентификации пользователя, может иметь малое число клавишей для ввода информации. Интерфейс недоверенного пользователя на коммуникационных устройствах типа маршрутизатора или межсетевого экрана еще более ограничен: пользователи могут связываться только косвенно, обычно через блоки данных или сообщения протоколов.

А.7.1.2 Объект оценки, не осуществляющий соответствующую политику безопасности

Для ОО, не осуществляющего политик управления доступом или информационными потоками, возможно, не имеет никакого значения получение каким-либо пользователем доступа к данным другого пользователя или ФБО. В этом случае нет особой необходимости в разделении пользователей, подразумевающем привлечение FPT_SEP «Разделение домена». Точно так же, если не имеется никаких значительных активов (типа ресурсов ИТ), требующих защиты (например, против отказа в обслуживании), то, возможно, нет смысла в применении требований из класса FPT.

А.7.1.3 Защита обеспечивается средой

Защиту ФБО часто необходимо обеспечить средой ОО, а не самим ОО (например, в случае приложения, выполняемого в доверенной операционной системе, где приложение является объектом оценки). В таких случаях при оценке учитывают, обеспечивают ли механизмы среды требуемую защиту. Предполагается, что меры защиты выполняются правильно, но способ их применения для защиты ОО может влиять на область оценки.

Например, привилегия, назначенная операционной системой объектным файлам в пределах приложения, определит потенциал нарушения приложением политики безопасности операционной системы. Возможны две реализации одного и того же приложения, приводящие к таким различиям в применении мер защиты операционной системы, которые подразумевают существенно различающиеся ФБО. Таким образом, даже там, где механизмы защиты реализованы средой ОО, все же необходимо проверить способ применения этих механизмов до того, как могут быть определены ФБО.

А.7.2 Воздействие на семейства доверия

Включение/исключение в/из ПЗ/ЗБ требований самозащиты из класса FPT затронет следующие требования доверия.

А.7.2.1 ADV

Там, где не существует угрозы воздействия или обхода, оценка сосредоточится на правильном выполнении ФБО. Она будет включать в себя рассмотрение всех функций в пределах ОО, которые прямо или косвенно вносят вклад в осуществление ПБО. Нет необходимости исследовать функции, которые не относятся ни к одной из этих категорий (присутствие в реализации этих функций ошибок, которые могут помешать правильному выполнению ФБО, будет установлено через тестирование ФБО).

Там, где заявлены функции самозащиты, описание их реализации определит механизмы защиты, на основе которых могут быть определены границы ФБО. Идентификация границ и интерфейсов ФБО вместе с определением заявленной эффективности механизмов защиты ФБО позволит ограничить оцениваемую область. Это ограничение исключит функции не из числа ФБО, так как они не могут мешать правильному выполнению ФБО. Во многих случаях в состав ФБО будут включены некоторые функции, которые не вносят вклад в осуществление ПБО, и эти функции придется исследовать в процессе оценки. Те функции, которые определены как не входящие в состав ФБО, оценщику нет необходимости исследовать.

А.7.2.2 AVA_VLA

Анализ уязвимостей в ИСО/МЭК 15408 определяет влияние уязвимостей на функционирование ОО в его предопределенной среде. Если в ЗБ не идентифицированы никакие угрозы воздействия или обхода, то из поиска уязвимостей разработчиком и оценщиком, где требуется, следует рассмотрение таких атак исключить.

А.7.2.3 ATE_IND

В замечаниях по применению для ATE_IND «Независимое тестирование» рекомендуется тестировать известные из общедоступных источников слабые места, которые могли бы иметься у ОО. Такие слабые места, которые дают основу для намерения исказить или обойти ФБО, необходимо рассматривать только тогда, когда идентифицирована подобная угроза.

А.8 Стойкость функций безопасности и анализ уязвимостей

Сравнение показывает, что между анализом стойкости функций безопасности ОО и анализом уязвимостей имеются как существенное сходство, так и существенные различия.

Существенное сходство основано на использовании потенциала нападения. Для обоих видов анализа оценщик определяет минимальный потенциал нападения, требуемый нарушителю, чтобы осуществить нападение, и приходит к заключению относительно возможностей ОО противостоять нападению. В таблицах А.1 и А.2 показаны и далее описаны взаимосвязи между этими видами анализа и потенциалом нападения.

