ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

ISO/IEC 15408-3:2005
Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements (IDT)

Издание официальное

БЗ 12—2007/463

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 № 521-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-3:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» (ISO/IEC 15408-3:2005 «Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements»).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 15408-3—2002

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, уведомления 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, определения, обозначения и сокращения . . . 1
4 Краткий обзор . . . 1
4.1 Структура данной части ИСО/МЭК 15408 . . . 1
5 Парадигма доверия ИСО/МЭК 15408 . . . 2
5.1 Основные принципы ИСО/МЭК 15408 . . . 2
5.2 Подход к доверию . . . 2
5.3 Шкала оценки доверия в ИСО/МЭК 15408 . . . 3
6 Требования доверия к безопасности . . . 3
6.1 Структуры . . . 3
6.2 Классификация компонентов . . . 8
6.3 Структура класса критериев оценки профиля защиты и задания по безопасности . . . 9
6.4 Использование терминов в настоящем стандарте . . . 9
6.5 Классификация доверия . . . 10
6.6 Краткий обзор классов и семейств доверия . . . 11
7 Критерии оценки профиля защиты и задания по безопасности . . . 14
7.1 Краткий обзор . . . 14
7.2 Краткий обзор критериев профиля защиты . . . 14
7.3 Краткий обзор критериев задания по безопасности . . . 15
8 Класс APE. Оценка профиля защиты . . . 16
8.1 Описание ОО (APE_DES) . . . 17
8.2 Среда безопасности (APE_ENV) . . . 17
8.3 Введение ПЗ (APE_INT) . . . 18
8.4 Цели безопасности (APE_OBJ) . . . 18
8.5 Требования безопасности ИТ (APE_REQ) . . . 19
8.6 Требования безопасности ИТ, сформулированные в явном виде (APE_SRE) . . . 21
9 Класс ASE. Оценка задания по безопасности . . . 22
9.1 Описание ОО (ASE_DES) . . . 23
9.2 Среда безопасности (ASE_ENV) . . . 23
9.3 Введение ЗБ (ASE_INT) . . . 24
9.4 Цели безопасности (ASE_OBJ) . . . 24
9.5 Утверждения о соответствии ПЗ (ASE_PPC) . . . 25
9.6 Требования безопасности ИТ (ASE_REQ) . . . 26
9.7 Требования безопасности ИТ, сформулированные в явном виде (ASE_SRE) . . . 27
9.8 Краткая спецификация ОО (ASE_TSS) . . . 29
10 Оценочные уровни доверия . . . 30
10.1 Краткий обзор оценочных уровней доверия . . . 30
10.2 Детализация оценочных уровней доверия . . . 31
10.3 Оценочный уровень доверия 1 (ОУД1), предусматривающий функциональное тестирование . . . 31
10.4 Оценочный уровень доверия 2 (ОУД2), предусматривающий структурное тестирование . . . 32
10.5 Оценочный уровень доверия 3 (ОУД3), предусматривающий методическое тестирование и проверку . . . 33
10.6 Оценочный уровень доверия 4 (ОУД4), предусматривающий методическое проектирование, тестирование и углубленную проверку . . . 34
10.7 Оценочный уровень доверия 5 (ОУД5), предусматривающий полуформальное проектирование и тестирование . . . 35
10.8 Оценочный уровень доверия 6 (ОУД6), предусматривающий полуформальную верификацию проекта и тестирование . . . 36
10.9 Оценочный уровень доверия 7 (ОУД7), предусматривающий формальную верификацию проекта и тестирование . . . 38
11 Классы, семейства и компоненты доверия . . . 39
12 Класс ACM. Управление конфигурацией . . . 39

12.1 Автоматизация УК (ACM_AUT) . . . 40
12.2 Возможности УК (ACM_CAP) . . . 42
12.3 Область УК (ACM_SCP) . . . 47
13 Класс ADO. Поставка и эксплуатация . . . 49
13.1 Поставка (ADO_DEL) . . . 49
13.2 Установка, генерация и запуск (ADO_IGS) . . . 51
14 Класс ADV. Разработка . . . 52
14.1 Функциональная спецификация (ADV_FSP) . . . 55
14.2 Проект верхнего уровня (ADV_HLD) . . . 58
14.3 Представление реализации (ADV_IMP) . . . 63
14.4 Внутренняя структура ФБО (ADV_INT) . . . 65
14.5 Проект нижнего уровня (ADV_LLD) . . . 68
14.6 Соответствие представлений (ADV_RCR) . . . 71
14.7 Моделирование политики безопасности (ADV_SPM) . . . 73
15 Класс AGD. Руководства . . . 75
15.1 Руководство администратора (AGD_ADM) . . . 75
15.2 Руководство пользователя (AGD_USR) . . . 76
16 Класс ALC. Поддержка жизненного цикла . . . 77
16.1 Безопасность разработки (ALC_DVS) . . . 78
16.2 Устранение недостатков (ALC_FLR) . . . 79
16.3 Определение жизненного цикла (ALC_LCD) . . . 82
16.4 Инструментальные средства и методы (ALC_TAT) . . . 84
17 Класс ATE. Тестирование . . . 86
17.1 Покрытие (ATE_COV) . . . 87
17.2 Глубина (ATE_DPT) . . . 89
17.3 Функциональное тестирование (ATE_FUN) . . . 91
17.4 Независимое тестирование (ATE_IND) . . . 93
18 Класс AVA. Оценка уязвимостей . . . 96
18.1 Анализ скрытых каналов (AVA_CCA) . . . 96
18.2 Неправильное применение (AVA_MSU) . . . 99
18.3 Стойкость функций безопасности ОО (AVA_SOF) . . . 102
18.4 Анализ уязвимостей (AVA_VLA) . . . 103
Приложение А (справочное) Перекрестные ссылки между компонентами доверия . . . 108
Приложение В (справочное) Перекрестные ссылки ОУД и компонентов доверия . . . 111
Приложение С (справочное) Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам . . . 112

Введение

Международный стандарт ИСО/МЭК 15408:2005 подготовлен Совместным техническим комитетом ИСО/МЭК СТК 1 «Информационные технологии», Подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ». Идентичный стандарту ИСО/МЭК 15408:2005 текст опубликован организациями-спонсорами проекта «Общие критерии» как «Общие критерии оценки безопасности информационных технологий», версия 2.3 (ОК, версия 2.3).

Второе издание стандарта (ИСО/МЭК 15408:2005) отменяет и заменяет первое издание (ИСО/МЭК 15408:1999), которое подверглось технической переработке.

ИСО/МЭК 15408 под общим наименованием «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» состоит из следующих частей:

- часть 1. Введение и общая модель;
- часть 2. Функциональные требования безопасности;
- часть 3. Требования доверия к безопасности.

Если имеют в виду все три части стандарта, используют обозначение ИСО/МЭК 15408.

Компоненты доверия к безопасности, определенные в данной части ИСО/МЭК 15408, являются основой для выражения требований доверия к безопасности в профиле защиты (ПЗ) или задании по безопасности (ЗБ).

Данные требования устанавливают стандартный способ выражения требований доверия для объекта оценки (ОО). Данная часть ИСО/МЭК 15408 каталогизирует наборы компонентов, семейств и классов доверия. Данная часть ИСО/МЭК 15408 также определяет критерии для оценки ПЗ и ЗБ и представляет оценочные уровни доверия, которые определяют предопределенную ИСО/МЭК 15408 шкалу для рейтинга доверия к ОО, называемую «оценочными уровнями доверия» (ОУД).

Аудитория для этой части ИСО/МЭК 15408 включает в себя потребителей, разработчиков и оценщиков безопасных ИТ-систем и продуктов. Дополнительная информация о потенциальных пользователях ИСО/МЭК 15408 и использовании ИСО/МЭК 15408 группами, которые включают в себя потенциальных пользователей, представлена в ИСО/МЭК 15408-1, раздел 4. Эти группы могут использовать данную часть ИСО/МЭК 15408 следующим образом:

a) потребители используют данную часть ИСО/МЭК 15408, выбирая компоненты, чтобы сформулировать требования доверия для удовлетворения целей безопасности, приведенных в ПЗ или ЗБ, определяя требуемые уровни доверия к безопасности ОО. Более подробная информация о взаимосвязях требований безопасности и целей безопасности приведена в ИСО/МЭК 15408-1, подраздел 5.3;

b) разработчики, несущие ответственность за выполнение существующих или предполагаемых требований безопасности потребителя при разработке ОО, ссылаются на данную часть ИСО/МЭК 15408, интерпретируя утверждения требований доверия и определяя подходы доверия к ОО;

c) оценщики используют требования доверия, определенные в данной части ИСО/МЭК 15408, как обязательное утверждение критериев оценки, которые определяют доверие к ОО и оценивание ПЗ и ЗБ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 3

Требования доверия к безопасности

Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance requirements

Дата введения — 2009—10—01

1 Область применения

Настоящий стандарт устанавливает требования доверия ИСО/МЭК 15408 и включает в себя оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия, собственно компоненты доверия, из которых составлены уровни доверия, и критерии для оценки ПЗ и ЗБ.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий международный стандарт:

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

3 Термины, определения, обозначения и сокращения

В настоящем стандарте применены термины, определения, обозначения и сокращения по ИСО/МЭК 15408-1.

4 Краткий обзор

4.1 Структура данной части ИСО/МЭК 15408

В разделе 5 приведено описание парадигмы, используемой в требованиях доверия к безопасности настоящего стандарта.

В разделе 6 приведена структура представления классов, семейств и компонентов доверия, оценочных уровней доверия и их взаимосвязь, а также дана характеристика классам и семействам доверия, представленным в разделах 12—18.

В разделах 7, 8 и 9 приведено краткое введение в критерии оценки ПЗ и ЗБ, сопровождаемое подробными объяснениями семейств и компонентов, применяемых для этих оценок.

В разделе 10 приведены детализированные определения оценочных уровней доверия.

В разделе 11 приведено краткое введение в классы доверия, за которым следуют разделы с 12 по 18, содержащие детализированные определения этих классов доверия.

В приложении А приведена сводка зависимостей между компонентами доверия.

В приложении В приведены перекрестные ссылки между ОУД и компонентами доверия.

Издание официальное

5 Парадигма доверия ИСО/МЭК 15408

Цель данного раздела состоит в изложении основных принципов и подходов к установлению доверия к безопасности. Данный раздел позволит читателю понять логику построения требований доверия в настоящем стандарте.

5.1 Основные принципы ИСО/МЭК 15408

Основные принципы ИСО/МЭК 15408 состоят в том, что следует четко сформулировать угрозы безопасности и положения политики безопасности организации, а достаточность предложенных мер безопасности должна быть продемонстрирована.

Более того, следует принять меры по уменьшению вероятности наличия уязвимостей, возможности их проявления (то есть преднамеренного использования или непреднамеренной активизации), а также степени ущерба, который может явиться следствием проявления уязвимостей. Дополнительно следует предпринять меры по облегчению последующей идентификации уязвимостей, а также их устранению, ослаблению и/или оповещению об их использовании или активизации.

5.2 Подход к доверию

Основная концепция ИСО/МЭК 15408 — обеспечение доверия, основанное на оценке (активном исследовании) продукта или системы ИТ, которые должны соответствовать определенным критериям безопасности. Оценка была традиционным способом обеспечения доверия и являлась основой предшествующих критериев оценки. Для согласования с существующими подходами в ИСО/МЭК 15408 принят тот же основной принцип. В ИСО/МЭК 15408 предполагается, что проверку правильности документации и разработанного продукта или системы ИТ будут проводить опытные оценщики, уделяя особое внимание области, глубине и строгости оценки.

ИСО/МЭК 15408 не отрицает и не комментирует относительные достоинства других способов получения доверия. Продолжаются исследования альтернативных путей достижения доверия. Если в результате этих исследований будут выявлены другие отработанные альтернативные подходы, то они могут в дальнейшем быть включены в ИСО/МЭК 15408, который структурно организован так, что предусматривает такую возможность.

5.2.1 Значимость уязвимостей

Предполагается, что существуют нарушители, которые будут пытаться активно использовать возможности нарушения политики безопасности как для получения незаконной выгоды, так и для незлонамеренных, но, тем не менее, опасных действий. Нарушители могут также случайно активизировать уязвимости безопасности, причиняя вред организации. При необходимости обрабатывать чувствительную информацию и отсутствии в достаточной степени доверенных продуктов или систем имеется значительный риск из-за отказов ИТ. Поэтому нарушения безопасности ИТ могут вызвать значительные потери.

Нарушения безопасности ИТ возникают вследствие преднамеренного использования или случайной активизации уязвимостей при применении ИТ по назначению.

Следует предпринять ряд шагов для предотвращения уязвимостей, возникающих в продуктах и системах ИТ. По возможности уязвимости должны быть:

a) устранены, то есть следует предпринять активные действия для выявления, а затем удаления или нейтрализации всех уязвимостей, которые могут проявиться;

b) минимизированы, то есть следует предпринять активные действия для снижения до допустимого остаточного уровня возможного ущерба от любого проявления уязвимостей;

c) отслежены, то есть следует предпринять активные действия для обнаружения любой попытки использовать оставшиеся уязвимости с тем, чтобы ограничить ущерб.

5.2.2 Причины уязвимостей

Уязвимости могут возникать из-за недостатков:

a) требований, то есть продукт или система ИТ могут обладать требуемыми от них функциями и свойствами, но содержать уязвимости, которые делают их непригодными или неэффективными в части безопасности;

b) проектирования, то есть продукт или система ИТ не отвечают спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

c) эксплуатации, то есть продукт или система ИТ разработаны в полном соответствии с корректными спецификациями, но уязвимости возникают как результат неадекватного управления при эксплуатации.

5.2.3 Доверие в ИСО/МЭК 15408

Доверие — основа для уверенности в том, что продукт или система ИТ отвечают целям безопасности. Доверие могло бы быть получено путем обращения к таким источникам, как бездоказательное утверждение, предшествующий аналогичный опыт или специфический опыт. Однако ИСО/МЭК 15408 обеспечивает доверие с использованием активного исследования. Активное исследование — это оценка продукта или системы ИТ для определения его свойств безопасности.

5.2.4 Доверие через оценку

Оценка является традиционным способом достижения доверия, и она положена в основу ИСО/МЭК 15408. Методы оценки могут, в частности, включать в себя:

a) анализ и проверку процессов и процедур;

b) проверку того, что процессы и процедуры действительно применяются;

c) анализ соответствия между представлениями проекта ОО;

d) анализ соответствия каждого представления проекта ОО требованиям;

e) верификацию доказательств;

f) анализ руководств;

g) анализ разработанных функциональных тестов и полученных результатов;

h) независимое функциональное тестирование;

i) анализ уязвимостей, включающий в себя предположения о недостатках;

j) тестирование проникновения.

5.3 Шкала оценки доверия в ИСО/МЭК 15408

Основные принципы ИСО/МЭК 15408 содержат утверждение, что большее доверие является результатом приложения больших усилий при оценке и что цель состоит в применении минимальных усилий, требуемых для обеспечения необходимого уровня доверия. Повышение уровня усилий может быть основано на:

a) области охвата, то есть увеличении рассматриваемой части продукта или системы ИТ;

b) глубине, то есть детализации рассматриваемых проектных материалов и реализации;

c) строгости, то есть применении более структурированного и формального подхода.

6 Требования доверия к безопасности

6.1 Структуры

Следующие пункты описывают конструкции, используемые в представлении классов, семейств и компонентов доверия, оценочных уровней доверия, и их взаимосвязь.

Требования доверия, определенные в настоящем стандарте, показаны на рисунке 1. Наиболее общую совокупность требований доверия называют «классом». Каждый класс содержит «семейства» доверия, которые разделены на «компоненты» доверия, содержащие, в свою очередь, «элементы» доверия. Классы и семейства используют для обеспечения таксономии классифицируемых требований доверия, в то время как компоненты применяют непосредственно для спецификации требований доверия в ПЗ/ЗБ.

6.1.1 Структура класса

Структура класса доверия показана на рисунке 1.

6.1.1.1 Имя класса

Каждому классу доверия присвоено уникальное имя. Это имя указывает на тематические разделы, на которые распространяется данный класс доверия.

В настоящем стандарте предусмотрена также уникальная краткая форма имени класса доверия. Она является основным средством для ссылки на класс доверия и включает в себя латинскую букву «А», за которой следуют еще две буквы латинского алфавита, относящиеся к имени класса.

6.1.1.2 Представление класса

Каждый класс доверия имеет вводный подраздел, в котором изложены состав и назначение класса.

6.1.1.3 Семейства доверия

Каждый класс доверия содержит, по меньшей мере, одно семейство доверия. Структура семейств доверия описана в 6.1.2.

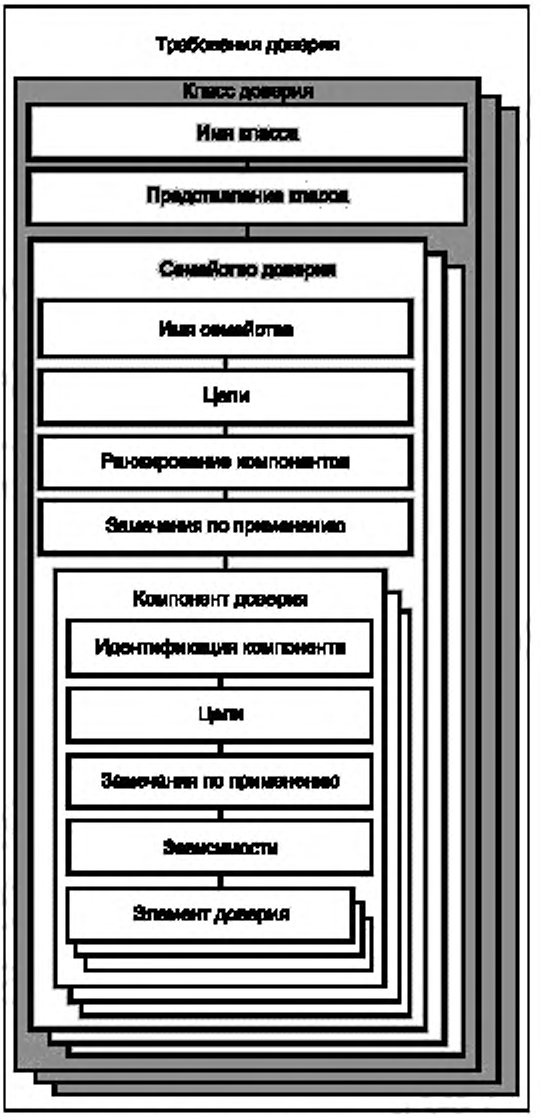


Рисунок 1 — Иерархическая структура представления требований доверия: класс-семейство-компонент-элемент

6.1.2 Структура семейства доверия

Рисунок 1 иллюстрирует структуру семейства доверия.

6.1.2.1 Имя семейства

Каждому семейству доверия присвоено уникальное имя. Это имя содержит описательную информацию по тематическим разделам, на которые распространяется данное семейство доверия. Каждое семейство доверия размещено в пределах класса доверия, который включает в себя другие семейства той же направленности.

В настоящем стандарте предусмотрена также уникальная краткая форма имени семейства доверия. Она является основным средством для ссылки на семейство доверия и включает в себя краткую форму имени класса и символ подчеркивания, за которым следуют три буквы латинского алфавита, относящиеся к имени семейства.

6.1.2.2 Цели

Пункт целей семейства доверия представляет назначение семейства доверия.

В нем изложены цели, для достижения которых предназначено семейство, особенно связанные с парадигмой доверия ИСО/МЭК 15408. Описание целей для семейства доверия представлено в общем виде. Любые конкретные подробности, требуемые для достижения целей, включены в конкретный компонент доверия.

6.1.2.3 Ранжирование компонентов

Каждое семейство доверия содержит один или несколько компонентов доверия. Этот пункт семейства доверия содержит описание имеющихся компонентов и объяснение их отличительных признаков. Его основная цель состоит в указании различий между компонентами при принятии решения о том, что семейство является необходимой или полезной частью требований доверия для ПЗ/ЗБ.

В семействах доверия, содержащих более одного компонента, выполнено ранжирование компонентов и приведено его обоснование. Это обоснование сформулировано в терминах области применения, глубины и/или строгости.

6.1.2.4 Замечания по применению

Необязательный пункт замечаний по применению семейства доверия содержит дополнительную информацию о семействе. Эта информация предназначена непосредственно для пользователей семейства доверия (например, разработчиков ПЗ и ЗБ, проектировщиков ОО, оценщиков). Представление неформально и включает в себя, например предупреждения об ограничениях использования или областях, требующих особого внимания.

6.1.2.5 Компоненты доверия

Каждое семейство содержит как минимум один компонент доверия. Структура компонентов доверия представлена в 6.1.3.

6.1.3 Структура компонента доверия

Структура компонента доверия показана на рисунке 2.



Рисунок 2 — Структура компонента доверия

Отношения между компонентами в пределах семейства показаны в настоящем стандарте с использованием выделения шрифтом. Те части требований, которые являются новыми, расширенными или модифицированными по сравнению с требованиями предыдущего по иерархии компонента, выделены полужирным шрифтом.

6.1.3.1 Идентификация компонента

Пункт идентификации компонента содержит описательную информацию, необходимую для идентификации, категорирования, регистрации и ссылок на компонент.

Каждому компоненту доверия присвоено уникальное имя. Это имя содержит информацию о тематических разделах, на которые распространяется компонент доверия. Каждый компонент доверия входит в состав конкретного семейства доверия, с которым имеет общую цель безопасности.

В настоящем стандарте предусмотрена также уникальная краткая форма имени компонента доверия. Она является основным средством для ссылки на компонент доверия и включает в себя краткую форму имени семейства, после которой ставится точка, а затем — цифра. Цифры для компонентов в пределах каждого семейства назначены последовательно, начиная с единицы.

6.1.3.2 Цели

Необязательный подпункт целей компонента доверия содержит конкретные цели этого компонента. Для компонентов доверия, которые имеют этот подпункт, он включает в себя конкретное назначение данного компонента и подробное разъяснение целей.

6.1.3.3 Замечания по применению

Необязательный подпункт замечаний по применению компонента доверия содержит дополнительную информацию для облегчения использования компонента.

6.1.3.4 Зависимости

Зависимости среди компонентов доверия возникают, если компонент не самодостаточен, а зависит от наличия другого компонента.

Для каждого компонента доверия приведен полный список зависимостей от других компонентов доверия. При отсутствии у компонента идентифицированных зависимостей вместо списка указано: «нет зависимостей». Компоненты из списка могут, в свою очередь, иметь зависимости от других компонентов.

Список зависимостей определяет минимальный набор компонентов доверия, на которые следует полагаться. Компоненты, иерархичные по отношению к компоненту из списка зависимостей, также могут использоваться для удовлетворения данной зависимости.

В отдельных ситуациях указанные в компонентах зависимости могут быть неприменимы. Разработчик ПЗ/ЗБ может отказаться от удовлетворения зависимости, представив обоснование, по каким причинам данная зависимость неприменима.

6.1.3.5 Элементы доверия

Каждый компонент доверия содержит набор элементов доверия. Элемент доверия — требование безопасности, при дальнейшем разделении которого значимый результат оценки не изменяется. Элемент является наименьшим требованием безопасности, распознаваемым в настоящем стандарте.

Каждый элемент доверия принадлежит к одному из трех типов:

1) элементы действий разработчика, определяющие действия, которые должны выполняться разработчиком. Этот набор действий далее уточняется доказательным материалом, упоминаемым в следующем наборе элементов. Требования к действиям разработчика обозначены латинской буквой «D» после номера элемента;

2) элементы содержания и представления свидетельств, определяющие требуемые свидетельства и отражаемую в них информацию, а также, при необходимости, — конкретные характеристики, которыми должны обладать либо ОО, либо данные свидетельства доверия. Требования к содержанию и представлению свидетельств обозначены латинской буквой «С» после номера элемента;

3) элементы действий оценщика, определяющие действия, которые должны выполняться оценщиком. Этот набор действий непосредственно включает в себя подтверждение того, что требования, предписанные элементами содержания и представления свидетельств, выполнены, а также — конкретные действия и анализ, выполняемые в дополнение к уже проведенным разработчиком. Должны также выполняться не указанные в явном виде действия оценщика как результат элементов действий разработчика, не охваченных требованиями к содержанию и представлению свидетельств. Требования к действиям оценщика обозначены латинской буквой «Е» после номера элемента;

Действия разработчика, содержание и представление свидетельств определяют требования, предъявляемые к разработчику по демонстрации доверия к ФБО. Выполняя эти требования, разработчик может повысить уверенность в том, что ОО соответствует функциональным требованиям и требованиям доверия ПЗ или ЗБ.

Действия оценщика определяют его ответственность в двух аспектах. Первый аспект — проверка правильности ПЗ/ЗБ в соответствии с требованиями классов APE «Оценка профиля защиты» и ASE «Оценка задания по безопасности» из разделов 8 и 9 настоящего стандарта. Второй аспект — верификация соответствия ОО его функциональным требованиям и требованиям доверия. Демонстрируя, что ПЗ/ЗБ правильны и их требования выполняются ОО, оценщик может предоставить основание для уверенности в том, что ОО будет соответствовать поставленным целям безопасности.

Элементы действий разработчика, элементы содержания и представления свидетельств и элементы установленных действий оценщика определяют уровень усилий оценщика, которые должны быть приложены при верификации утверждений о безопасности, сформулированных в ЗБ конкретного ОО.

6.1.4 Элементы доверия

Каждый элемент представляет собой требование для выполнения. Формулировки этих требований должны быть четкими, краткими и однозначными. Поэтому в требованиях отсутствуют сложносочиненные предложения. Каждое требование изложено как отдельный элемент.

6.1.5 Структура ОУД

Структура ОУД, определенная в настоящем стандарте, представлена на рисунке 3. Компоненты доверия, содержание которых показано на данном рисунке, включены в ОУД посредством ссылок на компоненты доверия, приведенные в настоящем стандарте.

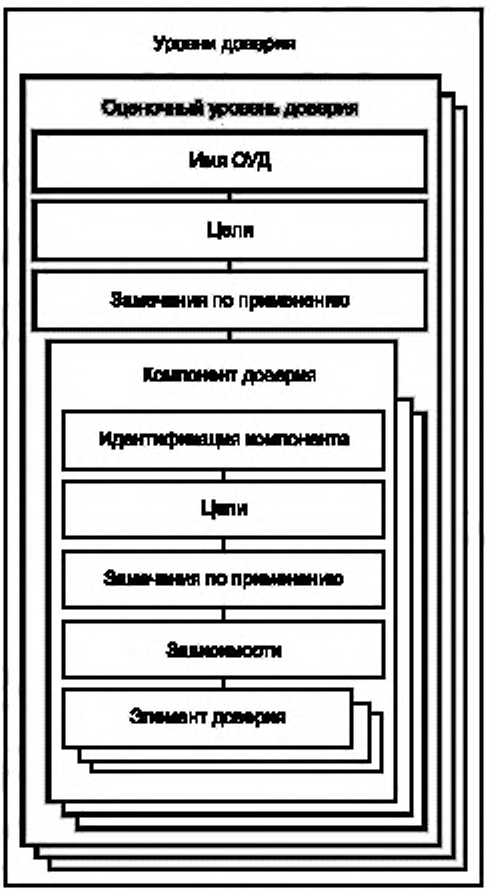


Рисунок 3 — Структура ОУД

6.1.5.1 Имя ОУД

Каждому ОУД присвоено уникальное имя. Имя представляет описательную информацию о предназначении ОУД.

Представлена также уникальная краткая форма имени ОУД. Она является основным средством ссылки на ОУД.

6.1.5.2 Цели

В пункте целей ОУД приведено назначение ОУД.

6.1.5.3 Замечания по применению

Необязательный пункт замечаний по применению ОУД содержит информацию, представляющую интерес для пользователей ОУД (например, для разработчиков ПЗ и ЗБ, проектировщиков ОО, планирующих использование этого ОУД, оценщиков). Представление неформально и включает в себя, например предупреждения об ограничениях использования или областях, требующих особого внимания.

6.1.5.3.1 Компоненты доверия

Для каждого ОУД выбран набор компонентов доверия.

Более высокий уровень доверия, чем предоставляемый данным ОУД, может быть достигнут:

a) включением дополнительных компонентов доверия из других семейств доверия;

b) заменой компонента доверия иерархичным компонентом из этого же семейства доверия.

6.1.5.4 Связь между требованиями и уровнями доверия

Связь между требованиями и уровнями доверия, определенными в настоящем стандарте, показана на рисунке 4. Компоненты доверия состоят из элементов доверия, но последние не могут по отдельности быть включены в уровни доверия. Стрелка на рисунке 4 отображает ссылку в ОУД на компонент доверия внутри класса, в котором он определен.

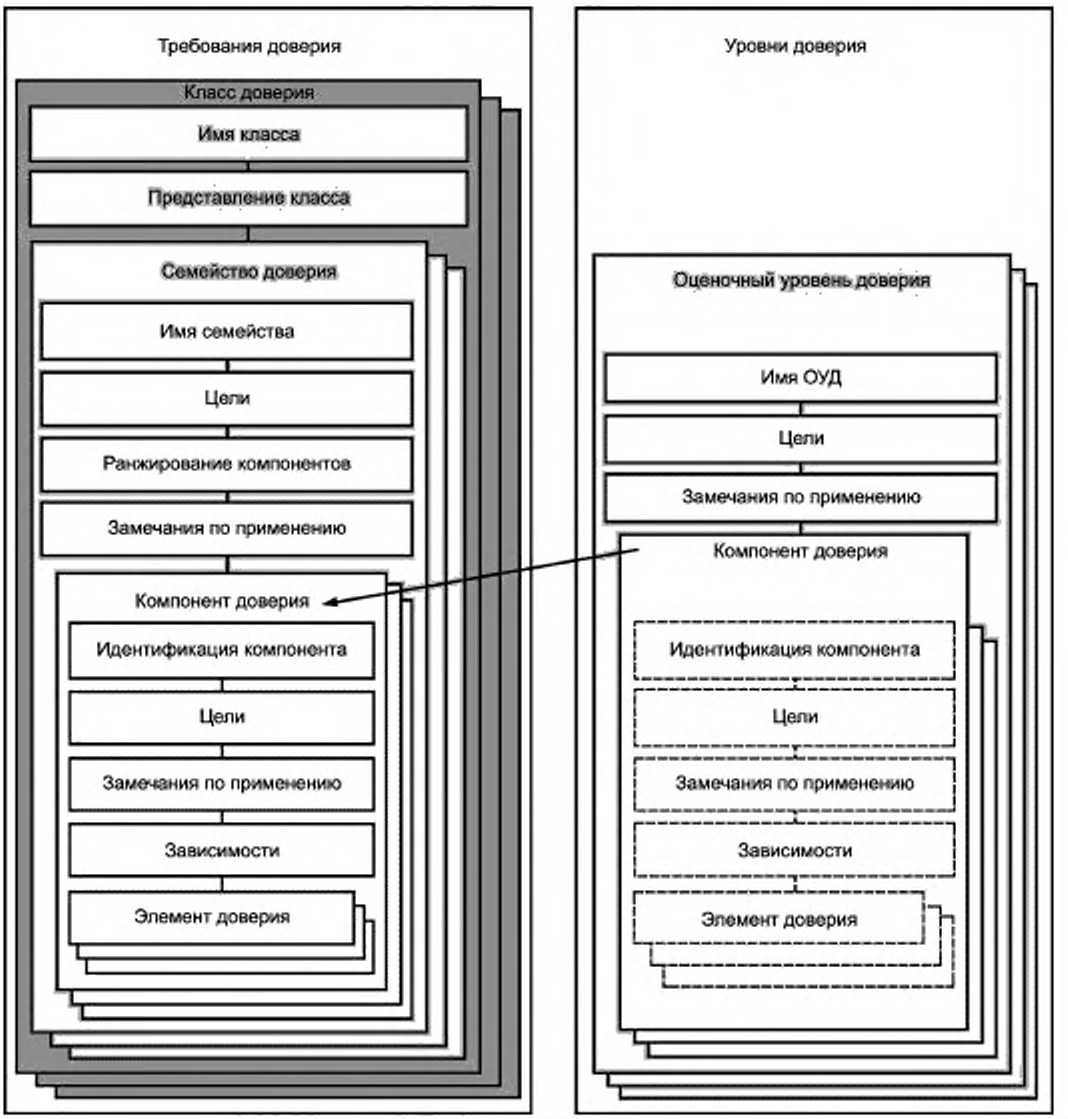


Рисунок 4 — Связь между требованиями и уровнями доверия

6.2 Классификация компонентов

Настоящий стандарт содержит классы семейств и компонентов, сгруппированные на основе, связанной с доверием. В начале каждого класса представлена диаграмма, указывающая на семейства в классе и компоненты в каждом семействе.

Класс, содержащий одно семейство, показан на рисунке 5. Семейство содержит три компонента, являющиеся линейно иерархичными (то есть компонент 2 содержит более высокие, чем компонент 1, требования к конкретным действиям, приводимым свидетельствам или строгости действий и/или свидетельств). Все семейства доверия в настоящем стандарте являются линейно иерархичными, хотя линейность не обязательна для семейств доверия, которые могут быть добавлены в дальнейшем.

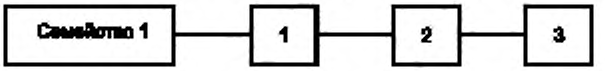


Рисунок 5 — Типовая диаграмма декомпозиции класса

6.3 Структура класса критериев оценки профиля защиты и задания по безопасности

Требования для оценки профиля защиты и задания по безопасности трактуют как классы доверия, структура которых подобна структуре других классов доверия, описанных ниже. Отличие заключается в отсутствии подраздела ранжирования компонентов в описаниях семейств и вызвано тем, что каждое семейство имеет только один компонент.

Названия классов APE и ASE, составляющих их семейств и их краткие имена приведены в таблицах 2, 3, 4, 5 раздела 7 настоящего стандарта. Содержание разделов ПЗ, рассматриваемых в семействах класса APE, представлено в ИСО/МЭК 15408-1, приложение А, а содержание разделов ЗБ, рассматриваемых в семействах класса ASE, — в 15408-1, приложение В.

6.4 Использование терминов в настоящем стандарте

Термины, список которых приведен ниже, используются в настоящем стандарте определенным образом. Они не включены в раздел 2 ИСО/МЭК 15408-1, так как являются общеупотребительными терминами, и их использование, хотя и ограничено приведенными в определениях разъяснениями, согласуется с определениями в словарях. Но именно такое толкование терминов использовалось как руководство при разработке настоящего стандарта, и поэтому оно полезно для общего понимания. В скобках приведены эквиваленты терминов на английском языке.

6.4.1 **логически упорядоченный** (coherent): Сущность логически упорядочена и имеет очевидный смысл. Применительно к документации этот термин относится как к тексту, так и к структуре, указывая, что они понятны потенциальной аудитории.

6.4.2 **непротиворечивый** (consistent): Описывает связь между двумя или более сущностями, указывая, что между ними нет явных противоречий.

6.4.3 **подтверждать** (confirm): Используется для указания необходимости подробного рассмотрения чего-либо; при этом требуется независимое заключение о его достаточности. Требуемый уровень строгости зависит от характера предмета оценки. Применим только к действиям оценщика.

6.4.4 **полный** (complete): Представлены все необходимые составляющие сущности. Применительно к документации это означает, что приведена вся необходимая информация, причем настолько детально, что на данном уровне абстракции дальнейшие пояснения не требуются.

6.4.5 **противостоять** (counter): Используется в том контексте, что некоторая цель безопасности заключается в противостоянии конкретной угрозе, но не обязательно указывает на полную ее ликвидацию.

6.4.6 **демонстрировать** (demonstrate): Относится к анализу, который приводит к заключению, но является менее строгим, чем «доказательство» («proof»).

6.4.7 **описывать** (describe): Требует, чтобы некоторые конкретные подробности сущности были представлены.

6.4.8 **делать заключение** (determine): Требуется независимый анализ для того, чтобы сделать конкретное заключение. Термин отличается от «подтверждать» («confirm») или «верифицировать» («verify»), так как последние подразумевают, что требует проверки анализ, проведенный ранее, в то время как термин «делать заключение» подразумевает совершенно независимый анализ обычно при отсутствии любого предшествующего анализа.

6.4.9 **обеспечивать** (ensure): Подразумевает сильную причинно-следственную связь между некоторым действием и его последствиями. Часто ему предшествует термин «способствует» («helps»), указывающий, что одно данное действие не полностью определяет последствия.

6.4.10 **исчерпывающий** (exhaustive): Используется применительно к проведению анализа или другой деятельности. Аналогичен термину «систематический» («systematic»), но более точен, так как указывает не только на то, что в соответствии с некоторым конкретным планом проведения анализа или другой деятельности был применен методический подход, но также и на то, что этот план достаточен для обеспечения проведения исследования по всем возможным направлениям.

6.4.11 **объяснять** (explain): Отличается от терминов «описывать» («describe») и «демонстрировать» («demonstrate»). Предназначен для ответа на вопрос «Почему?» без попытки аргументировать, что ход предпринимаемых действий обязательно оптимален.

6.4.12 **внутренне непротиворечивый** (internally consistent): Отсутствуют очевидные противоречия между любыми аспектами сущности. Применительно к документации это означает, что в ней не может быть изложено что-либо, что может быть воспринято как противоречащее чему-то другому.

6.4.13 **логическое обоснование** (justification): Относится к анализу, ведущему к заключению, но является более строгим, чем термин «демонстрация» («demonstration»), в смысле точных и подробных объяснений каждого шага логических суждений.

6.4.14 **взаимно поддерживающие** (mutually supportive): Описывает взаимосвязь в группе сущностей, указывая, что последние обладают некоторыми свойствами, которые не находятся в противоречии со свойствами других сущностей и могут способствовать выполнению другими сущностями их задач. Нет необходимости определять, что каждая из рассматриваемых отдельных сущностей непосредственно поддерживает другие сущности в этой группе; достаточно, если сделано обобщенное заключение.

6.4.15 **доказывать** (prove): Относится к формальному анализу в математическом смысле, полностью строгому во всех отношениях. Обычно используется, когда желательно показать соответствие между двумя представлениями ФБО на высоком уровне строгости.

6.4.16 **специфицировать** (specify): Используется в том же контексте, что и «описывать» («describe»), но является более строгим и точным. Аналогичен термину «определять» («define»).

6.4.17 **прослеживать или сопоставлять** (trace): Используется для указания, что между двумя сущностями требуется только минимальный уровень строгости неформального соответствия.

6.4.18 **верифицировать** (verify): Аналогичен термину «подтверждать» («confirm»), но имеет более глубокий смысл. При использовании в контексте действий оценщика указывает на то, что требуются независимые усилия оценщика.

6.5 Классификация доверия

Классы и семейства доверия, а также их краткие имена приведены в таблице 1.

Таблица 1 — Классы и семейства доверия

Класс доверия	Семейство доверия	Краткое имя
ACM: Управление конфигурацией	Автоматизация УК	ACM_AUT
	Возможности УК	ACM_CAP
	Область УК	ACM_SCP
ADO: Поставка и эксплуатация	Поставка	ADO_DEL
	Установка, генерация и запуск	ADO_IGS
ADV: Разработка	Функциональная спецификация	ADV_FSP
	Проект верхнего уровня	ADV_HLD
	Представление реализации	ADV_IMP
	Внутренняя структура ФБО	ADV_INT
	Проект нижнего уровня	ADV_LLD
	Соответствие представлений	ADV_RCR
	Моделирование политики безопасности	ADV_SPM
AGD: Руководства	Руководство администратора	AGD_ADM
	Руководство пользователя	AGD_USR
ALC: Поддержка жизненного цикла	Безопасность разработки	ALC_DVS
	Устранение недостатков	ALC_FLR
	Определение жизненного цикла	ALC_LCD
	Инструментальные средства и методы	ALC_TAT

Окончание таблицы 1

Класс доверия	Семейство доверия	Краткое имя
ATE: Тестирование	Покрытие	ATE_COV
	Глубина	ATE_DPT
	Функциональное тестирование	ATE_FUN
	Независимое тестирование	ATE_IND
AVA: Оценка уязвимостей	Анализ скрытых каналов	AVA_CCA
	Неправильное применение	AVA_MSU
	Стойкость функций безопасности ОО	AVA_SOF
	Анализ уязвимостей	AVA_VLA

6.6 Краткий обзор классов и семейств доверия

Ниже приведены краткие описания классов и семейств доверия из разделов 12 — 18, представленные в том же порядке, в котором они изложены в этих разделах.

6.6.1 Класс ACM: Управление конфигурацией

Управление конфигурацией (УК) помогает обеспечить сохранение целостности ОО, устанавливая и контролируя определенный порядок процессов уточнения и модификации ОО и предоставления связанной с ними информации. УК предотвращает несанкционированную модификацию, добавление или уничтожение составляющих ОО, обеспечивая тем самым доверие, что оцениваются именно те ОО и документация, которые подготовлены к распространению.

6.6.1.1 Автоматизация УК (ACM_AUT)

Семейство «Автоматизация управления конфигурацией» устанавливает уровень автоматизации, используемый для управления элементами конфигурации.

6.6.1.2 Возможности УК (ACM_CAP)

Семейство «Возможности управления конфигурацией» определяет характеристики системы управления конфигурацией.

6.6.1.3 Область УК (ACM_SCP)

Семейство «Область управления конфигурацией» указывает на те элементы ОО, для которых необходим контроль со стороны системы управления конфигурацией.

6.6.2 Класс ADO: Поставка и эксплуатация

Класс доверия ADO «Поставка и эксплуатация» определяет требования к мерам, процедурам и стандартам, применяемым для безопасной поставки, установки и эксплуатации ОО, обеспечивая, чтобы безопасность ОО не нарушалась во время его распространения, установки и эксплуатации.