Таблица А.1 — Анализ уязвимостей и потенциал нападения

Компонент анализа уязвимостей	ОО противостоит нарушителю с потенциалом нападения	Остаточные уязвимости способен использовать только нарушитель с потенциалом нападения
VLA.4	Высокий	Неприменимо — успешное нападение за пределами практически возможного
VLA.3	Умеренный	Высокий
VLA.2	Низкий	Умеренный

Таблица А.2 — Стойкость функции безопасности ОО и потенциал нападения

Уровень СФБ	Адекватная защита от нарушителя с потенциалом нападения	Недостаточная защита от нарушителя с потенциалом нападения
Высокая СФБ	Высокий	Неприменимо — успешное нападение за пределами практически возможного
Средняя СФБ	Умеренный	Высокий
Базовая СФБ	Низкий	Умеренный

Существенные различия между этими видами анализа основаны на природе функции безопасности ОО, а также на характере нападения. Анализ стойкости функции безопасности ОО выполняют только для функций безопасности, реализуемых вероятностными или перестановочными механизмами, за исключением тех из них, которые основаны на криптографии. Более того, при анализе предполагается, что вероятностный или перестановочный механизм безопасности реализован безупречно и что функция безопасности используется при нападении с учетом ограничений ее проекта и реализации. Как показано в таблице А.2, уровень СФБ также отражает нападение, описанное в терминах потенциала нападения, для защиты от которого спроектирована функция безопасности, реализуемая вероятностными или перестановочными механизмами.

Анализ уязвимостей применяют ко всем некриптографическим функциям безопасности ОО, включая те из них, механизмы реализации которых, по своей природе, являются вероятностными или перестановочными. В отличие от анализа стойкости не делается никаких предположений относительно корректности проекта и реализации функции безопасности, а также не налагается ограничений на метод нападения или взаимодействие нарушителя с ОО – если нападение возможно, то оно рассматривается в процессе анализа уязвимостей. Как показано в таблице А.1, успешная оценка в соответствии с компонентом доверия, связанным с анализом уязвимостей, отражает уровень угрозы, описанный в терминах потенциала нападения, для защиты от которого спроектированы и реализованы все функции безопасности ОО.

Общее использование понятия потенциала нападения устанавливает связь между утверждениями о СФБ и оценками уязвимостей, но эту связь не следует рассматривать в качестве обязательной привязки утверждения об уровне СФБ и компонента доверия, выбранного из семейства AVA_VLA «Анализ уязвимостей». Например, выбор компонента AVA_VLA.2 «Независимый анализ уязвимостей», который содержит требование о стойкости к нарушителю с низким потенциалом нападения, не сводит выбор оценки СФБ к базовой СФБ. Учитывая, что уязвимость неотъемлемо присутствует в любой функции, реализованной вероятностным или перестановочным механизмом, и что такие функции являются обычно видимыми свойствами общедоступного интерфейса (например, пароль), автор ПЗ/ЗБ может потребовать более высокого уровня стойкости к соответствующим нападениям и может выбрать более высокий уровень СФБ. Минимальное требование к СФБ как «базовая СФБ» необходимо всегда, когда заявлен компонент из семейства AVA_SOF «Стойкость функций безопасности ОО». Заявленный компонент семейства «Анализ уязвимостей» (AVA_VLA) устанавливает нижний уровень требований к СФБ, и, например, требование к СФБ «базовая СФБ» следует рассматривать как не соответствующее выбору компонента AVA_VLA.3 «Умеренно стойкий».

А.8.1 Потенциал нападения

А.8.1.1 Применение потенциала нападения

Потенциал нападения зависит от компетентности, ресурсов и мотивации нарушителя; каждый из этих факторов рассмотрен далее. Потенциал нападения специально рассматривается оценщиком двумя различными способами в процессе оценки ЗБ и при выполнении действий по оценке уязвимостей. В процессе оценки ЗБ оценщик делает заключение, является ли выбор компонентов требований доверия, в особенности компонентов класса AVA «Оценка уязвимостей», соразмерным с потенциалом нападения источника угроз (см. ASE_REQ.1.4C). Случаи, когда требования доверия несоразмерны, могут означать, что либо оценка не будет обеспечивать достаточное доверие, либо оценка будет излишне трудоемкой. В процессе оценки уязвимостей оценщик использует потенциал нападения как способ определения возможности использования идентифицированных уязвимостей в предопределенной среде.