6.6.2.1 Поставка (ADO_DEL)

Семейство «Поставка» распространяется на процедуры, используемые для поддержки безопасности во время передачи ОО пользователю при первоначальной поставке и последующих модификациях. Данное семейство включает в себя специальные процедуры или действия, необходимые для демонстрации подлинности поставленного ОО. Такие процедуры и меры — основа обеспечения безопасности ОО во время передачи. Несмотря на то, что при оценке ОО не всегда может быть определено его соответствие требованиям поставки, можно оценить процедуры, предусмотренные разработчиком для распространения ОО пользователям.

6.6.2.2 Установка, генерация и запуск (ADO_IGS)

Семейство «Установка, генерация и запуск» предусматривает, чтобы копия ОО была конфигурирована и активизирована администратором так, чтобы показать те же самые свойства защиты, что и у оригинала ОО. Процедуры установки, генерации и запуска обеспечивают уверенность в том, что администратор будет осведомлен о параметрах конфигурации ОО и об их способности повлиять на ФБО.

6.6.3 Класс ADV: Разработка

Класс доверия ADV «Разработка» определяет требования для пошагового уточнения ФБО, начиная с краткой спецификации ОО в ЗБ и до фактической реализации. Каждое из получаемых представлений ФБО содержит информацию, помогающую оценщику решить, были ли выполнены функциональные требования к ОО.

6.6.3.1 Функциональная спецификация (ADV_FSP)

Функциональная спецификация описывает ФБО и должна быть полным и точным отображением функциональных требований безопасности ОО. Функциональная спецификация также детализирует внешний интерфейс ОО. Предполагается, что пользователи ОО взаимодействуют с ФБО через этот интерфейс.

6.6.3.2 Проект верхнего уровня (ADV_HLD)

Проект верхнего уровня — проектная спецификация самого высокого уровня, уточняющая функциональную спецификацию ФБО в основных составляющих частях ФБО. Проект верхнего уровня идентифицирует базовую структуру ФБО, а также основные элементы аппаратных, программных и программно-аппаратных средств.

6.6.3.3 Представление реализации (ADV_IMP)

Представление реализации — наименее абстрактное представление ФБО. Оно фиксирует детализированное внутреннее содержание ФБО на уровне исходного текста, аппаратных схем и т.п.

6.6.3.4 Внутренняя структура ФБО (ADV_INT)

Требования к внутренней структуре ФБО определяют необходимое внутреннее структурирование ФБО.

6.6.3.5 Проект нижнего уровня (ADV_LLD)

Проект нижнего уровня — детализированная проектная спецификация, уточняющая проект верхнего уровня до уровня детализации, который может быть использован как основа для программирования и/или проектирования аппаратуры.

6.6.3.6 Соответствие представлений (ADV_RCR)

Соответствие представлений — демонстрация отображения между всеми смежными парами имеющихся представлений ФБО, от краткой спецификации ОО до наименее абстрактного из имеющихся представлений ФБО.

6.6.3.7 Моделирование политики безопасности (ADV_SPM)

Модели политики безопасности — структурированные представления политик безопасности ПБО, используемые для обеспечения повышенного доверия к тому, что функциональная спецификация соответствует политикам безопасности из ПБО и, в конечном счете, функциональным требованиям безопасности ОО. Это достигается посредством определения соответствия между функциональной спецификацией, моделью политики безопасности и моделируемыми политиками безопасности.

6.6.4 Класс AGD: Руководства

Класс доверия AGD «Руководства» определяет требования, направленные на обеспечение понятности, достаточности и законченности эксплуатационных документов, представляемых разработчиком. Данные документы, содержащие две категории информации (для пользователей и администраторов), являются важным фактором безопасной эксплуатации ОО.

6.6.4.1 Руководство администратора (AGD_ADM)

Требования к руководству администратора способствуют обеспечению того, что ограничения среды будут поняты администраторами и операторами ОО. Руководство администратора — основное средство, имеющееся в распоряжении разработчика, для предоставления администраторам ОО детальной и точной информации о том, как осуществлять администрирование ОО безопасным способом и эффективно использовать привилегии ФБО и функции защиты.

6.6.4.2 Руководство пользователя (AGD_USR)

Требования к руководству пользователя способствуют обеспечению того, что пользователи могут эксплуатировать ОО безопасным способом (например, ограничения использования, предусмотренные ПЗ или ЗБ, необходимо четко объяснить и проиллюстрировать). Руководство пользователя — основное средство, имеющееся в распоряжении разработчика, для предоставления пользователям ОО необходимой общей и специфической информации о том, как правильно использовать функции защиты ОО. В руководстве необходимо осветить два аспекта. Во-первых, требуется объяснить, что делают доступные пользователю функции безопасности и как они будут использоваться, чтобы пользователи имели возможность последовательно и действенно защищать свою информацию. Во-вторых, требуется разъяснить роль пользователя в поддержании безопасности ОО.

6.6.5 Класс ALC: Поддержка жизненного цикла

Класс доверия ALC «Поддержка жизненного цикла» определяет требования доверия посредством принятия для всех этапов разработки ОО четко определенной модели жизненного цикла, включая политики и процедуры устранения недостатков, правильное использование инструментальных средств и методов, а также меры безопасности среды разработки.

6.6.5.1 Безопасность разработки (ALC_DVS)

Семейство «Безопасность разработки» охватывает физические, процедурные, относящиеся к персоналу и другие меры безопасности, используемые применительно к среде разработки. Данное семейство также содержит требования к физической безопасности местоположения разработки и контролю за отбором и наймом персонала разработчиков.

6.6.5.2 Устранение недостатков (ALC_FLR)

Семейство «Устранение недостатков» обеспечивает отслеживание и исправление недостатков, обнаруженных потребителями ОО, пока ОО сопровождается разработчиком. Несмотря на то, что при оценке ОО не может быть принято решение о потенциальном соответствии требованиям устранения недостатков, можно оценить политики и процедуры, которые разработчик предусмотрел для выявления и устранения недостатков и распространения исправлений потребителям.

6.6.5.3 Определение жизненного цикла (ALC_LCD)

Семейство «Определение жизненного цикла» устанавливает, что технология разработки, используемая разработчиком для создания ОО, включает в себя положения и действия, указанные в требованиях к процессу разработки и поддержке эксплуатации. Уверенность в соответствии ОО требованиям больше, если анализ безопасности и подготовка свидетельств осуществляются на регулярной основе как неотъемлемая часть процесса разработки и поддержки эксплуатации. Это семейство не предназначено предписывать какой-либо конкретный процесс разработки.

6.6.5.4 Инструментальные средства и методы (ALC_TAT)

Семейство «Инструментальные средства и методы» связано с необходимостью определения инструментальных средств разработки, используемых для анализа и создания ОО. В него включены требования, относящиеся к инструментальным средствам разработки и опциям этих инструментальных средств, зависящим от реализации.

6.6.6 Класс APE: Оценка профиля защиты

Цель оценки ПЗ — продемонстрировать, что ПЗ является полным, непротиворечивым, технически правильным и поэтому пригоден для изложения требований к одному или нескольким оцениваемым ОО. Такой ПЗ может быть приемлем для включения в реестр ПЗ.

6.6.7 Класс ASE: Оценка задания по безопасности

Цель оценки ЗБ — продемонстрировать, что ЗБ является полным, непротиворечивым, технически правильным и поэтому пригодно для использования в качестве основы при оценке соответствующего ОО.

6.6.8 Класс ATE: Тестирование

Класс доверия ATE устанавливает требования к тестированию, которое демонстрирует, что ФБО удовлетворяют функциональным требованиям безопасности ОО.

6.6.8.1 Покрытие (ATE_COV)

Семейство «Покрытие» устанавливает полноту функциональных тестов, выполненных разработчиком для ОО. Оно связано со степенью тестирования функций безопасности ОО.

6.6.8.2 Глубина (ATE_DPT)

Семейство «Глубина» устанавливает уровень детализации, на котором разработчик проверяет ОО. Тестирование функций безопасности основано на увеличивающейся глубине информации, получаемой из анализа представлений ФБО.

6.6.8.3 Функциональное тестирование (ATE_FUN)

Семейство «Функциональное тестирование» устанавливает, что ФБО действительно демонстрируют свойства, необходимые для удовлетворения требований соответствующего ЗБ. Функциональное тестирование обеспечивает доверие к тому, что ФБО удовлетворяют, по меньшей мере, требованиям выбранных функциональных компонентов. Однако функциональные тесты не устанавливают, что ФБО не выполняют больше функций, чем от них ожидается. Данное семейство сосредоточено на функциональном тестировании, проводимом разработчиком.

6.6.8.4 Независимое тестирование (ATE_IND)

Семейство «Независимое тестирование» определяет степень выполнения функционального тестирования ОО кем-либо, кроме разработчика (например, третьей стороной). Это семейство повышает ценность тестирования добавлением тестов, дополняющих тесты разработчика.

6.6.9 Класс AVA: Оценка уязвимостей

Класс доверия AVA «Оценка уязвимостей» определяет требования, направленные на идентификацию уязвимостей, которые могут быть активизированы. Особое внимание уделено уязвимостям, которые вносятся при проектировании, эксплуатации, неправильном применении или неверной конфигурации ОО.

6.6.9.1 Анализ скрытых каналов (AVA_CCA)

Семейство «Анализ скрытых каналов» направлено на выявление и анализ непредусмотренных коммуникационных каналов, которые могут применяться для нарушения предписанной ПБО.

6.6.9.2 Неправильное применение (AVA_MSU)

Семейство «Анализ неправильного применения» позволяет выяснить, способен ли администратор или пользователь, используя руководства, определить, что ОО конфигурирован или эксплуатируется небезопасным способом.

6.6.9.3 Стойкость функций безопасности ОО (AVA_SOF)

Анализ стойкости направлен на функции безопасности ОО, которые реализованы с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Даже если такие функции нельзя обойти, отключить или исказить, не исключено, что их все же можно преодолеть прямой атакой. Для каждой из указанных функций безопасности может быть заявлен уровень или специальная метрика стойкости. Анализ стойкости функций проводят для принятия решения, отвечают ли такие функции сделанным заявлениям. Например, анализ стойкости механизма пароля может, показав достаточность области задания пароля, продемонстрировать, что функция, использующая этот механизм, отвечает заявленной стойкости.

6.6.9.4 Анализ уязвимостей (AVA_VLA)

Анализ уязвимостей заключается в идентификации недостатков, которые могли быть внесены на различных этапах разработки. В результате определяются тесты проникновения, позволяющие получить всю совокупность необходимой информации относительно:

1) полноты ФБО (противостоят ли ФБО всем ожидаемым угрозам?);

2) зависимостей между всеми функциями безопасности.

Потенциальные уязвимости оценивают посредством тестирования проникновения, позволяющего сделать заключение, могут ли они в действительности быть использованы для нарушения безопасности ОО.

7 Критерии оценки профиля защиты и задания по безопасности

7.1 Краткий обзор

Настоящий раздел знакомит с критериями оценки для ПЗ и ЗБ, полностью представленными в разделах 8 и 9.

Эти критерии — первые требования, представленные в настоящем стандарте, потому что, как правило, оценку ПЗ и ЗБ проводят до оценки ОО. Данные критерии играют особую роль в оценке информации об ОО и оценке функциональных требований и требований доверия для выяснения, являются ли ПЗ и ЗБ содержательной основой для оценки ОО.

Хотя данные критерии оценки несколько отличаются от требований в разделах 12 — 18, они представлены аналогичным образом, потому что действия разработчика и оценщика при оценке сопоставимы для ПЗ, ЗБ и ОО.

Классы для ПЗ и ЗБ отличаются от классов для ОО тем, что при оценке ПЗ или ЗБ необходимо учесть все требования классов для ПЗ или ЗБ соответственно, в то время как далеко не все требования, представленные в классах для ОО, придется учитывать при оценке конкретного ОО.

Критерии оценки ПЗ и ЗБ основаны на информации, приведенной в ИСО/МЭК 15408-1, приложения А и В. В нижеследующих подразделах приведена полезная информация о требованиях классов APE и ASE.

7.2 Краткий обзор критериев профиля защиты

7.2.1 Оценка профиля защиты

Цель оценки ПЗ — показать, что он является полным, непротиворечивым, технически правильным и поэтому пригоден для изложения требований к одному или нескольким оцениваемым ОО. Такой ПЗ может быть приемлемым для включения в реестр ПЗ.

7.2.2 Соотношение с критериями оценки задания по безопасности

Как показано в ИСО/МЭК 15408-1, приложения А и В, имеется много совпадений в структуре и содержании ПЗ, ориентированного на определенный тип ОО, и ЗБ, разработанного для конкретного ОО. Поэтому многие критерии для оценки ПЗ содержат требования, которые подобны аналогичным для ЗБ и представлены таким же образом.

7.2.3 Задачи оценщика

7.2.3.1 Задачи оценщика по оценке профиля защиты, основанного только на требованиях ИСО/МЭК 15408

Оценщики, проводящие оценку ПЗ, который содержит требования только из ИСО/МЭК 15408, должны применять требования класса APE «Оценка профиля защиты», приведенные в таблице 2.

Таблица 2 — Семейства оценки профиля защиты, содержащего требования только из ИСО/МЭК 15408

Класс	Семейство	Краткое имя
APE: Оценка профиля защиты	Профиль защиты, описание ОО	APE_DES
	Профиль защиты, среда безопасности	APE_ENV
	Профиль защиты, введение ПЗ	APE_INT
	Профиль защиты, цели безопасности	APE_OBJ
	Профиль защиты, требования безопасности ИТ	APE_REQ

7.2.3.2 Задачи оценщика по оценке профиля защиты, содержащего расширенные по отношению к ИСО/МЭК 15408 требования

Оценщики, проводящие оценку ПЗ, который содержит требования не из ИСО/МЭК 15408, должны применять требования класса APE «Оценка профиля защиты», приведенные в таблице 3.

Таблица 3 — Семейства оценки профиля защиты, содержащего расширенные по отношению к ИСО/МЭК 15408 требования

Класс	Семейство	Краткое имя
APE: Оценка профиля защиты	Профиль защиты, описание ОО	APE_DES
	Профиль защиты, среда безопасности	APE_ENV
	Профиль защиты, введение ПЗ	APE_INT
	Профиль защиты, цели безопасности	APE_OBJ
	Профиль защиты, требования безопасности ИТ	APE_REQ
	Профиль защиты, требования безопасности ИТ, сформулированные в явном виде	APE_SRE

7.3 Краткий обзор критериев задания по безопасности

7.3.1 Оценка задания по безопасности

Цель оценки ЗБ — показать, что оно является полным, непротиворечивым, технически правильным и поэтому пригодно для использования в качестве основы при оценке соответствующего ОО.

7.3.2 Соотношение с другими критериями оценки из настоящего стандарта

При оценке ОО различают две стадии: оценка ЗБ и непосредственно оценка ОО, к которому относится данное ЗБ. Требования оценки ЗБ полностью представлены в разделе 9, а требования оценки ОО содержатся в разделах 12 — 18.

Оценка ЗБ включает в себя оценку утверждений о соответствии ПЗ. Если в ЗБ не утверждается соответствие ПЗ, то в разделе ЗБ «Утверждения о соответствии ПЗ» должно быть указано, что соответствие какому-либо ПЗ для ОО не утверждается.

7.3.3 Задачи оценщика

7.3.3.1 Задачи оценщика по оценке задания по безопасности, основанного только на требованиях ИСО/МЭК 15408

Оценщики, проводящие оценку ЗБ, которое содержит требования только из ИСО/МЭК 15408, должны применять требования класса ASE «Оценка задания по безопасности», приведенные в таблице 4.

Таблица 4 — Семейства оценки задания по безопасности, содержащего требования только из ИСО/МЭК 15408

Класс	Семейство	Краткое имя
ASE: Оценка задания по безопасности	Задание по безопасности, описание ОО	ASE_DES
	Задание по безопасности, среда безопасности	ASE_ENV
	Задание по безопасности, введение ЗБ	ASE_INT
	Задание по безопасности, цели безопасности	ASE_OBJ
	Задание по безопасности, утверждения о соответствии ПЗ	ASE_PPC
	Задание по безопасности, требования безопасности ИТ	ASE_REQ
	Задание по безопасности, краткая спецификация ОО	ASE_TSS

7.3.3.2 Задачи оценщика по оценке задания по безопасности, содержащего расширенные по отношению к ИСО/МЭК 15408 требования

Оценщики, проводящие оценку ЗБ, которое содержит требования не из ИСО/МЭК 15408, должны применять требования класса ASE «Оценка задания по безопасности», приведенные в таблице 5.

Таблица 5 — Семейства оценки задания по безопасности, содержащего расширенные по отношению к ИСО/МЭК 15408 требования

Класс	Семейство	Краткое имя
ASE: Оценка задания по безопасности	Задание по безопасности, описание ОО	ASE_DES
	Задание по безопасности, среда безопасности	ASE_ENV
	Задание по безопасности, введение ЗБ	ASE_INT
	Задание по безопасности, цели безопасности	ASE_OBJ
	Задание по безопасности, утверждения о соответствии ПЗ	ASE_PPC
	Задание по безопасности, требования безопасности ИТ	ASE_REQ
	Задание по безопасности, требования безопасности ИТ, сформулированные в явном виде	ASE_SRE
	Задание по безопасности, краткая спецификация ОО	ASE_TSS

8 Класс APE. Оценка профиля защиты

Цель оценки ПЗ состоит в демонстрации того, что ПЗ является полным, непротиворечивым и технически правильным. Оцененный ПЗ пригоден в качестве основы для разработки заданий по безопасности. Такой ПЗ является приемлемым для включения в реестр ПЗ.

Декомпозиция класса APE «Оценка профиля защиты» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 6.

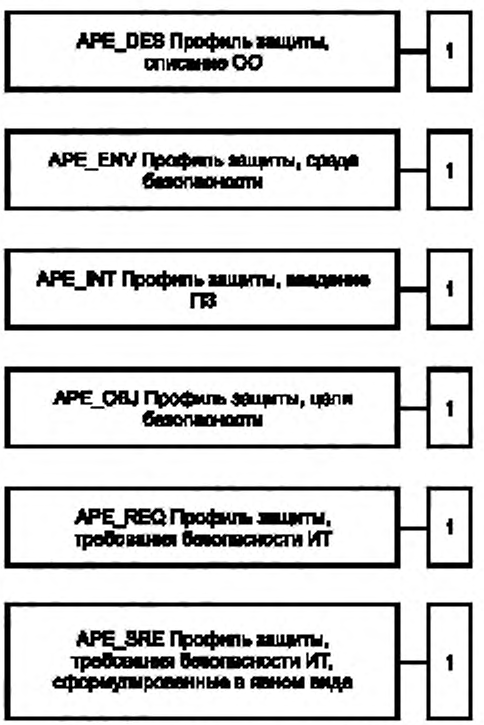


Рисунок 6 — Декомпозиция класса APE «Оценка профиля защиты»

8.1 Описание ОО (APE_DES)

8.1.1 Цели

Описание ОО способствует пониманию требований безопасности ОО. Оценка описания ОО требуется, чтобы показать, что оно является логически последовательным, внутренне непротиворечивым и согласованным со всеми другими частями ПЗ.

8.1.2 APE_DES.1 Профиль защиты, описание ОО, требования оценки

Зависимости: APE_ENV.1 Профиль защиты, среда безопасности, требования оценки
APE_INT.1 Профиль защиты, введение ПЗ, требования оценки
APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки
APE_REQ.1 Профиль защиты, требования безопасности ИТ, требования оценки

8.1.2.1 Элементы действий разработчика

8.1.2.1.1 APE_DES.1.1D

Разработчик ПЗ должен представить описание ОО как часть ПЗ.

8.1.2.2 Элементы содержания и представления свидетельств

8.1.2.2.1 APE_DES.1.1C

Описание ОО должно включать в себя тип продукта и общие свойства ИТ, присущие ОО.

8.1.2.3 Элементы действий оценщика

8.1.2.3.1 APE_DES.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.1.2.3.2 APE_DES.1.2E

Оценщик должен подтвердить, что описание ОО является логически последовательным и внутренне непротиворечивым.

8.1.2.3.3 APE_DES.1.3E

Оценщик должен подтвердить, что описание ОО согласуется с другими частями ПЗ.

8.2 Среда безопасности (APE_ENV)

8.2.1 Цели

Для принятия решения о достаточности требований безопасности ИТ в ПЗ важно, чтобы решаемая задача безопасности ясно понималась всеми участниками оценки.

8.2.2 APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

Зависимости: нет зависимостей.

8.2.2.1 Элементы действий разработчика

8.2.2.1.1 APE_ENV.1.1D

Разработчик ПЗ должен представить изложение среды безопасности ОО как часть ПЗ.

8.2.2.2 Элементы содержания и представления свидетельств

8.2.2.2.1 APE_ENV.1.1C

Изложение среды безопасности ОО должно идентифицировать и объяснить каждое предположение о предполагаемом применении ОО и среде использования ОО.

8.2.2.2.2 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.

8.2.2.2.3 APE_ENV.1.3C

Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.

8.2.2.3 Элементы действий оценщика

8.2.2.3.1 APE_ENV.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.2.2.3.2 APE_ENV.1.2E

Оценщик должен подтвердить, что описание среды безопасности ОО является логически последовательным и внутренне непротиворечивым.

8.3 Введение ПЗ (APE_INT)

8.3.1 Цели

Введение ПЗ содержит информацию для управления документооборотом и обзорную информацию о документе, необходимую для сопровождения реестра ПЗ. Оценка введения ПЗ требуется для демонстрации, что ПЗ правильно идентифицирован, и введение согласуется со всеми другими частями ЗБ.

8.3.2 APE_INT.1 Профиль защиты, введение ПЗ, требования оценки

Зависимости: APE_DES.1 Профиль защиты, описание ОО, требования оценки
APE_ENV.1 Профиль защиты, среда безопасности, требования оценки
APE_ODJ.1 Профиль защиты, цели безопасности, требования оценки
APE_REQ.1 Профиль защиты, требования безопасности ИТ, требования оценки

8.3.2.1 Элементы действий разработчика

8.3.2.1.1 APE_INT.1.1D

Разработчик ПЗ должен представить введение ПЗ как часть ПЗ.

8.3.2.2 Элементы содержания и представления свидетельств

8.3.2.2.1 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.

8.3.2.2.2 APE_INT.1.2C

Введение ПЗ должно содержать аннотацию ПЗ с общей характеристикой ПЗ в описательной форме.

8.3.2.3 Элементы действий оценщика

8.3.2.3.1 APE_INT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.3.2.3.2 APE_INT.1.2E

Оценщик должен подтвердить, что введение ПЗ является логически последовательным и внутренне непротиворечивым.

8.3.2.3.3 APE_INT.1.3E

Оценщик должен подтвердить, что введение ПЗ согласуется с другими частями ПЗ.

8.4 Цели безопасности (APE_OBJ)

8.4.1 Цели

Цели безопасности — краткое изложение предполагаемой реакции на проблему безопасности. Оценка целей безопасности требуется для демонстрации того, что установленные цели адекватны проблеме безопасности. Существуют цели безопасности для ОО и цели безопасности для среды. Необходимо сопоставить цели безопасности для ОО и среды с идентифицированными угрозами, которым они противостоят, и/или с политикой и предположениями, которым они соответствуют.

8.4.2 APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки

Зависимости: APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

8.4.2.1 Элементы действий разработчика

8.4.2.1.1 APE_OBJ.1.1D

Разработчик ПЗ должен представить изложение целей безопасности как часть ПЗ.

8.4.2.1.2 APE_OBJ.1.2D

Разработчик ПЗ должен представить обоснование целей безопасности.

8.4.2.2 Элементы содержания и представления свидетельств

8.4.2.2.1 APE_OBJ.1.1C

Изложение целей безопасности должно определить цели безопасности для ОО и его среды.

8.4.2.2.2 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.

8.4.2.2.3 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.

8.4.2.2.4 APE_OBJ.1.4C

Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.

8.4.2.2.5 APE_OBJ.1.5C

Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.

8.4.2.3 Элементы действий оценщика

8.4.2.3.1 APE_OBJ.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.4.2.3.2 APE_OBJ.1.2E

Оценщик должен подтвердить, что описание целей безопасности является полным, логически последовательным и внутренне непротиворечивым.

8.5 Требования безопасности ИТ (APE_REQ)

8.5.1 Цели

Требования безопасности ИТ, выбранные для ОО и представленные или указанные в ПЗ, необходимо оценить для подтверждения их внутренней непротиворечивости и пригодности для разработки ОО, соответствующего целям его безопасности.

Не все цели безопасности, выраженные в ПЗ, могут быть выполнены соответствующим ОО, так как некоторые ОО могут зависеть от требований безопасности ИТ, выполняемых средой ИТ. В этом случае требования безопасности ИТ, относящиеся к среде, необходимо ясно изложить и оценить в контексте требований к ОО.

Это семейство представляет требования оценки, которые позволяют оценщику принять решение о том, что ПЗ пригоден для использования в качестве изложения требований к оцениваемому ОО. Дополнительные критерии, необходимые для оценки требований, сформулированных в явном виде, приведены в семействе APE_SRE «Требования безопасности ИТ, сформулированные в явном виде».

8.5.2 Замечания по применению

Термин «требования безопасности ИТ» подразумевает «требования безопасности ОО» с возможным включением «требований безопасности для среды ИТ».

Термин «требования безопасности ОО» подразумевает «функциональные требования безопасности ОО» и/или «требования доверия к безопасности ОО».

В компоненте APE_REQ.1 «Профиль защиты, требования безопасности ИТ, требования оценки» использованы несколько близких по значению прилагательных («соответствующий», «необходимый», «приемлемый», «целесообразный») для указания на то, что данные элементы допускают выбор в конкретных случаях. То, какой выбор является приемлемым, зависит от контекста ПЗ. Подробная информация по этим аспектам содержится в ИСО/МЭК 15408-1, приложение А.

ИСО/МЭК 15408 предусматривает возможность выделения нескольких доменов СФБ в рамках конкретного ОО. Домен СФБ является подмножеством ОО (логическим или физическим), для которого необходим определенный уровень стойкости функции безопасности в контексте предопределенной среды. Это позволяет ОО для некоторых функциональных возможностей иметь более высокое требование к «минимальной стойкости функции», чем для других функциональных возможностей. Для ОО с несколькими доменами СФБ словосочетание «минимальная стойкость функции» используется для указания набора, содержащего определение минимальной стойкости функции для каждого домена. Кроме того, в обосновании требований должен быть рассмотрен уровень СФБ для каждого домена в свете того, какое влияние данный домен оказывает на удовлетворение целей безопасности.

8.5.3 APE_REQ.1 Профиль защиты, требования безопасности ИТ, требования оценки

Зависимости: APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки

8.5.3.1 Элементы действий разработчика

8.5.3.1.1 APE_REQ.1.1D

Разработчик ПЗ должен представить изложение требований безопасности ИТ как часть ПЗ.

8.5.3.1.2 APE_REQ.1.2D

Разработчик ПЗ должен представить обоснование требований безопасности.

8.5.3.2 Элементы содержания и представления свидетельств

8.5.3.2.1 APE_REQ.1.1C

Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований ИСО/МЭК 15408-2.

8.5.3.2.2 APE_REQ.1.2C

Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия настоящего стандарта.

8.5.3.2.3 APE_REQ.1.3C

В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в настоящем стандарте.

8.5.3.2.4 APE_REQ.1.4C

Свидетельство должно содержать логическое обоснование, что изложение требований доверия к ОО является соответствующим.

8.5.3.2.5 APE_REQ.1.5C

ПЗ должен, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.

8.5.3.2.6 APE_REQ.1.6C

Все завершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.

8.5.3.2.7 APE_REQ.1.7C

Любые незавершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.

8.5.3.2.8 APE_REQ.1.8C

Зависимости между требованиями безопасности ИТ, включенными в ПЗ, следует удовлетворить.

8.5.3.2.9 APE_REQ.1.9C

Свидетельство должно содержать логическое обоснование каждого неудовлетворения зависимостей.

8.5.3.2.10 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.

8.5.3.2.11 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.

8.5.3.2.12 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.

8.5.3.2.13 APE_REQ.1.13C

Обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.

8.5.3.2.14 APE_REQ.1.14C

Обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.

8.5.3.3 Элементы действий оценщика

8.5.3.3.1 APE_REQ.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.5.3.3.2 APE_REQ.1.2E

Оценщик должен подтвердить, что описание требований безопасности ИТ является полным, логически последовательным и внутренне непротиворечивым.

8.6 Требования безопасности ИТ, сформулированные в явном виде (APE_SRE)

8.6.1 Цели

Если после тщательного рассмотрения окажется, что ни один из компонентов требований ИСО/МЭК 15408-2 или настоящего стандарта не применим непосредственно ко всем или к части требований безопасности ИТ, разработчик ПЗ может сформулировать другие требования, которые не имеют ссылки на ИСО/МЭК 15408. Использование таких требований должно быть логически обосновано.

Данное семейство содержит требования оценки, позволяющие оценщику сделать заключение, что сформулированные в явном виде требования четко и однозначно выражены. Оценка требований по ИСО/МЭК 15408, используемых наряду со сформулированными в явном виде требованиями безопасности, определяется семейством APE_REQ «Требования безопасности ИТ».

Сформулированные в явном виде требования безопасности ИТ для ОО, представленные или указанные в ПЗ, требуется оценить для демонстрации четкости и однозначности их выражения.

8.6.2 Замечания по применению

Формулировка в явном виде требований по структуре, сопоставимой со структурой существующих компонентов и элементов по ИСО/МЭК 15408, включает в себя выбор подобной маркировки, способа выражения и уровня детализации.

Использование требований ИСО/МЭК 15408 в качестве образца означает, что требования могут быть четко идентифицированы, что они автономны, что применение каждого требования возможно, и даст значимый результат оценки, основанный на анализе соответствия ОО конкретному требованию.

Термин «требования безопасности ИТ» подразумевает «требования безопасности ОО» с возможным включением «требований безопасности для среды ИТ».

Термин «требования безопасности ОО» подразумевает «функциональные требования безопасности ОО» и/или «требования доверия к безопасности ОО».

Элементы APE_SRE.1.5C и APE_SRE.1.6C требуют, чтобы сформулированные в явном виде требования безопасности ИТ были измеримыми и объективными, а также четко и однозначно выраженными. Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны использоваться как образец.

8.6.3 APE_SRE.1 Профиль защиты, требования безопасности ИТ, сформулированные в явном виде, требования оценки

Зависимости: APE_REQ.1 Профиль защиты, требования безопасности ИТ, требования оценки

8.6.3.1 Элементы действий разработчика

8.6.3.1.1 APE_SRE.1.1D

Разработчик ПЗ должен представить изложение требований безопасности ИТ как часть ПЗ.

8.6.3.1.2 APE_SRE.1.2D

Разработчик ПЗ должен представить обоснование требований безопасности.

8.6.3.2 Элементы содержания и представления свидетельств

8.6.3.2.1 APE_SRE.1.1C

Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.

8.6.3.2.2 APE_SRE.1.2C

Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.

8.6.3.2.3 APE_SRE.1.3C

Свидетельство должно содержать логическое обоснование, почему требования безопасности должны быть сформулированы в явном виде.

8.6.3.2.4 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.

8.6.3.2.5 APE_SRE.1.5C

Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать такие объективные требования оценки, чтобы соответствие или несоответствие им ОО могло быть определено и последовательно продемонстрировано.

8.6.3.2.6 APE_SRE.1.6C

Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.

8.6.3.2.7 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.

8.6.3.3 Элементы действий оценщика

8.6.3.3.1 APE_SRE.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

8.6.3.3.2 APE_SRE.1.2E

Оценщик должен определить, что все зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.

9 Класс ASE. Оценка задания по безопасности

Цель оценки ЗБ состоит в демонстрации того, что ЗБ является полным, непротиворечивым, технически правильным и поэтому пригодно в качестве основы для оценки соответствующего ОО.

Декомпозиция класса ASE «Оценка задания по безопасности» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 7.

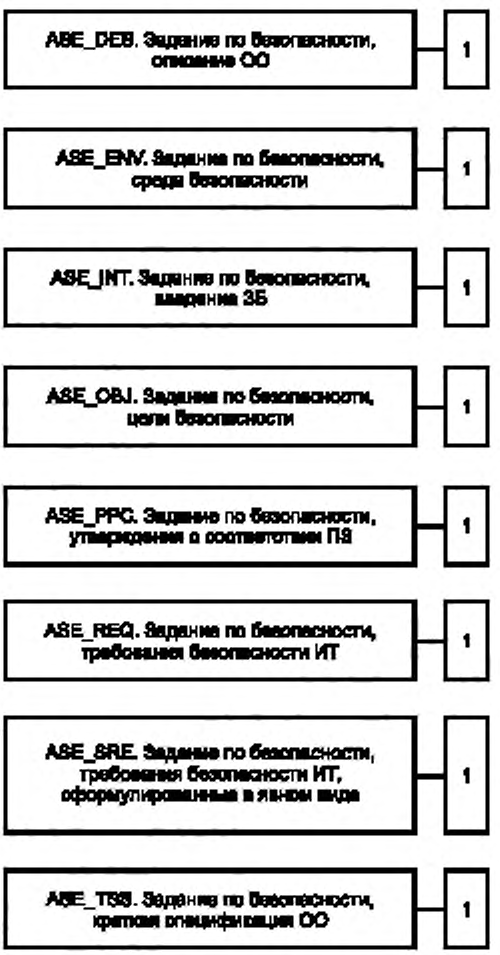


Рисунок 7 — Декомпозиция класса ASE «Оценка задания по безопасности»

9.1 Описание ОО (ASE_DES)

9.1.1 Цели

Описание ОО способствует пониманию требований безопасности ОО. Оценка описания ОО требуется, чтобы показать, что оно является логически последовательным, внутренне непротиворечивым и согласованным со всеми другими частями ЗБ.

9.1.2 ASE_DES.1 Задание по безопасности, описание ОО, требования оценки

Зависимости: ASE_ENV.1 Задание по безопасности, среда безопасности, требования оценки
ASE_INT.1 Задание по безопасности, введение ЗБ, требования оценки
ASE_OBJ.1 Задание по безопасности, цели безопасности, требования оценки
ASE_PPC.1 Задание по безопасности, утверждения о соответствии ПЗ, требования оценки
ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки
ASE_TSS.1 Задание по безопасности, краткая спецификация ОО, требования оценки

9.1.2.1 Элементы действий разработчика

9.1.2.1.1 ASE_DES.1.1D

Разработчик должен представить описание ОО как часть ЗБ.

9.1.2.2 Элементы содержания и представления свидетельств

9.1.2.2.1 ASE_DES.1.1C

Описание ОО должно включать в себя тип продукта или системы, область применения ОО, а также физические и логические границы ОО.

9.1.2.3 Элементы действий оценщика

9.1.2.3.1 ASE_DES.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.1.2.3.2 ASE_DES.1.2E

Оценщик должен подтвердить, что описание ОО является логически последовательным и внутренне непротиворечивым.

9.1.2.3.3 ASE_DES.1.3E

Оценщик должен подтвердить, что описание ОО согласуется с другими частями ЗБ.

9.2 Среда безопасности (ASE_ENV)

9.2.1 Цели

Для принятия решения о достаточности требований безопасности ИТ в ЗБ важно, чтобы решаемая задача безопасности ясно понималась всеми участниками оценки.

9.2.2 ASE_ENV.1 Задание по безопасности, среда безопасности, требования оценки

Зависимости: нет зависимостей.

9.2.2.1 Элементы действий разработчика

9.2.2.1.1 ASE_ENV.1.1D

Разработчик должен представить изложение среды безопасности ОО как часть ЗБ.

9.2.2.2 Элементы содержания и представления свидетельств

9.2.2.2.1 ASE_ENV.1.1C

Изложение среды безопасности ОО должно идентифицировать и объяснить каждое предположение о предполагаемом применении ОО и среде использования ОО.

9.2.2.2.2 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.

9.2.2.2.3 ASE_ENV.1.3C

Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.

9.2.2.3 Элементы действий оценщика

9.2.2.3.1 ASE_ENV.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.2.2.3.2 ASE_ENV.1.2E

Оценщик должен подтвердить, что описание среды безопасности ОО является логически последовательным и внутренне непротиворечивым.

9.3 Введение ЗБ (ASE_INT)

9.3.1 Цели

Введение ЗБ содержит материалы по идентификации и индексации материалов. Оценка введения ЗБ требуется для демонстрации, что ЗБ правильно идентифицировано, и введение согласуется со всеми другими частями ЗБ.

9.3.2 ASE_INT.1 Задание по безопасности, введение ЗБ, требования оценки

Зависимости: ASE_DES.1 Задание по безопасности, описание ОО, требования оценки
ASE_ENV.1 Задание по безопасности, среда безопасности, требования оценки
ASE_OBJ.1 Задание по безопасности, цели безопасности, требования оценки
ASE_PPC.1 Задание по безопасности, утверждения о соответствии ПЗ, требования оценки
ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки
ASE_TSS.1 Задание по безопасности, краткая спецификация ОО, требования оценки

9.3.2.1 Элементы действий разработчика

9.3.2.1.1 ASE_INT.1.1D

Разработчик должен представить введение ЗБ как часть ЗБ.

9.3.2.2 Элементы содержания и представления свидетельств

9.3.2.2.1 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.

9.3.2.2.2 ASE_INT.1.2C

Введение ЗБ должно содержать аннотацию ЗБ с общей характеристикой ЗБ в описательной форме.

9.3.2.2.3 ASE_INT.1.3C

Введение ЗБ должно содержать утверждение о соответствии ИСО/МЭК 15408, излагающее все оцениваемые утверждения о соответствии ОО ИСО/МЭК 15408.

9.3.2.3 Элементы действия оценщика

9.3.2.3.1 ASE_INT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.3.2.3.2 ASE_INT.1.2E

Оценщик должен подтвердить, что введение ЗБ является логически последовательным и внутренне непротиворечивым.

9.3.2.3.3 ASE_INT.1.3E

Оценщик должен подтвердить, что введение ЗБ согласуется с другими частями ЗБ.

9.4 Цели безопасности (ASE_OBJ)

9.4.1 Цели

Цели безопасности — краткое изложение предполагаемой реакции на проблему безопасности. Оценка целей безопасности требуется для демонстрации того, что установленные цели адекватны проблеме безопасности. Существуют цели безопасности для ОО и цели безопасности для среды. Необходимо сопоставить цели безопасности для ОО и среды с идентифицированными угрозами, которым они противостоят, и/или с политикой и предположениями, которым они соответствуют.

9.4.2 ASE_OBJ.1 Задание по безопасности, цели безопасности, требования оценки

Зависимости: ASE_ENV.1 Задание по безопасности, среда безопасности, требования оценки

9.4.2.1 Элементы действий разработчика

9.4.2.1.1 ASE_OBJ.1.1D

Разработчик должен представить изложение целей безопасности как часть ЗБ.

9.4.2.1.2 ASE_OBJ.1.2D

Разработчик должен представить обоснование целей безопасности.

9.4.2.2 Элементы содержания и представления свидетельств

9.4.2.2.1 ASE_OBJ.1.1C

Изложение целей безопасности должно определить цели безопасности для ОО и его среды.

9.4.2.2.2 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.

9.4.2.2.3 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.

9.4.2.2.4 ASE_OBJ.1.4C

Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.

9.4.2.2.5 ASE_OBJ.1.5C

Обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.

9.4.2.3 Элементы действий оценщика

9.4.2.3.1 ASE_OBJ.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.4.2.3.2 ASE_OBJ.1.2E

Оценщик должен подтвердить, что описание целей безопасности является полным, логически последовательным и внутренне непротиворечивым.

9.5 Утверждения о соответствии ПЗ (ASE_PPC)

9.5.1 Цели

Цель оценки утверждений о соответствии ПЗ состоит в том, чтобы решить, является ли ЗБ корректным отображением ПЗ.

9.5.2 Замечания по применению

Семейство применяют только при наличии утверждений о соответствии ПЗ. В противном случае не требуется никаких действий разработчика и оценщика.

Хотя при наличии утверждений о соответствии ПЗ необходимы дополнительные действия по оценке, затраты на оценку ЗБ обычно меньше, чем в случае если ПЗ не применяется, потому что при оценке ЗБ можно использовать результаты оценки данного ПЗ.

9.5.3 ASE_PPC.1 Задание по безопасности, утверждения о соответствии ПЗ, требования оценки

Зависимости: ASE_OBJ.1 Задание по безопасности, цели безопасности, требования оценки
ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки

9.5.3.1 Элементы действий разработчика

9.5.3.1.1 ASE_PPC.1.1D

Разработчик должен представить каждое утверждение о соответствии ПЗ как часть ЗБ.

9.5.3.1.2 ASE_PPC.1.2D

Разработчик должен представить обоснование утверждений о соответствии ПЗ для каждого представленного утверждения о соответствии ПЗ.

9.5.3.2 Элементы содержания и представления свидетельств

9.5.3.2.1 ASE_PPC.1.1C

Каждое утверждение о соответствии ПЗ должно идентифицировать ПЗ, соответствие которому утверждается, включая необходимые уточнения, связанные с этим утверждением.

9.5.3.2.2 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.

9.5.3.2.3 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.

9.5.3.3 Элементы действий оценщика

9.5.3.3.1 ASE_PPC.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.5.3.3.2 ASE_PPC.1.2E

Оценщик должен подтвердить, что утверждения о соответствии профилям защиты являются корректным отображением соответствующих ПЗ.

9.6 Требования безопасности ИТ (ASE_REQ)

9.6.1 Цели

Требования безопасности ИТ, выбранные для ОО и представленные или указанные в ЗБ, необходимо оценить для подтверждения их внутренней непротиворечивости и пригодности для разработки ОО, соответствующего целям его безопасности.

Данное семейство представляет требования оценки, позволяющие оценщику принять решение о том, что ЗБ пригодно для использования в качестве изложения требований к соответствующему ОО. Дополнительные критерии, необходимые для оценки требований, сформулированных в явном виде, приведены в семействе ASE_SRE «Требования безопасности ИТ, сформулированные в явном виде».