А.8.1.2 Трактовка мотивации

Мотивация является фактором потенциала нападения, который может быть использован, чтобы описать различные аспекты, относящиеся к нарушителю и активам, которые интересуют нарушителя. Во-первых, мотивация может подразумевать определенную вероятность нападения — из угрозы, описанной как высокомотивированная, можно предположить, что нападение неизбежно или что вследствие немотивированной угрозы нападение не ожидается. Однако, за исключением этих двух крайних уровней мотивации, затруднительно, исходя из мотивации, установить вероятность осуществления нападения.

Во-вторых, мотивация может подразумевать определенную ценность актива в денежном или ином выражении для нарушителя или владельца актива. Более ценный актив обусловит, вероятно, более высокую мотивацию по сравнению с менее ценным активом. Однако, кроме общих рассуждений, трудно связать ценность актива

с мотивацией, потому что ценность актива субъективна — она в значительной степени зависит от того, что вкладывает в понятие ценности владелец актива.

В-третьих, мотивация может подразумевать определенную компетентность и ресурсы, с помощью которых нарушитель намеревается осуществить нападение. Можно предположить, что нарушитель с высокой мотивацией, вероятно, приобретет достаточную компетентность и ресурсы, чтобы преодолеть меры защиты актива. И, наоборот, можно предположить, что нарушитель с высокой компетентностью и значительными ресурсами не захочет, используя их, провести нападение, если имеет низкую мотивацию.

В ходе подготовки и проведения оценки, так или иначе, рассматривают все три аспекта мотивации. Первый аспект, вероятность нападения — это то, что может побудить разработчика добиваться оценки. Если разработчик полагает, что у нарушителей имеется достаточная мотивация, чтобы организовать нападение, то оценка может обеспечить доверие к способности ОО помешать усилиям нарушителя. Когда предполагаемая среда полностью определена, например при оценке системы, уровень мотивации нападения может быть известен и повлияет на выбор контрмер.

Рассматривая второй аспект, владелец актива может полагать, что ценность активов (как-либо измеренная) достаточна, чтобы мотивировать нападение на них. Как только оценку посчитают необходимой, рассматривают мотивацию нарушителя для определения методов нападения, которое может быть предпринято, а также компетентность и ресурсы, которые могут быть использованы при этих нападениях. После проведения исследований разработчик способен выбрать соответствующий уровень доверия, в частности компоненты требований из класса AVA, соразмерные с потенциалом нападения для данных угроз. В ходе оценки и, в частности, по результатам завершения вида деятельности по оценке уязвимостей оценщик делает заключение, достаточен ли ОО, функционирующий в предопределенной среде, чтобы помешать нарушителям с идентифицированной компетентностью и ресурсами.

А.8.2 Вычисление потенциала нападения

В настоящем подразделе приведены факторы, которые определяют потенциал нападения, и предоставлено руководство, способствующее устранению некоторой субъективности этого аспекта процесса оценивания. Данный подход следует выбрать, если оценщик не сделает заключение, что этот подход не является надлежащим; в последнем случае требуется логическое обоснование правильности альтернативного подхода.

А.8.2.1 Идентификация и использование

Чтобы нарушитель использовал уязвимость, ее необходимо сначала идентифицировать, а затем использовать. Несмотря на кажущуюся тривиальность, это разделение на самом деле является существенным. Для иллюстрации этого можно рассмотреть уязвимость, которая обнаружена после нескольких месяцев проведения анализа экспертом, и простой метод нападения, опубликованный в Интернете, и сравнить это с уязвимостью, которая широко известна, но требует огромного времени и ресурсов для использования. Понятно, что такие факторы, как время необходимо в этих случаях трактовать по-разному.

Для анализа СФБ проблема использования обычно более важна, так как уязвимости в вероятностных или перестановочных механизмах будут зачастую сами по себе очевидны. Однако это не всегда так. Для криптографических механизмов, например, знание неочевидных уязвимостей может значительно влиять на эффективность нападения «грубой силой». Знание того, что пользователи системы имеют склонность выбирать имена людей в качестве паролей, будет иметь подобный результат. Для оценки уязвимостей выше, чем по AVA_VLA.1 «Анализ уязвимостей разработчиком», начальная идентификация уязвимостей приобретет гораздо более важное значение, так как существование трудных для раскрытия уязвимостей может быть сделано общедоступным, что приведет к тривиальному их использованию.

А.8.2.2 Учитываемые факторы

При анализе потенциала нападения, требуемого для использования уязвимости, необходимо учитывать следующие факторы:

a) идентификация:

1) время, затрачиваемое на идентификацию уязвимости;

2) техническая компетентность специалиста;

3) знание проекта и функционирования ОО;

4) доступ к ОО;

5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для анализа;

b) использование:

1) время, затрачиваемое на использование уязвимости;

2) техническая компетентность специалиста;

3) знание проекта и функционирования ОО;

4) доступ к ОО;

5) аппаратные средства/программное обеспечение ИТ или другое оборудование, требуемое для использования уязвимости.

Во многих случаях эти факторы не являются независимыми и могут в различной степени заменять друг друга. Например, компетентность или аппаратные средства/программное обеспечение могут быть заменой времени. Эти факторы рассмотрены далее.

Время — это время, непрерывно затрачиваемое нарушителем, чтобы идентифицировать или использовать уязвимость. Применительно к данному рассмотрению, «за минуты» означает, что при нападении идентификация и использование уязвимости занимают менее получаса; «за часы» означает нападение, которое может быть успешным менее чем за сутки; «за сутки» означает, что нападение может быть успешным менее чем за месяц, и «за месяцы» означает, что успешное нападение требует, по меньшей мере, месяца.

Компетентность специалиста относится к уровню общих знаний прикладной области или типа продукта (например, операционной системы Unix, протоколов Интернета). Идентифицированными уровнями являются следующие:

a) эксперты хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами и т.п., реализованными в типе продукта или системы, а также с применяемыми принципами и концепциями безопасности;

b) профессионалы хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа;

c) непрофессионал слабо осведомлен по сравнению с экспертом или профессионалом и не обладает специфической компетентностью.

Знание ОО указывает на определенный уровень знаний. Оно отличается от общей компетентности, хотя и связано с ней. Идентифицированными уровнями являются следующие:

a) отсутствие информации об ОО, кроме его назначения;

b) общедоступная информация об ОО (например, полученная из руководства пользователя);

c) чувствительная информация об ОО (например, сведения о содержании проекта).

Здесь требуется внимательность, чтобы отделить информацию, необходимую для идентификации уязвимости, от информации, необходимой для ее использования, особенно в области чувствительной информации. Требовать чувствительную информацию об использовании уязвимости было бы необычно.

Доступ к ОО также является важным обстоятельством и имеет отношение к фактору «время». Идентификация или использование уязвимости может требовать продолжительного доступа к ОО, что может увеличить вероятность обнаружения. Некоторые нападения могут требовать значительных автономных усилий и лишь краткого доступа к ОО для использования уязвимости. Может также потребоваться непрерывный доступ или доступ в виде нескольких сеансов. Применительно к данному рассмотрению, «за минуты» означает, что требуется доступ менее получаса; «за часы» означает, что требуется доступ менее чем сутки; «за сутки» означает, что требуется доступ менее чем месяц, и «за месяцы» означает, что требуется доступ, по меньшей мере, в течение месяца. Когда доступ к ОО не увеличивает вероятность обнаружения (например, смарт-карта в распоряжении нарушителя), этот фактор следует игнорировать.

Аппаратные средства/программное обеспечение ИТ или другое оборудование указывает на оборудование, которое требуется для идентификации или использования уязвимости.

a) Стандартное оборудование — это оборудование либо для идентификации уязвимости, либо для нападения, которое легко доступно нарушителю. Это оборудование может быть частью самого ОО (например, отладчик в операционной системе) или может быть легко получено (например, программное обеспечение, загружаемое из Интернета, или простые сценарии нападения).

b) Специализированное оборудование нелегко доступно нарушителю, но может быть приобретено без значительных усилий. Это может быть покупка небольшого количества оборудования (например, анализатора протоколов) или разработка более сложных сценариев и программ нападения.

c) Заказное оборудование нелегко доступно широкому кругу, поскольку либо может потребоваться его специальная разработка (например, очень сложное программное обеспечение), либо оборудование настолько специализировано, что его распространение является контролируемым и, возможно, даже ограниченным. Или же оборудование может быть очень дорогим. Использование сотен персональных компьютеров, связанных через Интернет, как правило, относится к этой категории.