9.6.2 Замечания по применению

Термин «требования безопасности ИТ» подразумевает «требования безопасности ОО» с возможным включением «требований безопасности для среды ИТ».

Термин «требования безопасности ОО» подразумевает «функциональные требования безопасности ОО» и/или «требования доверия к безопасности ОО».

В компоненте ASE_REQ.1 «Задание по безопасности, требования безопасности ИТ, сформулированные в явном виде, требования оценки» использованы несколько значений, близких по значению прилагательных («соответствующий», «необходимый», «приемлемый», «целесообразный») для указания на то, что данные элементы допускают выбор в определенных случаях. То, какой выбор является приемлемым, зависит от контекста ЗБ. Подробная информация по этим аспектам содержится в ИСО/МЭК 15408-1, приложение В.

ИСО/МЭК 15408 предусматривает возможность выделения нескольких доменов СФБ в рамках конкретного ОО. Домен СФБ является подмножеством ОО (логическим или физическим), для которого является необходимым определенный уровень стойкости функции безопасности в контексте предопределенной среды. Это позволяет ОО для некоторых функциональных возможностей иметь более высокое требование к «минимальной стойкости функции», чем для других функциональных возможностей. Для ОО с несколькими доменами СФБ словосочетание «минимальная стойкость функции» используется для указания набора, содержащего определение минимальной стойкости функции для каждого домена. Кроме того, в обосновании требований должен быть рассмотрен уровень СФБ для каждого домена в свете того, какое влияние данный домен оказывает на удовлетворение целей безопасности.

9.6.3 ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки

Зависимости: ASE_OBJ. 1 Задание по безопасности, цели безопасности, требования оценки

9.6.3.1 Элементы действий разработчика

9.6.3.1.1 ASE_REQ.1.1D

Разработчик должен представить изложение требований безопасности ИТ как часть ЗБ.

9.6.3.1.2 ASE_REQ.1.2D

Разработчик должен представить обоснование требований безопасности.

9.6.3.2 Элементы содержания и представления свидетельств

9.6.3.2.1 ASE_REQ.1.1C

Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований ИСО/МЭК 15408-2.

9.6.3.2.2 ASE_REQ.1.2C

Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия настоящего стандарта.

9.6.3.2.3 ASE_REQ.1.3C

В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в настоящем стандарте.

9.6.3.2.4 ASE_REQ.1.4C

Свидетельство должно содержать логическое обоснование, что изложение требований доверия к ОО является соответствующим.

9.6.3.2.5 ASE_REQ.1.5C

ЗБ должно, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.

9.6.3.2.6 ASE_REQ.1.6C

Операции, предусмотренные в требованиях безопасности ИТ, включенных в ЗБ, должны быть идентифицированы и выполнены.

9.6.3.2.7 ASE_REQ.1.7C

Зависимости между требованиями безопасности ИТ, включенными в ЗБ, следует удовлетворить.

9.6.3.2.8 ASE_REQ.1.8C

Свидетельство должно содержать логическое обоснование каждого неудовлетворения зависимостей.

9.6.3.2.9 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.

9.6.3.2.10 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.

9.6.3.2.11 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.

9.6.3.2.12 ASE_REQ.1.12C

Обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.

9.6.3.2.13 ASE_REQ.1.13C

Обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.

9.6.3.3 Элементы действий оценщика

9.6.3.3.1 ASE_REQ.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.6.3.3.2 ASE_REQ.1.2E

Оценщик должен подтвердить, что описание требований безопасности ИТ является полным, логически последовательным и внутренне непротиворечивым.

9.7 Требования безопасности ИТ, сформулированные в явном виде (ASE_SRE)

9.7.1 Цели

Если после тщательного рассмотрения окажется, что ни один из компонентов требований ИСО/МЭК 15408-2 или настоящего стандарта не применим непосредственно ко всем или к части требований безопасности ИТ, разработчик ЗБ может сформулировать другие требования, которые не имеют ссылки на ИСО/МЭК 15408. Использование таких требований должно быть логически обосновано.

Данное семейство содержит требования оценки, позволяющие оценщику сделать заключение, что сформулированные в явном виде требования четко и однозначно выражены. Оценка требований по ИСО/МЭК 15408, используемых наряду со сформулированными в явном виде требованиями безопасности, определяется семейством ASE_REQ «Требования безопасности ИТ».

Сформулированные в явном виде требования безопасности ИТ для ОО, представленные или указанные в ЗБ, требуется оценить для демонстрации четкости и однозначности их выражения.

9.7.2 Замечания по применению

Формулировка в явном виде требований по структуре, сопоставимой со структурой существующих компонентов и элементов по ИСО/МЭК 15408, включает в себя выбор подобной маркировки, способа выражения и уровня детализации.

Использование требований ИСО/МЭК 15408 в качестве образца означает, что требования могут быть четко идентифицированы, что они автономны, и что применение каждого требования возможно и даст значимый результат оценки, основанный на изложении соответствия ОО этому конкретному требованию.

Термин «требования безопасности ИТ» подразумевает «требования безопасности ОО» с возможным включением «требований безопасности для среды ИТ».

Термин «требования безопасности ОО» подразумевает «функциональные требования безопасности ОО» и/или «требования доверия к безопасности ОО».

Элементы APE_SRE.1.5C и APE_SRE.1.6C требуют, чтобы сформулированные в явном виде требования безопасности ИТ должны быть измеримыми, объективными, а также четко и однозначно выраженными. Имеющиеся в ИСО/МЭК 15408 функциональные требования и требования доверия должны использоваться как образец.

9.7.3 ASE_SRE.1 Задание по безопасности, требования безопасности ИТ, сформулированные в явном виде, требования оценки

Зависимости: ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки

9.7.3.1 Элементы действий разработчика

9.7.3.1.1 ASE_SRE.1.1D

Разработчик должен представить изложение требований безопасности ИТ как часть ЗБ.

9.7.3.1.2 ASE_SRE.1.2D

Разработчик должен представить обоснование требований безопасности.

9.7.3.2 Элементы содержания и представления свидетельств

9.7.3.2.1 ASE_SRE.1.1C

Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.

9.7.3.2.2 ASE_SRE.1.2C

Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ИСО/МЭК 15408, должны быть идентифицированы.

9.7.3.2.3 ASE_SRE.1.3C

Свидетельство должно содержать логическое обоснование, почему требования безопасности должны быть сформулированы в явном виде.

9.7.3.2.4 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.

9.7.3.2.5 ASE_SRE.1.5C

Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать такие объективные требования оценки, чтобы соответствие или несоответствие им ОО могло быть определено и последовательно продемонстрировано.

9.7.3.2.6 ASE_SRE.1.6C

Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.

9.7.3.2.7 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.

9.7.3.3 Элементы действий оценщика

9.7.3.3.1 ASE_SRE.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.7.3.3.2 ASE_SRE.1.2E

Оценщик должен определить, что все зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.

9.8 Краткая спецификация ОО (ASE_TSS)

9.8.1 Цели

Краткая спецификация ОО предоставляет определение в самом общем виде функций безопасности, заявленных для удовлетворения функциональных требований, и мер доверия, выбранных для удовлетворения требований доверия.

9.8.2 Замечания по применению

Отношение между функциями безопасности ИТ и функциональными требованиями безопасности ОО может быть отношением типа «многие ко многим». Тем не менее каждая функция безопасности должна способствовать удовлетворению, по меньшей мере, одного требования безопасности, чтобы можно было четко определить ФБО. Функции безопасности, не соответствующие этому требованию, обычно необязательны. Следует отметить, что требование о том, чтобы функция безопасности способствовала удовлетворению, по меньшей мере, одного требования безопасности, сформулировано в достаточно общем виде с тем, чтобы для всех функций безопасности, которые полезны для ОО, существовала бы возможность обоснования.

Изложение мер доверия уместно во всех случаях, когда в ЗБ включены требования доверия, не входящие в настоящий стандарт. Если требования доверия к ОО в ЗБ основаны исключительно на оценочных уровнях доверия или других компонентах доверия из настоящего стандарта, то меры доверия могут быть представлены в форме ссылки на документы, которые указывают на удовлетворение требований доверия.

В компоненте ASE_TSS.1 «Задание по безопасности, краткая спецификация ОО, требования оценки» использованы несколько значений близких по значению прилагательных («соответствующий», «необходимый») для указания, что данные элементы допускают выбор в определенных случаях. Какой выбор является приемлемым, зависит от контекста ЗБ. Подробная информация по этим аспектам содержится в ИСО/МЭК 15408-1, приложение В.

9.8.3 ASE_TSS.1 Задание по безопасности, краткая спецификация ОО, требования оценки

Зависимости: ASE_REQ.1 Задание по безопасности, требования безопасности ИТ, требования оценки

9.8.3.1 Элементы действий разработчика

9.8.3.1.1 ASE_TSS.1.1D

Разработчик должен представить краткую спецификацию ОО как часть ЗБ.

9.8.3.1.2 ASE_TSS.1.2D

Разработчик должен представить обоснование краткой спецификации ОО.

9.8.3.2 Элементы содержания и представления свидетельств

9.8.3.2.1 ASE_TSS.1.1C

Краткая спецификация ОО должна содержать описание функций безопасности ИТ и мер доверия к ОО.

9.8.3.2.2 ASE_TSS.1.2C

Краткая спецификация ОО должна сопоставить функции безопасности ИТ и функциональные требования безопасности ОО так, 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.

9.8.3.2.3 ASE_TSS.1.3C

Функции безопасности ИТ должны быть определены в неформальном стиле на уровне детализации, необходимом для понимания их назначения.

9.8.3.2.4 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.

9.8.3.2.5 ASE_TSS.1.5C

Обоснование краткой спецификации ОО должно демонстрировать, что функции безопасности ИТ пригодны для удовлетворения функциональных требований безопасности ОО.

9.8.3.2.6 ASE_TSS.1.6C

Обоснование краткой спецификации ОО должно демонстрировать, что сочетание специфицированных функций безопасности ИТ в совокупности способно удовлетворить функциональные требования безопасности ОО.

9.8.3.2.7 ASE_TSS.1.7C

Краткая спецификация ОО должна сопоставить меры и требования доверия так, чтобы можно было отметить, какие меры способствуют удовлетворению каких требований.

9.8.3.2.8 ASE_TSS.1.8C

Обоснование краткой спецификации ОО должно демонстрировать, что меры доверия удовлетворяют всем требованиям доверия к ОО.

9.8.3.2.9 ASE_TSS.1.9C

Краткая спецификация ОО должна идентифицировать все функции безопасности ИТ, которые реализованы вероятностным или перестановочным механизмом соответственно.

9.8.3.2.10 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.

9.8.3.3 Элементы действий оценщика

9.8.3.3.1 ASE_TSS.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

9.8.3.3.2 ASE_TSS.1.2E

Оценщик должен подтвердить, что краткая спецификация ОО является полной, логически последовательной и внутренне непротиворечивой.

10 Оценочные уровни доверия

Оценочные уровни доверия (ОУД) образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия.

Важно обратить внимание, что не все семейства и компоненты настоящего стандарта включены в оценочные уровни доверия. Это не означает, что они не обеспечивают значимое и полезное доверие. Напротив, ожидается, что эти семейства и их компоненты будут рассматриваться для усиления ОУД в тех ПЗ и ЗБ, где они полезны.

10.1 Краткий обзор оценочных уровней доверия

Сводка оценочных уровней доверия представлена в таблице 6. Столбцы таблицы представляют собой иерархически упорядоченный набор ОУД, а строки — семейства доверия. Каждый номер в образованной ими матрице идентифицирует конкретный компонент доверия, применяемый в соответствующем ОУД.

Как показано в следующем подразделе, в настоящем стандарте определены семь иерархически упорядоченных оценочных уровней доверия для ранжирования доверия к ОО. Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается заменой компонента доверия иерархичным компонентом из того же семейства доверия (то есть увеличением строгости, области и/или глубины оценки) и добавлением компонентов из других семейств доверия (то есть добавлением новых требований). В таблице 6 это показано с использованием полужирного шрифта.

ОУД состоят из определенной комбинации компонентов доверия в соответствии с разделом 6. Точнее, каждый ОУД включает в себя не более одного компонента каждого семейства доверия, а все зависимости каждого компонента доверия учтены.

Хотя в настоящем стандарте определены именно ОУД, можно применять другие комбинации компонентов доверия. Специально введенное понятие «усиление» («augmentation») допускает добавление (из семейств доверия, до этого не включенных в ОУД) или замену компонентов доверия в ОУД (другими, иерархичными компонентами из того же самого семейства доверия). Из конструкций установления доверия, определенных в ИСО/МЭК 15408, только ОУД могут быть усилены. Понятие «ОУД за исключением какого-либо составляющего его компонента доверия» не признано в ИСО/МЭК 15408 как допустимое утверждение. При использовании усиления необходимо логически обосновать полезность и дополнительную ценность добавленного к ОУД компонента доверия. ОУД может быть также расширен требованиями доверия, сформулированными в явном виде.

Таблица 6 — Сводка оценочных уровней доверия

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Управление конфигурацией	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Поставка и эксплуатация	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Разработка	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Руководства	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Тестирование	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Оценка уязвимостей	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

10.2 Детализация оценочных уровней доверия

Следующие подразделы содержат определения ОУД с использованием полужирного шрифта для выделения и описания новых требований.

10.3 Оценочный уровень доверия 1 (ОУД1), предусматривающий функциональное тестирование

10.3.1 Цели

ОУД1 применяют, если требуется некоторая уверенность в правильном функционировании, а угрозы безопасности не рассматривают как серьезные. Он будет полезен в случае, если требуется независимо полученное доверие утверждению, что было уделено должное внимание защите персональных данных или подобной информации.

ОУД1 обеспечивает оценку ОО в том виде, в каком он доступен потребителю, путем независимого тестирования на соответствие спецификации и экспертизы представленной документации. Предполагается, что оценка может успешно проводиться без помощи разработчика ОО и с минимальными затратами.

При оценке на этом уровне следует предоставить свидетельство, что ОО функционирует в соответствии с документацией и предоставляет приемлемую защиту против идентифицированных угроз.

10.3.2 Компоненты доверия

ОУД1 (см. таблицу 7) предоставляет базовый уровень доверия посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов и руководств.

Анализ поддержан независимым тестированием ФБО.

ОУД1 обеспечивает значимое увеличение доверия по сравнению с неоцененным продуктом или системой ИТ.

Таблица 7 — ОУД1

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_CAP.1 Номера версий
ADO: Поставка и эксплуатация	ADO_IGS.1 Процедуры установки, генерации и запуска
ADV: Разработка	ADV_FSP.1 Неформальная функциональная спецификация
	ADV_RCR.1 Неформальная демонстрация соответствия
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ATE: Тестирование	ATE_IND.1 Независимое тестирование на соответствие

10.4 Оценочный уровень доверия 2 (ОУД2), предусматривающий структурное тестирование

10.4.1 Цели

ОУД2 содержит требование сотрудничества с разработчиком для получения информации о проекте и результатах тестирования, но при этом не следует требовать от разработчика усилий, превышающих обычную коммерческую практику. Следовательно, не требуется существенного увеличения стоимости или затрат времени.

Поэтому ОУД2 применяют в случаях, если разработчикам или пользователям требуется независимо подтверждаемый уровень доверия от невысокого до умеренного при отсутствии доступа к полной документации по разработке. Такая ситуация может возникать при обеспечении безопасности разработанных ранее (наследуемых) систем или при ограниченной доступности разработчика.

10.4.2 Компоненты доверия

ОУД2 (см. таблицу 8) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов, руководств **и проекта ОО верхнего уровня.**

Анализ поддержан независимым тестированием ФБО, **свидетельством разработчика об испытаниях, основанных на функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска разработчиком явных уязвимостей (например, из общедоступных источников).**

ОУД2 также обеспечивает доверие посредством списка конфигурации ОО и свидетельства безопасных процедур поставки.

ОУД2 представляет значимое увеличение доверия по сравнению с ОУД1, требуя тестирования и анализа уязвимостей разработчиком, а также независимого тестирования, основанного на более детализированных спецификациях ОО.

Таблица 8 — ОУД2

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_CAP.2 Элементы конфигурации
ADO: Поставка и эксплуатация	ADO_DEL.1 Процедуры поставки
	ADO_IGS.1 Процедуры установки, генерации и запуска
ADV: Разработка	ADV_FSP.1 Неформальная функциональная спецификация
	ADV_HLD.1 Описательный проект верхнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия

Окончание таблицы 8

Класс доверия	Компоненты доверия
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ATE: Тестирование	ATE_COV.1 Свидетельство покрытия
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.1 Анализ уязвимостей разработчиком

10.5 Оценочный уровень доверия 3 (ОУД3), предусматривающий методическое тестирование и проверку

10.5.1 Цели

ОУД3 позволяет добросовестному разработчику достичь максимального увеличения доверия путем применения надлежащего проектирования безопасности без значительного изменения существующей практики качественной разработки.

ОУД3 применяют в случаях, если разработчикам или пользователям требуется независимо подтверждаемый умеренный уровень доверия на основе всестороннего исследования ОО и процесса его разработки без существенных затрат на изменение технологии проектирования.

10.5.2 Компоненты доверия

ОУД3 (см. таблицу 9) обеспечивает доверие путем анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов, руководств и проекта ОО верхнего уровня.

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации **и проекте верхнего уровня**, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций и свидетельством поиска разработчиком явных уязвимостей (например, из общедоступных источников).

ОУД3 также обеспечивает доверие **посредством использования мер управления средой разработки, управления конфигурацией ОО** и свидетельства безопасных процедур поставки.

ОУД3 представляет значимое увеличение доверия по сравнению с ОУД2, требуя более полного покрытия тестированием функций и механизмов безопасности и/или процедур безопасности, что дает некоторую уверенность в том, что в ОО не будут внесены искажения во время разработки.

Таблица 9 — ОУД3

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_CAP.3 Средства контроля авторизации
	ACM_SCP.1 Охват УК объекта оценки
ADO: Поставка и эксплуатация	ADO_DEL.1 Процедуры поставки
	ADO_IGS.1 Процедуры установки, генерации и запуска
ADV: Разработка	ADV_FSP.1 Неформальная функциональная спецификация
	ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ALC: Поддержка жизненного цикла	ALC_DVS.1 Идентификация мер безопасности

Окончание таблицы 9

Класс доверия	Компоненты доверия
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.1 Тестирование: проект верхнего уровня
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA:Оценка уязвимостей	AVA_MSU.1 Экспертиза руководств
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.1 Анализ уязвимостей разработчиком

10.6 Оценочный уровень доверия 4 (ОУД4), предусматривающий методическое проектирование, тестирование и углубленную проверку

10.6.1 Цели

ОУД4 позволяет разработчику достичь максимального увеличения доверия путем применения надлежащего проектирования безопасности, основанного на обычной коммерческой практике разработки, которая, будучи строгой, не требует глубоких специальных знаний, навыков и других ресурсов. ОУД4 — самый высокий уровень, на который, вероятно, экономически целесообразно ориентироваться при оценке уже существующих продуктов.

Поэтому ОУД4 применяют, если разработчикам или пользователям требуется независимо подтверждаемый уровень доверия от умеренного до высокого в ОО общего назначения и имеется готовность нести дополнительные, производственные затраты, связанные с обеспечением безопасности.

10.6.2 Компоненты доверия

ОУД4 (см. таблицу 10) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, **полной** спецификации интерфейсов, руководств, проекта ОО верхнего уровня **и нижнего уровня, а также подмножества реализации. Доверие дополнительно достигается применением неформальной модели политики безопасности ОО.**

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации и проекте верхнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей **и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с низким потенциалом нападения.**

ОУД4 также обеспечивает доверие посредством использования мер управления средой разработки, **дополнительного** управления конфигурацией ОО, **включая автоматизацию,** и свидетельства безопасных процедур поставки.

ОУД4 представляет значимое увеличение доверия по сравнению с ОУД3, требуя более детального описания проекта, подмножества реализации и улучшенных механизмов и/или процедур, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки или поставки.

Таблица 10 — ОУД4

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_AUT.1 Частичная автоматизация УК
	ACM_CAP.4 Поддержка генерации, процедуры приемки
	ACM_SCP.2 Охват УК отслеживания проблем
ADO: Поставка и эксплуатация	ADO_DEL.2 Обнаружение модификации
	ADO_IGS.1 Процедуры установки, генерации и запуска

Окончание таблицы 10

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_FSP.2 Полностью определенные внешние интерфейсы
	ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1 Подмножество реализации ФБО
	ADV_LLD.1 Описательный проект нижнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия
	ADV_SPM.1 Неформальная модель политики безопасности ОО
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ALC: Поддержка жизненного цикла	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Модель жизненного цикла, определенная разработчиком
	ALC_TAT.1 Полностью определенные инструментальные средства разработки
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.1 Тестирование: проект верхнего уровня
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_MSU.2 Подтверждение правильности анализа
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.2 Независимый анализ уязвимостей

10.7 Оценочный уровень доверия 5 (ОУД5), предусматривающий полуформальное проектирование и тестирование

10.7.1 Цели

ОУД5 позволяет разработчику достичь максимального увеличения доверия путем проектирования безопасности, основанного на строгой коммерческой практике разработки, поддержанного умеренным применением узкоспециализированных методов проектирования безопасности. Такие ОО будут, вероятно, проектироваться и разрабатываться с намерением достичь ОУД5. Скорее всего, дополнительные затраты, сопутствующие требованиям ОУД5 в части строгости разработки, не будут большими без учета применения специализированных методов.