Компетентность специалиста и знание ОО связаны с информацией, необходимой нарушителям, чтобы быть способными к нападению на ОО. Существует неявная зависимость между компетентностью нарушителя и его способностью эффективно использовать оборудование при нападении. Чем ниже компетентность нарушителя, тем ниже потенциал использования оборудования. Аналогично, чем выше компетентность, тем выше потенциал оборудования, используемого при нападении. Будучи неявной, зависимость между компетентностью и использованием оборудования проявляется не всегда: например, если условия среды предотвращают использование оборудования опытным нарушителем или если кем-то другим созданы и свободно распространяются (например, через Интернет) инструментальные средства нападения, требующие невысокой квалификации для эффективного использования.

A.8.2.3 Подход к вычислению

В предыдущем пункте определены факторы, подлежащие рассмотрению. Однако для проведения стандартной оценки требуется дополнительное руководство. Для поддержки этого процесса предусмотрен следующий подход. Должны быть представлены конкретные числа в целях достижения рейтингов, которые согласуются с соответствующими уровнями оценки.

В таблице А.3 идентифицированы факторы, обсуждавшиеся в предыдущем пункте, и приведены числовые значения, которые поставлены в соответствие с двумя факторами: идентификацией и использованием

уязвимости. При определении потенциала нападения для конкретной уязвимости из каждого столбца для каждого фактора следует выбрать определенное значение (10 значений). При выборе значений должна быть учтена предопределенная среда ОО. Выбранные 10 значений далее суммируют, получая итоговое значение. Это значение затем сверяют с таблицей А.4 для определения рейтинга.

Если значение фактора оказывается близким к границе диапазона, оценщик может использовать значение, усредняющее табличные. Например, если для использования уязвимости требуется доступ к ОО в течение одного часа или если доступ обнаруживается очень быстро, то для этого фактора может быть выбрано значение между 0 и 4. Таблица А.3 предназначена для руководства.

Таблица А.3 — Вычисление потенциала нападения

Фактор	Диапазон	Значение при идентификации уязвимости	Значение при использовании уязвимости
Затрачиваемое время	< 0,5 ч	0	0
	< 1 сут	2	3
	< 1 мес	3	5
	> 1 мес	5	8
	Непрактично	*	*
Компетентность	Непрофессионал	0	0
	Профессионал	2	2
	Эксперт	5	4
Знание ОО	Отсутствие информации	0	0
	Общедоступная информация	2	2
	Чувствительная информация	5	4
Доступ к ОО	< 0,5 ч или необнаруживаемый доступ	0	0
	< 1 сут	2	4
	< 1 мес	3	6
	> 1 мес	4	9
	Непрактично	*	*
Оборудование	Отсутствует	0	0
	Стандартное	1	2
	Специализированное	3	4
	Заказное	5	6
* Означает, что нападение невозможно в пределах тех временных рамок, которые были бы приемлемы для нарушителя. Любое значение «*» указывает на «высокий» рейтинг.			

Для конкретной уязвимости может возникнуть необходимость использовать таблицу неоднократно для различных сценариев нападения (например, попеременно использовать разные значения компетентности в сочетании со значениями факторов времени или оборудования). Следует сохранить наименьшее значение, полученное в результате этих вычислений.

В случае уязвимости, которая уже идентифицирована и информация о которой общедоступна, идентифицируемые значения для нарушителя следует выбирать исходя из раскрытия этой уязвимости в общедоступных источниках, а не из начальной ее идентификации нарушителем.

Затем для получения рейтинга уязвимости следует использовать таблицу А.4.

Таблица А.4 — Рейтинг уязвимостей

Диапазон значений	ОО противостоит нарушителю с потенциалом нападения	Уровень СФБ
< 10	Нет рейтинга	—
10—17	Низкий	Базовый
18—24	Умеренный	Средний
> 24	Высокий	Высокий

Подобный подход не позволяет учесть все обстоятельства и факторы, но должен более точно указывать на уровень противодействия нападениям, требуемый для достижения рейтингов, приведенных в таблице А.4. Другие факторы, такие как расчет на малую вероятность случайных воздействий или вероятность обнаружения атаки до того, как она может быть завершена, не включены в базовую модель, но могут быть использованы оценщиком как логическое обоснование для рейтинга иного, чем тот, на который может указывать базовая модель.

В случаях, когда, например, определяется рейтинг механизма пароля, а реализация ОО такова, что допускается очень мало попыток до ограничения нападения, рейтинг стойкости будет почти полностью связан с вероятностью правильного угадывания пароля в течение этих немногочисленных попыток. Такие меры ограничения обычно рассматривают как часть функции управления доступом, и в то время как сам механизм пароля может получить, например, только рейтинг «средняя СФБ», для функции управления доступом может быть вынесено суждение о рейтинге «высокая СФБ».

В то время как ряд уязвимостей, оцененных по отдельности, может указывать на высокое противодействие нападениям, наличие других уязвимостей может изменять табличные значения так, что комбинация уязвимостей будет свидетельствовать о применимости более низкого общего рейтинга. Таким образом, наличие одной уязвимости может упростить использование другой. Предполагается, что такая оценка является частью анализа уязвимостей разработчиком и оценщиком.

А.8.3 Пример анализа стойкости функции

Ниже представлен анализ СФБ для гипотетического механизма цифрового пароля.

Информация, полученная из ЗБ и свидетельств проекта, показывает, что идентификация и аутентификация предоставляют основу для управления доступом к сетевым ресурсам с терминалов, расположенных далеко друг от друга. Управление физическим доступом к терминалам каким-либо эффективным способом не осуществляется. Управление продолжительностью доступа к терминалу каким-либо эффективным способом не осуществляется. Уполномоченные пользователи системы подбирают себе свои собственные цифровые пароли для входа в систему во время начальной авторизации использования системы и в дальнейшем — по запросу пользователя. Система содержит следующие ограничения на цифровые пароли, выбираемые пользователем:

a) цифровой пароль должен быть не менее четырех и не более шести цифр длиной;

b) последовательные числовые ряды (типа 7,6,5,4,3) не допускаются;

c) повторение цифр не допускается (каждая цифра должна быть уникальной).

Руководство, предоставляемое пользователям на момент выбора цифрового пароля, является таковым, чтобы цифровые пароли были случайны, насколько это возможно, и не связаны каким-либо способом с конкретным пользователем, например с датой рождения.

Число возможных значений цифровых паролей рассчитывают следующим образом:

a) Шаблоны, используемые людьми, являются важным обстоятельством, которое может влиять на подход к поиску возможных значений цифровых паролей и таким образом влиять на СФБ. Допуская самый плохой вариант сценария, когда пользователь выбирает число, состоящее только из четырех цифр, число перестановок цифрового пароля в предположении, что каждая цифра уникальна, равно:

$$7(8)(9)(10) = 5040.$$

b) Число возможных увеличивающихся рядов – семь, как и число убывающих рядов. После отбрасывания этих рядов число возможных значений цифровых паролей равно:

$$5040 - 14 = 5026.$$

На основе дополнительной информации, полученной из свидетельств проекта, в механизме цифрового пароля спроектирована характеристика блокировки терминала. После шестой подряд неудачной попытки аутентификации терминал блокируется на один час. Счетчик неудачной аутентификации сбрасывается через пять минут; таким образом, нарушитель в лучшем случае может осуществить пять попыток ввода цифрового пароля каждые пять минут или 60 вводов цифрового пароля в час.

В среднем нарушитель должен был бы ввести 2513 цифровых паролей более чем за 2513 мин до ввода правильного цифрового пароля. Как результат, в среднем, успешное нападение произошло бы чуть меньше, чем за:

$$\frac{2513\,\text{мин}}{60\,\frac{\text{мин}}{\text{ч}}} \approx 42\,\text{ч}.$$

Используя подход, описанный в предыдущем подразделе, при идентификации следует выбирать значения факторов, минимальные из каждой категории (все 0), так как существование уязвимости в такой функции очевидно. На основании приведенных выше вычислений для непрофессионала является возможным нанести поражение механизму в пределах нескольких суток (при получении доступа к ОО) без использования какого-либо оборудования и без знания ОО, что дает значение 11. Получив результирующую сумму — 11, потенциал нападения, требуемый для осуществления успешной атаки, определяют, по меньшей мере, как умеренный.

Уровни СФБ определены в терминах потенциала нападения в ИСО/МЭК 15408-1, раздел 2. Поскольку для того, чтобы утверждать о базовой СФБ, механизм должен противодействовать нарушителю с низким потенциалом нападения и поскольку механизм цифрового пароля является стойким к нарушителю с низким потенциалом, то этот механизм цифрового пароля, в лучшем случае, соответствует уровню «базовая СФБ».