Поэтому ОУД5 применяют, если разработчикам или пользователям требуется независимо получаемый высокий уровень доверия для запланированной разработки со строгим подходом к разработке, не влекущим излишних затрат на применение узкоспециализированных методов проектирования безопасности.

10.7.2 Компоненты доверия

ОУД5 (см. таблицу 11) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего уровня и нижнего уровня, а также **всей** реализации. Доверие дополнительно достигается применением **формальной** модели политики безопасности ОО **и полуформального представления функциональной спецификации и проекта верхнего уровня, а также полуформальной демонстрации соответствия между ними. Кроме этого, требуется модульное проектирование ОО.**

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня **и проекте нижнего уровня**, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, де-

монстрирующим противодействие попыткам проникновения нарушителей с **умеренным** потенциалом нападения. **Анализ также включает в себя проверку правильности анализа разработчиком скрытых каналов.**

ОУД5 также обеспечивает доверие посредством использования контроля среды разработки, **всестороннего** управления конфигурацией ОО, включая автоматизацию, и свидетельства безопасных процедур поставки.

ОУД5 представляет значимое увеличение доверия по сравнению с ОУД4, требуя полуформального описания проекта, полной реализации, более структурированной (и, следовательно, лучше анализируемой) архитектуры, анализа скрытых каналов и улучшенных механизмов и/или процедур, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки.

Таблица 11 — ОУД5

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_AUT.1 Частичная автоматизация УК
	ACM_CAP.4 Поддержка генерации, процедуры приемки
	ACM_SCP.3 Охват УК инструментальных средств разработки
ADO: Поставка и эксплуатация	ADO_DEL.2 Обнаружение модификации
	ADO_IGS.1 Процедуры установки, генерации и запуска
ADV: Разработка	ADV_FSP.3 Полуформальная функциональная спецификация
	ADV_HLD.3 Полуформальный проект верхнего уровня
	ADV_IMP.2 Реализация ФБО
	ADV_INT.1 Модульность
	ADV_LLD.1 Описательный проект нижнего уровня
	ADV_RCR.2 Полуформальная демонстрация соответствия
	ADV_SPM.3 Формальная модель политики безопасности ОО
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ALC: Поддержка жизненного цикла	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.2 Стандартизованная модель жизненного цикла
	ALC_TAT.2 Соответствие стандартам реализации
ATE: Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.2 Тестирование: проект нижнего уровня
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_CCA.1 Анализ скрытых каналов
	AVA_MSU.2 Подтверждение правильности анализа
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.3 Умеренно стойкий

10.8 Оценочный уровень доверия 6 (ОУД6), предусматривающий полуформальную верификацию проекта и тестирование

10.8.1 Цели

ОУД6 позволяет разработчикам достичь высокого уровня доверия путем применения специальных методов проектирования безопасности в строго контролируемой среде разработки с целью получения высококачественного ОО для защиты высоко оцениваемых активов от значительных рисков.

Поэтому ОУД6 применяют для разработки безопасных ОО с целью использования в ситуациях высокого риска, где ценность защищаемых активов оправдывает дополнительные затраты.

10.8.2 Компоненты доверия

ОУД6 (см. таблицу 12) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего уровня и нижнего уровня, а также **структурированного представления** реализации. Доверие дополнительно достигается применением формальной модели политики безопасности ОО и полуформального представления функциональной спецификации, проекта верхнего уровня **и проекта нижнего уровня**, а также полуформальной демонстрации соответствия между ними. Кроме того, требуется модульное **и иерархическое (по уровням)** проектирование ОО.

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня и проекте нижнего уровня, выборочным независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с **высоким** потенциалом нападения. Анализ также включает в себя проверку правильности **систематического** анализа разработчиком скрытых каналов.

ОУД6 также обеспечивает доверие посредством использования **структурированного процесса разработки**, контроля среды разработки, всестороннего управления конфигурацией ОО, включая **полную** автоматизацию, и свидетельства безопасных процедур поставки.

ОУД6 представляет значимое увеличение доверия по сравнению с ОУД5, требуя всестороннего анализа, структурированного представления реализации, более стройной структуры (например, с разбиением на уровни), всестороннего независимого анализа уязвимостей, систематической идентификации скрытых каналов, улучшенного управления конфигурацией и улучшенного контроля среды разработки.

Таблица 12 — ОУД6

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_AUT.2 Полная автоматизация УК
	ACM_CAP.5 Расширенная поддержка
	ACM_SCP.3 Охват УК инструментальных средств разработки
ADO: Поставка и эксплуатация	ADO_DEL.2 Обнаружение модификации
	ADO_IGS.1 Процедуры установки, генерации и запуска
ADV: Разработка	ADV_FSP.3 Полуформальная функциональная спецификация
	ADV_HLD.4 Пояснения в полуформальном проекте верхнего уровня
	ADV_IMP.3 Структурированная реализация ФБО
	ADV_INT.2 Уменьшение сложности
	ADV_LLD.2 Полуформальный проект нижнего уровня
	ADV_RCR.2 Полуформальная демонстрация соответствия
	ADV_SPM.3 Формальная модель политики безопасности ОО
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ALC: Поддержка жизненного цикла	ALC_DVS.2 Достаточность мер безопасности
	ALC_LCD.2 Стандартизованная модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей объекта оценки стандартам реализации

Окончание таблицы 12

Класс доверия	Компоненты доверия
ATE: Тестирование	ATE_COV.3 Строгий анализ покрытия
	ATE_DPT.2 Тестирование: проект нижнего уровня
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_CCA.2 Систематический анализ скрытых каналов
	AVA_MSU.3 Анализ и тестирование опасных состояний
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.4 Высокостойкий

10.9 Оценочный уровень доверия 7 (ОУД7), предусматривающий формальную верификацию проекта и тестирование

10.9.1 Цели

ОУД7 применим при разработке безопасных ОО для использования в ситуациях чрезвычайно высокого риска и/или там, где высокая ценность активов оправдывает повышенные затраты. Практическое применение ОУД7 в настоящее время ограничено ОО, которые строго ориентированы на реализацию функциональных возможностей безопасности и для которых возможен подробный формальный анализ.

10.9.2 Компоненты доверия

ОУД7 (см. таблицу 13) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего и нижнего уровней, а также структурированного представления реализации. Доверие дополнительно достигается применением формальной модели политики безопасности ОО, **формального представления функциональной спецификации и проекта верхнего уровня,** полуформального представления проекта нижнего уровня, а также **формальной (если требуется)** и полуформальной демонстрации соответствия между ними. Кроме того, требуется модульное, иерархическое (по уровням) **и простое** проектирование ОО.

Анализ поддержан независимым тестированием ФБО, свидетельством разработчика об испытаниях, основанных на функциональной спецификации, проекте верхнего уровня, проекте нижнего уровня **и представлении реализации, полным** независимым подтверждением результатов тестирования разработчиком, анализом стойкости функций, свидетельством поиска разработчиком уязвимостей и независимым анализом уязвимостей, демонстрирующим противодействие попыткам проникновения нарушителей с высоким потенциалом нападения. Анализ также включает в себя проверку правильности систематического анализа разработчиком скрытых каналов.

ОУД7 также обеспечивает доверие посредством использования структурированного процесса разработки, средств контроля среды разработки, всестороннего управления конфигурацией ОО, включая полную автоматизацию, и свидетельства безопасных процедур поставки.

ОУД7 представляет значимое увеличение доверия по сравнению с ОУД6, требуя всестороннего анализа, использующего формальные представления и формальное соответствие, а также всестороннего тестирования.

Таблица 13 — ОУД7

Класс доверия	Компоненты доверия
ACM: Управление конфигурацией	ACM_AUT.2 Полная автоматизация УК
	ACM_CAP.5 Расширенная поддержка
	ACM_SCP.3 Охват УК инструментальных средств разработки
ADO: Поставка и эксплуатация	ADO_DEL.3 Предотвращение модификации
	ADO_IGS.1 Процедуры установки, генерации и запуска

Окончание таблицы 13

Класс доверия	Компоненты доверия
ADV: Разработка	ADV_FSP.4 Формальная функциональная спецификация
	ADV_HLD.5 Формальный проект верхнего уровня
	ADV_IMP.3 Структурированная реализация ФБО
	ADV_INT.3 Минимизация сложности
	ADV_LLD.2 Полуформальный проект нижнего уровня
	ADV_RCR.3 Формальная демонстрация соответствия
	ADV_SPM.3 Формальная модель политики безопасности ОО
AGD: Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
ALC: Поддержка жизненного цикла	ALC_DVS.2 Достаточность мер безопасности
	ALC_LCD.3 Измеримая модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей объекта оценки стандартам реализации
ATE: Тестирование	ATE_COV.3 Строгий анализ покрытия
	ATE_DPT.3 Тестирование на уровне реализации
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.3 Полное независимое тестирование
AVA: Оценка уязвимостей	AVA_CCA.2 Систематический анализ скрытых каналов
	AVA_MSU.3 Анализ и тестирование опасных состояний
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.4 Высокостойкий

11 Классы, семейства и компоненты доверия

Разделы 12 — 18 содержат детализированные требования, представленные во всех компонентах доверия, сгруппированных в классы и семейства в алфавитном порядке в соответствии с латинским алфавитом.

12 Класс ACM. Управление конфигурацией

Управление конфигурацией (УК) — один из способов установить, что в созданном ОО реализованы функциональные требования и спецификации. УК отвечает этим целям, предъявляя требования дисциплины и контроля в процессе уточнения и модификации ОО и связанной с ним информации. Системы УК используют для обеспечения целостности частей ОО, которые они контролируют, предоставляя метод отслеживания любых изменений, и для того, чтобы все изменения были санкционированы.

Декомпозиция класса ACM «Управление конфигурацией» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 8.

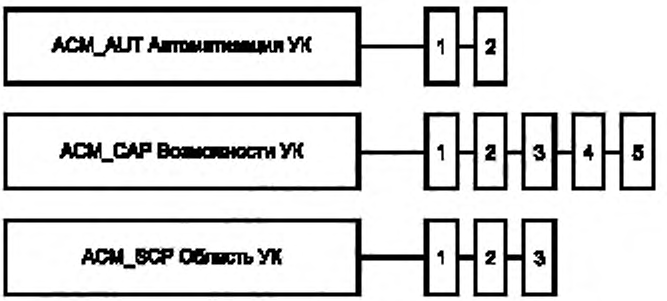


Рисунок 8 — Декомпозиция класса ACM
«Управление конфигурацией»

12.1 Автоматизация УК (ACM_AUT)

12.1.1 Цели

Цель привлечения инструментальных средств автоматизации УК — повышение эффективности системы УК. Несмотря на то, что как автоматизированные, так и ручные системы УК могут быть обойдены, проигнорированы или оказаться недостаточными для предотвращения несанкционированной модификации, автоматизированные системы менее восприимчивы к человеческому фактору — ошибке или небрежности.

12.1.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе набора элементов конфигурации, которые управляются с применением автоматизированных средств.

12.1.3 Замечания по применению

ACM_AUT.1.1C содержит требование, которое связано с представлением реализации ОО. Представление реализации ОО включает в себя все аппаратные, программные и программно-аппаратные средства, которые фактически составляют ОО. В случае, когда ОО состоит только из программных средств, представление реализации может состоять исключительно из исходного и объектного кода.

ACM_AUT.1.2C содержит требование, чтобы система УК предоставила автоматизированные средства для поддержки генерации ОО. При этом требуется, чтобы система УК предоставила автоматизированные средства, содействующие принятию заключения, что при генерации ОО использованы правильные элементы конфигурации.

ACM_AUT.2.5C содержит требование, чтобы система УК предоставила автоматизированные средства, позволяющие установить различия между ОО и его предыдущей версией. Если предыдущей версии ОО не существует, разработчик все равно нуждается в предоставлении автоматизированных средств, чтобы установить различия между ОО и последующей версией ОО.

12.1.4 ACM_AUT.1 Частичная автоматизация УК

Зависимости: ACM_CAP.3 Средства контроля авторизации

12.1.4.1 Цели

В тех средах разработки, где представление реализации является сложным или создается многими разработчиками, трудно контролировать изменения без использования автоматизированных инструментальных средств. В частности, от этих автоматизированных инструментальных средств требуется способность поддерживать многочисленные изменения, которые возникают в процессе разработки, и обеспечить санкционированность этих изменений. Целью данного компонента является обеспечение контроля представления реализации с использованием автоматизированных средств.

12.1.4.2 Элементы действий разработчика

12.1.4.2.1 ACM_AUT.1.1D

Разработчик должен использовать систему УК.

12.1.4.2.2 ACM_AUT.1.2D

Разработчик должен представить план УК.

12.1.4.3 Элементы содержания и представления свидетельств

12.1.4.3.1 ACM_AUT.1.1C

Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО проводятся только санкционированные изменения.

12.1.4.3.2 ACM_AUT.1.2C

Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

12.1.4.3.3 ACM_AUT.1.3C

План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

12.1.4.3.4 ACM_AUT.1.4C

План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

12.1.4.4 Элементы действий оценщика

12.1.4.4.1 ACM_AUT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.1.5 ACM_AUT.2 Полная автоматизация УК

Зависимости: ACM_CAP.3 Средства контроля авторизации

12.1.5.1 Цели

В тех средах разработки, где элементы конфигурации являются сложными или создаются многими разработчиками, трудно контролировать изменения без использования автоматизированных инструментальных средств. В частности, требуется, чтобы эти автоматизированные инструментальные средства были способны поддерживать многочисленные изменения, которые возникают в процессе разработки, и обеспечить санкционированность этих изменений. Целью данного компонента является обеспечение контроля всех элементов конфигурации с использованием автоматизированных средств.

Применение автоматизированных средств для выявления различий между версиями ОО и определение, на какие элементы конфигурации воздействует модификация других элементов конфигурации, содействуют определению воздействия изменений на последовательные версии ОО. Последнее, в свою очередь, может предоставить ценную информацию, позволяющую определить, реализованы ли изменения ОО во всех элементах конфигурации, требующих согласования между собой.

12.1.5.2 Элементы действий разработчика

12.1.5.2.1 ACM_AUT.2.1D

Разработчик должен использовать систему УК.

12.1.5.2.2 ACM_AUT.2.2D

Разработчик должен представить план УК.

12.1.5.3 Элементы содержания и представления свидетельств

12.1.5.3.1 ACM_AUT.2.1C

Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО и во всех остальных элементах конфигурации производятся только санкционированные изменения.

12.1.5.3.2 ACM_AUT.2.2C

Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

12.1.5.3.3 ACM_AUT.2.3C

План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

12.1.5.3.4 ACM_AUT.2.4C

План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

12.1.5.3.5 ACM_AUT.2.5C

Система УК должна предоставить автоматизированные средства для выявления различий между ОО и его предшествующей версией.

12.1.5.3.6 ACM_AUT.2.6C

Система УК должна предоставить автоматизированные средства для определения всех других элементов конфигурации, на которые воздействует модификация данного элемента конфигурации.

12.1.5.4 Элементы действий оценщика

12.1.5.4.1 ACM_AUT.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.2 Возможности УК (ACM_CAP)

12.2.1 Цели

Возможности системы УК связаны с вероятностью того, что могут произойти случайные или несанкционированные модификации элементов конфигурации. Необходимо, чтобы система УК обеспечивала целостность ОО, начиная с ранних этапов проектирования и на протяжении всей последующей деятельности по сопровождению.

Цели этого семейства состоят в:

a) обеспечении корректности и полноты ОО к моменту представления его потребителю;

b) обеспечении того, чтобы никакие элементы конфигурации не были пропущены в процессе оценки;

c) предотвращении несанкционированной модификации, добавления или удаления элементов конфигурации ОО.

В случае, если ОО является подмножеством некоторого продукта, требования класса ACM применяют только к элементам конфигурации ОО, а не к продукту в целом. Хотя желательно, чтобы управление конфигурацией применялось уже на ранних стадиях проектирования и продолжалось в дальнейшем, класс ACM содержит только требования, чтобы управление конфигурацией имелось и использовалось к моменту окончания оценки.

12.2.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе возможностей системы УК, объема документации УК, представленной разработчиком, и того, представлено ли разработчиком логическое обоснование соответствия системы УК требованиям безопасности.

12.2.3 Замечания по применению

ACM_CAP.2 «Элементы конфигурации» содержит отдельные требования, которые относятся к элементам конфигурации. Семейство ACM_SCP содержит требования по составу элементов конфигурации, отслеживаемых системой УК.

ACM_CAP.2.3C содержит требование, чтобы был представлен список конфигурации. Список конфигурации содержит все элементы конфигурации, которые сопровождаются системой УК.

ACM_CAP.2.7C содержит требование, чтобы система УК уникально идентифицировала все элементы конфигурации. Также требуется, чтобы модификация элемента конфигурации приводила к назначению нового уникального идентификатора.

ACM_CAP.3.9C содержит требование, чтобы свидетельство демонстрировало функционирование системы УК в соответствии с планом УК. Примерами такого свидетельства являются как документация типа образов экрана или журнала аудита для системы УК, так и подробная демонстрация системы УК разработчиком. Оценщик является ответственным за заключение, что это свидетельство является достаточным для демонстрации того, что система УК функционирует в соответствии с планом УК.

ACM_CAP.3.10C содержит требование представления свидетельства, показывающего, что все элементы конфигурации поддерживаются системой УК. Так как элементом конфигурации считается элемент, включенный в список конфигурации, данное требование устанавливает, что все элементы списка конфигурации поддерживаются системой УК.

ACM_CAP.4.12C содержит требование, чтобы система УК поддерживала генерацию ОО. Для этого требуется, чтобы система УК предоставила информационные и/или электронные средства, содействующие принятию заключения, что при генерации ОО использованы правильные элементы конфигурации.

В семействе ACM_CAP «Возможности УК» определяются требования УК, предъявляемые ко всем элементам, идентифицированным в списке элементов конфигурации. Кроме самого ОО, ACM_CAP «Возможности УК» оставляет содержание списка элементов конфигурации на усмотрение разработчика (семейство ACM_CAP «Возможности УК» может использоваться для идентификации конкретных элементов, которые должны быть включены в список элементов конфигурации и, следовательно, охвачены УК).

12.2.4 ACM_CAP.1 Номера версий

Зависимости: нет зависимостей.

12.2.4.1 Цели

Требуется уникальная маркировка для обеспечения однозначности в определении оцениваемого экземпляра ОО. Обозначение ОО соответствующей маркировкой дает пользователям ОО возможность знать о том, какой экземпляр ОО они используют.

12.2.4.2 Элементы действий разработчика

12.2.4.2.1 ACM_CAP.1.1D

Разработчик должен предоставить маркировку для ОО.

12.2.4.3 Элементы содержания и представления свидетельств

12.2.4.3.1 ACM_CAP.1.1C

Маркировка ОО должна быть уникальна для каждой версии ОО.

12.2.4.3.2 ACM_CAP.1.2C

ОО должен быть помечен маркировкой.

12.2.4.4 Элементы действий оценщика

12.2.4.4.1 ACM_CAP.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.2.5 ACM_CAP.2 Элементы конфигурации

Зависимости: нет зависимостей.

12.2.5.1 Цели

Требуется уникальная маркировка для обеспечения однозначности в определении оцениваемого экземпляра ОО. Обозначение ОО соответствующей маркировкой дает пользователям ОО возможность знать о том, какой экземпляр ОО они используют.

Уникальная идентификация элементов конфигурации ведет к лучшему пониманию состава ОО, что, в свою очередь, способствует определению элементов, на которые направлены требования оценки для ОО.

12.2.5.2 Элементы действий разработчика

12.2.5.2.1 ACM_CAP.2.1D

Разработчик должен предоставить маркировку для ОО.

12.2.5.2.2 ACM_CAP.2.2D

Разработчик должен использовать систему УК.

12.2.5.2.3 ACM_CAP.2.3D

Разработчик должен представить документацию УК.

12.2.5.3 Элементы содержания и представления свидетельств

12.2.5.3.1 ACM_CAP.2.1C

Маркировка ОО должна быть уникальна для каждой версии ОО.

12.2.5.3.2 ACM_CAP.2.2C

ОО должен быть помечен маркировкой.

12.2.5.3.3 ACM_CAP.2.3C

Документация УК должна включать в себя список конфигурации.

12.2.5.3.4 ACM_CAP.2.4C

Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.5.3.5 ACM_CAP.2.5C

Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

12.2.5.3.6 ACM_CAP.2.6C

Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.

12.2.5.3.7 ACM_CAP.2.7C

Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.5.4 Элементы действий оценщика

12.2.5.4.1 ACM_CAP.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.2.6 ACM_CAP.3 Средства контроля авторизации

Зависимости: ALC_DVS.1 Идентификация мер безопасности

12.2.6.1 Цели

Требуется уникальная маркировка для обеспечения однозначности в определении оцениваемого экземпляра ОО. Обозначение ОО соответствующей маркировкой дает пользователям ОО возможность знать о том, какой экземпляр ОО они используют.

Уникальная идентификация элементов конфигурации ведет к лучшему пониманию состава ОО, что, в свою очередь, способствует определению элементов, на которые направлены требования оценки для ОО.

Поддержанию целостности ОО способствуют применение средств контроля, предупреждающих выполнение несанкционированных модификаций ОО, а также обеспечение надлежащих функциональных возможностей и использование системы УК.

12.2.6.2 Элементы действий разработчика

12.2.6.2.1 ACM_CAP.3.1D

Разработчик должен предоставить маркировку для ОО.

12.2.6.2.2 ACM_CAP.3.2D

Разработчик должен использовать систему УК.

12.2.6.2.3 ACM_CAP.3.3D

Разработчик должен представить документацию УК.

12.2.6.3 Элементы содержания и представления свидетельств

12.2.6.3.1 ACM_CAP.3.1C

Маркировка ОО должна быть уникальна для каждой версии ОО.

12.2.6.3.2 ACM_CAP.3.2C

ОО должен быть помечен маркировкой.

12.2.6.3.3 ACM_CAP.3.3C

Документация УК должна включать в себя список конфигурации и план УК.

12.2.6.3.4 ACM_CAP.3.4C

Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.6.3.5 ACM_CAP.3.5C

Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

12.2.6.3.6 ACM_CAP.3.6C

Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.

12.2.6.3.7 ACM_CAP.3.7C

Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.6.3.8 ACM_CAP.3.8C

План УК должен содержать описание, как используется система УК.

12.2.6.3.9 ACM_CAP.3.9C

Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

12.2.6.3.10 ACM_CAP.3.10C

Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

12.2.6.3.11 ACM_CAP.3.11C

Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

12.2.6.4 Элементы действий оценщика

12.2.6.4.1 ACM_CAP.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.2.7 ACM_CAP.4 Поддержка генерации, процедуры приемки

Зависимости: ALC_DVS.1 Идентификация мер безопасности

12.2.7.1 Цели

Требуется уникальная маркировка для обеспечения однозначности в определении оцениваемого экземпляра ОО. Обозначение ОО соответствующей маркировкой дает пользователям ОО возможность знать, какой экземпляр ОО они используют.

Уникальная идентификация элементов конфигурации ведет к лучшему пониманию состава ОО, что, в свою очередь, способствует определению тех элементов, на которые направлены требования оценки для ОО.

Поддержанию целостности ОО способствуют применение средств контроля, предупреждающих выполнение несанкционированных модификаций ОО, а также обеспечение надлежащих функциональных возможностей и использование системы УК.

Предназначение процедур приемки — подтвердить, что любое создание или модификация элементов конфигурации санкционировано.

12.2.7.2 Элементы действий разработчика

12.2.7.2.1 ACM_CAP.4.1D

Разработчик должен предоставить маркировку для ОО.

12.2.7.2.2 ACM_CAP.4.2D

Разработчик должен использовать систему УК.

12.2.7.2.3 ACM_CAP.4.3D

Разработчик должен представить документацию УК.

12.2.7.3 Элементы содержания и представления свидетельств

12.2.7.3.1 ACM_CAP.4.1C

Маркировка ОО должна быть уникальна для каждой версии ОО.

12.2.7.3.2 ACM_CAP.4.2C

ОО должен быть помечен маркировкой.

12.2.7.3.3 ACM_CAP.4.3C

Документация УК должна включать в себя список конфигурации, план УК **и план приемки под УК** (подпункт 12.2.7.3.13).

12.2.7.3.4 ACM_CAP.4.4C

Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.7.3.5 ACM_CAP.4.5C

Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

12.2.7.3.6 ACM_CAP.4.6C

Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.

12.2.7.3.7 ACM_CAP.4.7C

Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.7.3.8 ACM_CAP.4.8C

План УК должен содержать описание, как используется система УК.

12.2.7.3.9 ACM_CAP.4.9C

Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

12.2.7.3.10 ACM_CAP.4.10C

Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

12.2.7.3.11 ACM_CAP.4.11C

Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

12.2.7.3.12 ACM_CAP.4.12C

Система УК должна поддерживать генерацию ОО.

12.2.7.3.13 ACM_CAP.4.13C

План приемки должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.

12.2.7.4 Элементы действий оценщика

12.2.7.4.1 ACM_CAP.4.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.2.8 ACM_CAP.5 Расширенная поддержка

Зависимости: ALC_DVS.2 Достаточность мер безопасности

12.2.8.1 Цели

Требуется уникальная маркировка для обеспечения однозначности в определении оцениваемого экземпляра ОО. Обозначение ОО соответствующей маркировкой дает пользователям ОО возможность знать, какой экземпляр ОО они используют.

Уникальная идентификация элементов конфигурации ведет к лучшему пониманию состава ОО, что, в свою очередь, способствует определению тех элементов, на которые направлены требования оценки для ОО.

Поддержанию целостности ОО способствуют применение средств контроля, предупреждающих выполнение несанкционированных модификаций ОО, а также обеспечение надлежащих функциональных возможностей и использование системы УК.

Предназначение процедур приемки — подтвердить, что любое создание или модификация элементов конфигурации санкционировано.

Процедуры компоновки способствуют правильному выполнению генерации ОО из управляемого набора элементов конфигурации санкционированным способом.

Требование, чтобы система УК была способна идентифицировать оригинал материала, используемый для генерации ОО, способствует сохранению целостности этого материала путем применения приемлемых технических, физических и процедурных мер защиты.

12.2.8.2 Элементы действий разработчика

12.2.8.2.1 ACM_CAP.5.1D

Разработчик должен предоставить маркировку для ОО.

12.2.8.2.2 ACM_CAP.5.2D

Разработчик должен использовать систему УК.

12.2.8.2.3 ACM_CAP.5.3D

Разработчик должен представить документацию УК.

12.2.8.3 Элементы содержания и представления свидетельств

12.2.8.3.1 ACM_CAP.5.1C

Маркировка ОО должна быть уникальна для каждой версии ОО.

12.2.8.3.2 ACM_CAP.5.2C

ОО должен быть помечен маркировкой.

12.2.8.3.3 ACM_CAP.5.3C

Документация УК должна включать в себя список конфигурации, план УК, план приемки под УК **и процедуры компоновки.**

12.2.8.3.4 ACM_CAP.5.4C

Список конфигурации должен уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.8.3.5 ACM_CAP.5.5C

Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

12.2.8.3.6 ACM_CAP.5.6C

Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации, входящих в ОО.

12.2.8.3.7 ACM_CAP.5.7C

Система УК должна уникально идентифицировать все элементы конфигурации, входящие в ОО.

12.2.8.3.8 ACM_CAP.5.8C

План УК должен содержать описание, как используется система УК.

12.2.8.3.9 ACM_CAP.5.9C

Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

12.2.8.3.10 ACM_CAP.5.10C

Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

12.2.8.3.11 ACM_CAP.5.11C

Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

12.2.8.3.12 ACM_CAP.5.12C

Система УК должна поддерживать генерацию ОО.

12.2.8.3.13 ACM_CAP.5.13C

План приемки должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.

12.2.8.3.14 ACM_CAP.5.14C

Процедуры компоновки должны описать, как систему УК применяют в процессе изготовления ОО.

12.2.8.3.15 ACM_CAP.5.15C

Система УК должна содержать требование, чтобы лицо, ответственное за включение элемента конфигурации под УК, не являлось его разработчиком.

12.2.8.3.16 ACM_CAP.5.16C

Система УК должна четко идентифицировать элементы конфигурации, которые составляют ФБО.

12.2.8.3.17 ACM_CAP.5.17C

Система УК должна поддерживать аудит всех модификаций ОО с регистрацией, как минимум, инициатора, даты и времени модификации в журнале аудита.

12.2.8.3.18 ACM_CAP.5.18C

Система УК должна быть способна идентифицировать оригиналы всех материалов, используемые для генерации ОО.

12.2.8.3.19 ACM_CAP.5.19C

Документация УК должна демонстрировать, что использование системы УК совместно с мерами безопасности разработки сделает возможными только санкционированные изменения в ОО.

12.2.8.3.20 ACM_CAP.5.20C

Документация УК должна демонстрировать, что использование процедур компоновки обеспечивает выполнение генерации ОО правильно и санкционированным способом.

12.2.8.3.21 ACM_CAP.5.21C

Документация УК должна демонстрировать, что система УК достаточна для обеспечения того, чтобы лицо, ответственное за включение элемента конфигурации под УК, не было его разработчиком.

12.2.8.3.22 ACM_CAP.5.22C

Документация УК должна содержать логическое обоснование, что процедуры приемки обеспечивают адекватный и удобный просмотр изменений всех элементов конфигурации.

12.2.8.4 Элементы действий оценщика

12.2.8.4.1 ACM_CAP.5.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.3 Область УК (ACM_SCP)

12.3.1 Цели

Цель этого семейства — требовать, чтобы были определены элементы в качестве элементов конфигурации и, следовательно, помещены под УК в соответствии с требованиями семейства ACM_CAP «Возможности УК». Применение управления конфигурацией по отношению к элементам обеспечивает дополнительное доверие к поддержанию целостности ОО.

12.3.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе того, что именно из перечисленного ниже требуется определить в качестве элементов конфигурации: представление реализации, свидетельства оценки, требуемые компонентами доверия из ЗБ, недостатки безопасности, инструментальные средства разработки и связанная с ними информация.

12.3.3 Замечания по применению

Требования семейства ACM_CAP «Возможности УК» определяют необходимость списка элементов конфигурации (помимо самого ОО) и то, чтобы каждый элемент из этого списка находился под УК; при этом содержание списка элементов конфигурации оставляют на усмотрение разработчика. Требования семейства ACM_SCP «Область УК» ограничивают эту возможность разработчика, идентифицируя элементы, которые должны быть включены в список элементов конфигурации и, следовательно, находиться под УК в соответствии с требованиями семейства ACM_CAP «Возможности УК».

ACM_SCP.1.1C содержит требование, чтобы представление реализации ОО было включено в список элементов конфигурации. Представление реализации ОО относится ко всем аппаратным, программным и программно-аппаратным средствам, которые составляют ОО. В случае, если ОО состоит только из программных средств, представление реализации может состоять исключительно из исходного и объектного кода.

ACM_SCP.1.1C также содержит требование, чтобы свидетельства оценки, требуемые компонентами доверия из ЗБ, были включены в список элементов конфигурации.

ACM_SCP.2.1C содержит требование, чтобы системой УК отслеживались недостатки безопасности, то есть сопровождалась информация об имевших место недостатках безопасности и их устранении, а также подробные сведения о существующих недостатках безопасности.

ACM_SCP.3.1C содержит требование, чтобы системой УК отслеживались инструментальные средства разработки и относящаяся к ним информация. Примеры инструментальных средств разработки — это языки программирования и компиляторы. Информация, имеющая отношение к элементам генерации ОО (например, опции компилятора, опции инсталляции/генерации и опции компоновки) — пример информации, относящейся к инструментальным средствам разработки.

12.3.4 ACM_SCP.1 Охват УК объекта оценки

Зависимости: ACM_CAP.3 Средства контроля авторизации

12.3.4.1 Цели

Система УК может контролировать изменения только тех элементов, которые были включены под УК (например, элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под УК представления реализации ОО, свидетельств оценки, требуемых другими компонентами доверия из ЗБ, обеспечивает доверие, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

12.3.4.2 Элементы действий разработчика

12.3.4.2.1 ACM_SCP.1.1D

Разработчик должен представить список элементов конфигурации для ОО.

12.3.4.3 Элементы содержания и представления свидетельств

12.3.4.3.1 ACM_SCP.1.1C

Список элементов конфигурации должен включать в себя: представление реализации и свидетельства оценки, требуемые компонентами доверия из ЗБ.

12.3.4.4 Элементы действий оценщика

12.3.4.4.1 ACM_SCP.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.3.5 ACM_SCP.2 Охват УК отслеживания проблем

Зависимости: ACM_CAP.3 Средства контроля авторизации

12.3.5.1 Цели

Система УК может контролировать изменения только тех элементов, которые включены под УК (то есть элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под УК представления реализации ОО и свидетельств оценки, требуемых другими компонентами доверия из ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Включение недостатков безопасности под УК не позволяет утратить или игнорировать сообщения о недостатках безопасности, позволяя разработчику контролировать недостатки безопасности вплоть до их устранения.

12.3.5.2 Элементы действий разработчика

12.3.5.2.1 ACM_SCP.2.1D

Разработчик должен представить список элементов конфигурации для ОО.

12.3.5.3 Элементы содержания и представления свидетельств

12.3.5.3.1 ACM_SCP.2.1C

Список элементов конфигурации должен включать следующее: представление реализации, **недостатки безопасности** и свидетельства оценки, требуемые компонентами доверия из ЗБ.

12.3.5.4 Элементы действий оценщика

12.3.5.4.1 ACM_SCP.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

12.3.6 ACM_SCP.3 Охват УК инструментальных средств разработки

Зависимости: ACM_CAP.3 Средства контроля авторизации

12.3.6.1 Цели

Система УК может контролировать изменения только тех элементов, которые включены под УК (то есть элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под УК представления реализации ОО и свидетельств оценки, требуемых другими компонентами доверия из ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Включение недостатков безопасности под УК не позволяет утратить или игнорировать сообщения о недостатках безопасности, позволяя разработчику контролировать недостатки безопасности вплоть до их устранения.

Инструментальные средства разработки играют важную роль в обеспечении изготовления качественной версии ОО. Следовательно, важно контролировать модификацию этих средств.

12.3.6.2 Элементы действий разработчика

12.3.6.2.1 ACM_SCP.3.1D

Разработчик должен представить список элементов конфигурации для ОО.

12.3.6.3 Элементы содержания и представления свидетельств

12.3.6.3.1 ACM_SCP.3.1C

Список элементов конфигурации должен включать в себя: представление реализации, недостатки безопасности, **инструментальные средства разработки и связанную с ними информацию**, а также свидетельства оценки, требуемые компонентами доверия из ЗБ.

12.3.6.4 Элементы действий оценщика

12.3.6.4.1 ACM_SCP.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13 Класс ADO. Поставка и эксплуатация

Класс ADO «Поставка и эксплуатация» содержит требования правильной поставки, установки, генерации и запуска ОО.

Декомпозиция класса ADO «Поставка и эксплуатация» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 9.



Рисунок 9 — Декомпозиция класса ADO «Поставка и эксплуатация»

13.1 Поставка (ADO_DEL)

13.1.1 Цели

Требования для поставки предусматривают такие средства и процедуры системы контроля и распространения, которые конкретизируют меры, необходимые для обеспечения доверия к тому, что безопасность ОО поддерживается во время распространения ОО. Для правильного выполнения распространения ОО процедуры, используемые для распространения ОО, должны учитывать идентифицированные в ПЗ/ЗБ угрозы, относящиеся к безопасности ОО во время поставки.

13.1.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе повышения требований к разработчику по поддержанию безопасности ОО во время его поставки.

13.1.3 Замечания по применению

Процедуры поставки могут затрагивать следующие проблемы:

a) обеспечение точного соответствия ОО, полученного потребителем, эталону ОО;

b) избежание/обнаружение какой-либо подделки актуальной версии ОО;

c) предотвращение представления фальсифицированной версии ОО;

d) избежание распространения нежелательной информации о распространении ОО потребителю;

e) избежание/обнаружение перехвата ОО во время поставки и

f) избежание задержки или недоставки ОО во время его распространения.

Хотя в процедурах рассматривается защита ОО во всех аспектах (целостность, конфиденциальность, доступность), технические меры, представленные в ADO_DEL.2 «Обнаружение модификации» и ADO_DEL.3 «Предотвращение модификации», требуются только в отношении проблем целостности.

13.1.4 ADO_DEL.1 Процедуры поставки

Зависимости: нет зависимостей.

13.1.4.1 Элементы действий разработчика

13.1.4.1.1 ADO_DEL.1.1D

Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

13.1.4.1.2 ADO_DEL.1.2.D

Разработчик должен использовать процедуры поставки.

13.1.4.2 Элементы содержания и представления свидетельств

13.1.4.2.1 ADO_DEL.1.1C

Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.

13.1.4.3 Элементы действий оценщика

13.1.4.3.1 ADO_DEL.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13.1.5 ADO_DEL.2 Обнаружение модификации

Зависимости: ACM_CAP.3 Средства контроля авторизации

13.1.5.1 Элементы действий разработчика

13.1.5.1.1 ADO_DEL.2.1D

Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

13.1.5.1.2 ADO_DEL.2.2D

Разработчик должен использовать процедуры поставки.

13.1.5.2 Элементы содержания и представления свидетельств

13.1.5.2.1 ADO_DEL.2.1C

Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

13.1.5.2.2 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.

13.1.5.2.3 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.

13.1.5.2.3 Элементы действий оценщика

13.1.5.3.1 ADO_DEL.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13.1.6 ADO_DEL.3 Предотвращение модификации

Зависимости: ACM_CAP.3 Средства контроля авторизации

13.1.6.1 Элементы действий разработчика

13.1.6.1.1 ADO_DEL.3.1D

Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

13.1.6.1.2 ADO_DEL.3.2D

Разработчик должен использовать процедуры поставки.

13.1.6.2 Элементы содержания и представления свидетельств

13.1.6.2.1 ADO_DEL.3.1C

Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.

13.1.6.2.2 ADO_DEL.3.2C

Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают предотвращение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

13.1.6.2.3 ADO_DEL.3.3C

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.

13.1.6.3 Элементы действий оценщика

13.1.6.3.1 ADO_DEL.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13.2 Установка, генерация и запуск (ADO_IGS)

13.2.1 Цели

Процедуры установки, генерации и запуска полезны для обеспечения того, чтобы ОО был установлен, сгенерирован и запущен безопасным способом так, как это предписано разработчиком. Требования, предъявляемые к установке, генерации и запуску, предусматривают безопасный переход от нахождения представления реализации ОО под управлением конфигурации к началу его эксплуатации в среде использования.

13.2.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы с учетом того, регистрируются ли опции генерации ОО.

13.2.3 Замечания по применению

Установлено, что применение указанных выше требований будет меняться в зависимости от различных аспектов, например, является ли ОО продуктом или системой ИТ, поставлен ли ОО в готовом к эксплуатации состоянии или он должен устанавливаться владельцем на месте эксплуатации и т.д. Для конкретного ОО обычно будет иметь место разделение ответственности по установке, генерации и запуску между разработчиком и владельцем ОО, но имеются примеры, когда все действия выполняются одной стороной. Например, для смарт-карты все аспекты установки, генерации и запуска могут выполняться по месту разработки ОО. С другой стороны, ОО может быть поставлен как система ИТ в форме программного обеспечения, где все аспекты установки, генерации и запуска выполняются по месту использования ОО.

Также возможен случай, когда ОО уже установлен до начала оценки. В этом случае может быть неуместным требовать и анализировать процедуры установки.

Более того, требования генерации применимы только к тем ОО, которые дают возможность генерировать составляющие вводимого в эксплуатацию ОО из их представления реализации.

Процедуры установки, генерации и запуска могут быть приведены в отдельном документе либо включены в другое административное руководство. Требования доверия в этом семействе представлены отдельно от требований семейства AGD_ADM «Руководство администратора» из-за редкого, возможно одноразового, использования процедур установки, генерации и запуска.

13.2.4 ADO_IGS.1 Процедуры установки, генерации и запуска

Зависимости: AGD_ADM.1 Руководство администратора

13.2.4.1 Элементы действий разработчика

13.2.4.1.1 ADO_IGS.1.1D

Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

13.2.4.2 Элементы содержания и представления свидетельств

13.2.4.2.1 ADO_IGS.1.1C

Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.

13.2.4.3 Элементы действий оценщика

13.2.4.3.1 ADO_IGS.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13.2.4.3.2 ADO_IGS.1.2E

Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

13.2.5 ADO_IGS.2 Журнал регистрации генерации

Зависимости: AGD_ADM.1 Руководство администратора

13.2.5.1 Элементы действий разработчика

13.2.5.1.1 ADO_IGS.2.1D

Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

13.2.5.2 Элементы содержания и представления свидетельств

13.2.5.2.1 ADO_IGS.2.1C

Документация установки, генерации и запуска должна содержать описание последовательности всех действий, необходимых для безопасной установки, генерации и запуска ОО.

13.2.5.2.2 ADO_IGS.2.2C

Документация установки, генерации и запуска должна содержать описание процедур, позволяющих таким образом создать журнал регистрации, содержащий применявшиеся опции генерации ОО, чтобы можно было точно определить, как и когда ОО был сгенерирован.

13.2.5.3 Элементы действий оценщика

13.2.5.3.1 ADO_IGS.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

13.2.5.3.2 ADO_IGS.2.2E

Оценщик должен сделать независимое заключение о том, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

14 Класс ADV. Разработка

Класс ADV «Разработка» содержит четыре семейства требований для представления ФБО на различных уровнях абстракции — от функционального интерфейса до представления реализации. Класс ADV «Разработка» включает в себя также семейство требований для отображения соответствия между различными представлениями ФБО, требуя, в конечном счете, демонстрацию соответствия от наименее абстрактного представления через все промежуточные представления до краткой спецификации ОО, содержащейся в ЗБ. Кроме того, имеется семейство требований для модели ПБО и для отображения соответствия между ПБО, моделью ПБО и функциональной спецификацией. И, наконец, имеется семейство требований к внутренней структуре ФБО, которое распространяется на такие аспекты, как модульность, разбиение на уровни и минимизация сложности.

Уровни декомпозиции представлений ФБО для семейств данного класса могут быть следующими: функциональная спецификация ФБО, декомпозиция ФБО на подсистемы, декомпозиция подсистем на модули, показ реализации модулей и демонстрация соответствия между всеми декомпозициями, которые предоставляются как свидетельства. Требования для различных представлений ФБО выделены в разные семейства, чтобы позволить разработчику ПЗ/ЗБ определить, какое именно подмножество представлений ФБО требуется.

Связи между различными представлениями ФБО и требованиями, с которыми они связаны, показаны на рисунке 10. Классы APE и ASE определяют требования соответствия между функциональными требованиями и целями безопасности, а также между целями безопасности и ожидаемой средой ОО. Класс ASE также определяет требования к соответствию между целями безопасности, функциональными требованиями и краткой спецификацией ОО.

Требования для всех других соответствий, показанных на рисунке 10, определены в классе ADV «Разработка». Семейство ADV_SPM «Моделирование политики безопасности» определяет требования соответствия между ПБО и моделью ПБО, а также между моделью ПБО и функциональной спецификацией. Семейство ADV_RCR «Соответствие представлений» определяет требования соответствия между всеми имеющимися представлениями ФБО — от краткой спецификации ОО до представления реализации. Наконец, каждое семейство доверия, относящееся к конкретному представлению ФБО (то есть ADV_FSP «Функциональная спецификация», ADV_HLD «Проект верхнего уровня», ADV_LLD «Проект нижнего уровня» и ADV_IMP «Представление реализации»), определяет требования, устанавливающие связь между представлением ФБО и функциональными требованиями, сочетание которых помогает убедиться в том, что функциональные требования безопасности ОО были учтены. Анализ прослеживания будет выполняться всегда, начиная с самого высокого уровня представления ФБО, включая каждое из имеющихся представлений ФБО. ИСО/МЭК 15408 реализует это требование прослеживания, используя зависимости от семейства ADV_RCR «Соответствие представлений». Семейство ADV_INT «Внутренняя структура ФБО» на рисунке 10 не представлено, поскольку оно связано с внутренней структурой ФБО и имеет лишь косвенное отношение к процессу уточнения представлений ФБО.

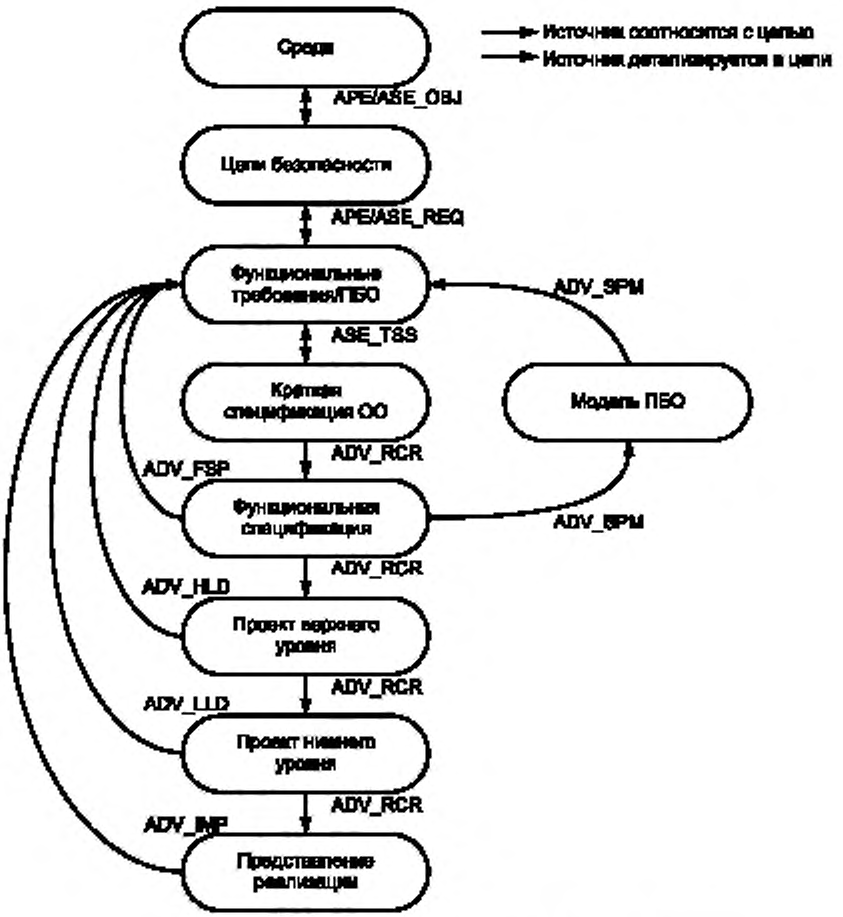


Рисунок 10 — Связи между представлениями ОО и требованиями

Политика безопасности ОО (ПБО) — совокупность правил, регулирующих управление ресурсами, их защиту и распределение в пределах ОО и выражаемых посредством функциональных требований безопасности ОО. От разработчика в явном виде не требуется представление ПБО, поскольку ПБО выражается посредством функциональных требований безопасности ОО, через сочетание политик функций безопасности (ПФБ) и других отдельных элементов требований.

Функции безопасности ОО (ФБО) — совокупность всех функциональных возможностей различных частей ОО, направленных на осуществление ПБО. ФБО включают в себя как функции, которые непосредственно осуществляют ПБО, так и функции, которые, не реализуя ПБО непосредственно, косвенно содействуют осуществлению ПБО.

Хотя требования семейства ASE_TSS «Краткая спецификация ОО» и некоторых других семейств класса ASE предусматривают несколько различных представлений ФБО, совсем необязателен отдельный документ для каждого представления ФБО. Действительно, возможен случай, когда один документ выполняет требования по документированию нескольких представлений ФБО, а объединение в нем требуемой информации по каждому из этих представлений ФБО предпочтительнее, несмотря на усложнение структуры данного документа. В случае, если несколько представлений ФБО объединены в одном документе, разработчику следует указать конкретно, в каких документах какие представления содержатся.

Данным классом узаконены три типа стиля изложения спецификаций: неформальный, полуформальный и формальный. Функциональная спецификация, проект верхнего уровня, проект нижнего уровня и модель ПБО будут изложены с применением одного или нескольких из этих стилей спецификации. Неоднозначность в этих спецификациях уменьшается с повышением уровня формализации стиля изложения.

Неформальную спецификацию излагают как текст на естественном языке. Под «естественным языком» здесь подразумевается применение выразительных средств общения любого разговорного языка (например, английского, немецкого, русского, французского). Неформальная спецификация не подчинена никаким нотационным или специальным ограничениям, отличным от общепринятых соглашений для этого языка (таких, как грамматика и синтаксис). Хотя нотационные ограничения в неформальной спецификации не применяют, все же требуется привести определения значений терминов, использование которых в контексте отличается от общепринятого.

Полуформальную спецификацию излагают на языке с ограниченным синтаксисом и обычно сопровождают вспомогательным пояснительным (неформальным) текстом. Язык с ограниченным синтаксисом может быть естественным языком с ограниченной структурой предложения и ключевыми словами со специальными значениями или языком схем (таких как схемы потоков данных, переходов, взаимосвязей сущностей, структур данных и процессов или структур программ). В обоих случаях обязателен набор соглашений, позволяющих определить ограничения, накладываемые на синтаксис.

Формальную спецификацию излагают с использованием нотации, основанной на известных математических понятиях, и обычно сопровождают вспомогательным пояснительным (неформальным) текстом. Эти математические понятия используют для того, чтобы определить синтаксис и семантику нотации и правила доказательства, поддерживающие логическую аргументацию. Необходимо, чтобы синтаксические и семантические правила, регламентирующие формальную нотацию, определяли, как однозначно распознавать конструкции и определять их значение. Требуется свидетельство невозможности вывода противоречий, а правила, регламентирующие нотацию, необходимо определить или привести ссылку на них.

Существенное доверие может быть достигнуто обеспечением прослеживания ФБО до каждого из представлений и соответствия модели ПБО функциональной спецификации. Семейство ADV_RCR «Соответствие представлений» содержит требования к отображению соответствия между различными представлениями ФБО, а семейство ADV_SPM «Моделирование политики безопасности» — между моделью ПБО и функциональной спецификацией. Соответствие может принять форму неформальной или полуформальной демонстрации либо формального доказательства.

Когда требуется неформальная демонстрация соответствия, это означает, что требуется только соответствие по сути. Методы демонстрации включают в себя, например использование двумерной таблицы с входами, обозначающими соответствие, или подходящей для этого нотации схем проекта. Могут быть также использованы указатели и ссылки на другие документы.

Полуформальная демонстрация соответствия требует структурного подхода при анализе соответствия. Необходимо, чтобы при этом подходе уменьшалась неоднозначность, которая может существовать при неформальном соответствии, ограничивая интерпретацию применяемых терминов. Могут быть также использованы указатели и ссылки на другие документы.

Формальное доказательство соответствия требует, чтобы были использованы известные математические понятия для определения синтаксиса и семантики формальной нотации и правил доказательства, которые поддерживают логическую аргументацию. Необходимо, чтобы свойства безопасности могли быть выражены на языке формальной спецификации, и было показано, что эти свойства удовлетворяются формальной спецификацией. Могут быть также использованы указатели и ссылки на другие документы.

Элементы ADV_RCR.*.1C содержат требование, чтобы разработчик представил свидетельство для каждой смежной пары представлений ФБО, что все относящиеся к безопасности функциональные возможности более абстрактного представления ФБО уточнены в менее абстрактном представлении ФБО. Каждый из элементов ADV_FSP.*.2E, ADV_HLD.*.2E, ADV_LLD.*.2E и ADV_IMP.*.2E содержит требование, чтобы оценщик сделал заключение о том, что ФБО, представляемые этим семейством требований, — точное и полное отображение функциональных требований безопасности ОО. Предполагается, что оценщик использует свидетельство, предоставленное разработчиком в соответствии с ADV_RCR.*.1C, как основание для такого заключения. Устанавливая соответствие между функциональными требованиями безопасности ОО и каждым из цепочки последовательных представлений ФБО, этот пошаговый процесс предоставит, в конечном счете, более высокое доверие соответствию наименее абстрактного представления ФБО функциональным требованиям безопасности ОО, что и является конечной целью данного класса.

Если оценщик не устанавливает соответствие функциональным требованиям безопасности ОО для промежуточных представлений ФБО, то попытка сделать заключение о соответствии наименее абстрактного представления ФБО функциональным требованиям безопасности ОО может представлять собой слишком большой шаг для точного его выполнения. И, наконец, в зависимости от требуемой совокупности представлений ФБО, вполне возможно, что проект нижнего уровня, проект верхнего уровня или даже функциональная спецификация могут являться наименее абстрактным имеющимся представлением ФБО.

Декомпозиция класса ADV «Разработка» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 11.

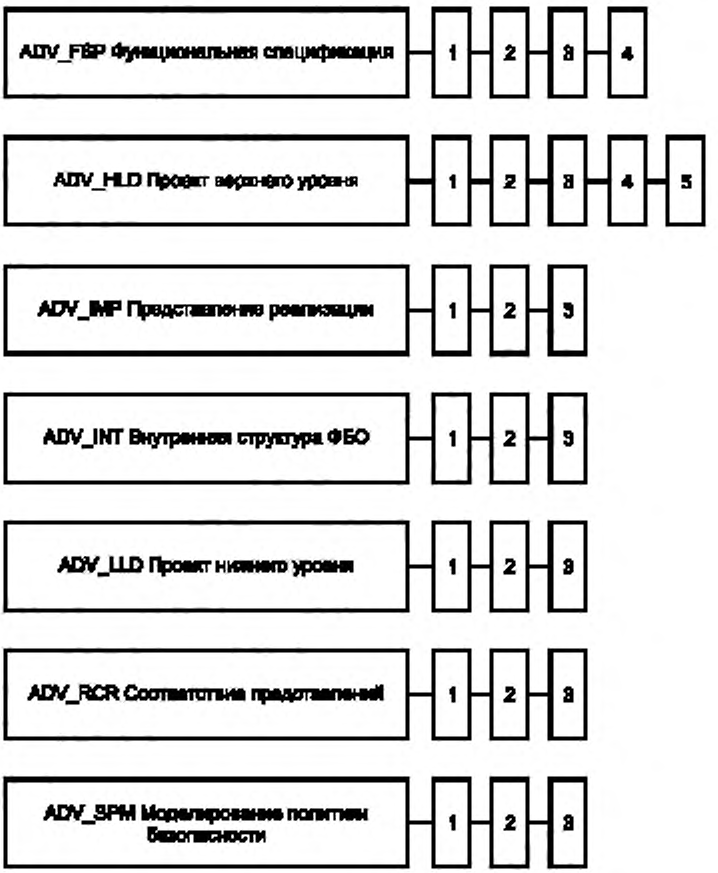


Рисунок 11 — Декомпозиция класса «Разработка»

14.1 Функциональная спецификация (ADV_FSP)

14.1.1 Цели

Функциональная спецификация — это описание на верхнем уровне видимого пользователем интерфейса и режима выполнения ФБО. Она представляет собой отображение функциональных требований безопасности ОО. Функциональная спецификация должна показать, что все функциональные требования безопасности ОО учтены.

14.1.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе степени формализации, требуемой для функциональной спецификации, и степени детализации, предусмотренной для внешних интерфейсов ФБО.

14.1.3 Замечания по применению

Элементы ADV_FSP.*.2E этого семейства определяют требование, чтобы оценщик сделал заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО. Этим заключением обеспечивается прямое соответствие между функциональными требованиями безопасности ОО и функциональной спецификацией в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, включенное в ADV_RCR «Соответствие представлений», как основание для данного заключения, а требование полноты предполагает соотнесение с уровнем абстракции функциональной спецификации.

Для ADV_FSP.1.3C предполагается, что в функциональной спецификации предоставляется информация, достаточная для понимания того, как были учтены функциональные требования безопасности ОО, и дается возможность спецификации тестов, которые отражают функциональные требования безопасности ОО в ЗБ. Необязательно, чтобы такое тестирование охватывало все возможные возвращаемые значения и сообщения об ошибках, которые могут быть сформированы интерфейсом, но следует, чтобы приведенная информация сделала ясными результаты использования интерфейса в случае нормального завершения и наиболее общих примеров отказа.

ADV_FSP.2.3C содержит требование полного представления функционального интерфейса. Этим требованием будет обеспечена необходимая детализация для поддержки как полного тестирования ОО, так и оценки уязвимостей.

Применительно к уровню формализации функциональной спецификации неформальная, полуформальная и формальная спецификации рассматриваются как иерархичные по сути. Так, элементы требований ADV_FSP.1.1C и ADV_FSP.2.1C могут быть удовлетворены использованием полуформальной или формальной функциональной спецификации, поддержанной, где это необходимо, неформальным пояснительным текстом. Аналогично, ADV_FSP.3.1C может быть удовлетворен использованием формальной функциональной спецификации.

14.1.4 ADV_FSP.1 Неформальная функциональная спецификация

Зависимости: ADV_RCR.1 Неформальная демонстрация соответствия

14.1.4.1 Элементы действий разработчика

14.1.4.1.1 ADV_FSP.1.1D

Разработчик должен представить функциональную спецификацию.

14.1.4.2 Элементы содержания и представления свидетельств

14.1.4.2.1 ADV_FSP.1.1C

Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

14.1.4.2.2 ADV_FSP.1.2C

Функциональная спецификация должна быть внутренне непротиворечивой.

14.1.4.2.3 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.

14.1.4.2.4 ADV_FSP.1.4C

Функциональная спецификация должна полностью представить ФБО.

14.1.4.3 Элементы действий оценщика

14.1.4.3.1 ADV_FSP.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.1.4.3.2 ADV_FSP.1.2E

Оценщик должен сделать независимое заключение о том, что функциональная спецификация — точное и полное отображение функциональных требований безопасности ОО.

14.1.5 ADV_FSP.2 Полностью определенные внешние интерфейсы

Зависимости: ADV_RCR.1 Неформальная демонстрация соответствия

14.1.5.1 Элементы действий разработчика

14.1.5.1.1 ADV_FSP.2.1D

Разработчик должен представить функциональную спецификацию.

14.1.5.2 Элементы содержания и представления свидетельств

14.1.5.2.1 ADV_FSP.2.1C

Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

14.1.5.2.2 ADV_FSP.2.2C

Функциональная спецификация должна быть внутренне непротиворечивой.

14.1.5.2.3 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.

14.1.5.2.4 ADV_FSP.2.4C

Функциональная спецификация должна полностью представить ФБО.

14.1.5.2.5 ADV_FSP.2.5C

Функциональная спецификация должна включать в себя обоснование того, что ФБО полностью представлены.

14.1.5.3 Элементы действий оценщика

14.1.5.3.1 ADV_FSP.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.1.5.3.2 ADV_FSP.2.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация — точное и полное отображение функциональных требований безопасности ОО.

14.1.6 ADV_FSP.3 Полуформальная функциональная спецификация

Зависимости: ADV_RCR.1 Неформальная демонстрация соответствия

14.1.6.1 Элементы действий разработчика

14.1.6.1.1 ADV_FSP.3.1D

Разработчик должен представить функциональную спецификацию.

14.1.6.2 Элементы содержания и представления свидетельств

14.1.6.2.1 ADV_FSP.3.1C

Функциональная спецификация должна содержать **полуформальное** описание ФБО и их внешних интерфейсов, **поддержанное, где это необходимо, неформальным пояснительным текстом.**

14.1.6.2.2 ADV_FSP.3.2C

Функциональная спецификация должна быть внутренне непротиворечивой.

14.1.6.2.3 ADV_FSP.3.3C

Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

14.1.6.2.4 ADV_FSP.3.4C

Функциональная спецификация должна полностью представить ФБО.

14.1.6.2.5 ADV_FSP.3.5C

Функциональная спецификация должна включать в себя обоснование, что ФБО полностью представлены.

14.1.6.3 Элементы действий оценщика

14.1.6.3.1 ADV_FSP.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.1.6.3.2 ADV_FSP.3.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация — точное и полное отображение функциональных требований безопасности ОО.

14.1.7 ADV_FSP.4 Формальная функциональная спецификация

Зависимости: ADV_RCR.1 Неформальная демонстрация соответствия

14.1.7.1 Элементы действий разработчика

14.1.7.1.1 ADV_FSP.4.1D

Разработчик должен представить функциональную спецификацию.

14.1.7.2 Элементы содержания и представления свидетельств

14.1.7.2.1 ADV_FSP.4.1C

Функциональная спецификация должна содержать **формальное** описание ФБО и их внешних интерфейсов, поддержанное, где это необходимо, неформальным пояснительным текстом.

14.1.7.2.2 ADV_FSP.4.2C

Функциональная спецификация должна быть внутренне непротиворечивой.

14.1.7.2.3 ADV_FSP.4.3C

Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

14.1.7.2.4 ADV_FSP.4.4C

Функциональная спецификация должна полностью представить ФБО.

14.1.7.2.5 ADV_FSP.4.5C

Функциональная спецификация должна включать в себя обоснование того, что ФБО полностью представлены.

14.1.7.3 Элементы действий оценщика

14.1.7.3.1 ADV_FSP.4.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.1.7.3.2 ADV_FSP.4.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация — точное и полное отображение функциональных требований безопасности ОО.

14.2 Проект верхнего уровня (ADV_HLD)

14.2.1 Цели

Проект верхнего уровня ОО представляет описание ФБО в терминах основных структурных частей (то есть подсистем) и связывает эти части с функциями, которые они выполняют. Требования к проекту верхнего уровня предназначены для обеспечения доверия к тому, что ОО имеет архитектуру, приемлемую для реализации функциональных требований безопасности ОО.

Проект верхнего уровня уточняет функциональную спецификацию, преобразуя ее в подсистемы. Для каждой подсистемы ФБО проект верхнего уровня описывает ее назначение, а также идентифицирует функции безопасности, включаемые в подсистему. В проекте верхнего уровня также определяются взаимосвязи всех подсистем. Эти взаимосвязи будут представлены как внешние интерфейсы по данным, управлению и т.д.

14.2.2 Ранжирование компонентов

Компоненты в данном семействе ранжированы на основе степени формализации, требуемой для проекта верхнего уровня, и на степени детализации, требуемой для спецификаций интерфейса.

14.2.3 Замечания по применению

Ожидается, что разработчик опишет проект ФБО в терминах подсистем. Термин