А.9 Сфера ответственности системы оценки

Настоящий стандарт описывает минимальный объем технической работы, которую необходимо выполнить при оценках, проводимых под контролем органов оценки. Тем не менее, в нем также указаны (как явно, так и неявно) виды деятельности или методы, на которые не распространяется взаимное признание результатов оценки. Для внесения ясности и в целях уточнения границ, показывающих, где заканчивается настоящий стандарт и где начинается методология конкретной системы оценки, ниже перечислены вопросы, оставленные на усмотрение систем. В конкретной системе оценки возможно как решение всех указанных вопросов, так и оставление некоторых из них неопределенными. (Было сделано все возможное для обеспечения полноты приведенного списка; оценщикам, столкнувшимся с вопросом, не приведенным ниже и не рассмотренным в настоящем стандарте, следует проконсультироваться в своей системе оценки, чтобы выяснить, к чьей компетенции относится решение этого вопроса.)

К вопросам, которые могут быть определены в конкретной системе оценки, относятся:

a) необходимое для обеспечения достаточности оценки — каждая система имеет способ (средства) верификации работы ее оценщиков, либо требуя от оценщиков представления результатов работы органу оценки, либо требуя от органа оценки повторения работы оценщика, либо еще каким-то способом, обеспечивающим, что все органы оценки выполняют работу приемлемым образом и выдают сопоставимые результаты;

b) процесс распоряжения свидетельствами оценки после завершения оценки;

c) требования по конфиденциальности (как со стороны оценщика, так и относительно неразглашения информации, полученной в процессе оценки);

d) действия, предпринимаемые при возникновении проблем в процессе оценки (после решения проблемы процесс оценки либо возобновляется, либо немедленно прекращается и исправленный продукт необходимо заново представить для оценки);

e) конкретный (естественный) язык, на котором необходимо представить документацию;

f) документальные свидетельства, которые необходимо представить в составе ТОО; настоящий стандарт определяет минимум, который следует привести в ТОО, а в конкретных системах оценки возможно требование включения дополнительной информации;

g) дополнительные отчеты (помимо ТОО), требуемые от оценщиков, например отчеты о тестировании;

h) любые специфические СП, которые могут потребоваться в соответствии с системой, включая структуру, получателей и т.д. для таких СП;

i) структура конкретного содержания документальных сообщений (отчетов), разрабатываемых при оценке ЗБ, — система оценки может иметь установленный формат для всех сообщений (отчетов), детализирующих результаты оценки, будь это оценка ОО или ЗБ;

j) любая требуемая дополнительно информация по идентификации ПЗ/ЗБ;

k) любые виды деятельности по принятию решения о пригодности сформулированных в явном виде требований в ЗБ;

l) любые требования по подготовке свидетельства оценщика для поддержки переоценки и повторного применения свидетельств;

m) любые конкретные способы применения идентификаторов, эмблем, торговых марок и т.д. системы оценки;

n) любые конкретные указания по применению криптографии;

o) способы трактовки и применения системы оценки, национальных и международных интерпретаций;

p) перечень или описание приемлемых альтернатив тестированию там, где тестирование неосуществимо;

q) механизм, посредством которого орган оценки может определить, какие шаги оценщик предпринял при тестировании;

r) предпочтительный подход при тестировании (если таковой имеется): на внутреннем интерфейсе или на внешнем интерфейсе;

s) перечень или характеристика приемлемых способов (средств) проведения оценщиком анализа уязвимостей (например, методология гипотез о недостатках);

t) информация относительно любых уязвимостей и недостатков, которые необходимо учитывать при оценке.

Приложение В
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица В.1

Обозначение ссылочного международного стандарта	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 15408-1:2005	ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ИСО/МЭК 15408-2:2005	ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ИСО/МЭК 15408-3:2005	ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
ИСО 9000:2000	ГОСТ Р ИСО 9000—2008 Системы менеджмента качества. Основные положения и словарь

УДК 681.324:006.354 ОКС 35.040 П85

Ключевые слова: информационная технология, методология оценки, объект оценки, вид деятельности, шаг оценивания

Редактор *Л. В. Афанасенко*
Технический редактор *В. Н. Прусакова*
Корректор *С. И. Фирсова*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 30.06.2009. Подписано в печать 30.09.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 26,97. Уч.-изд. л. 30,20. Тираж 300 экз. Зак. 871

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru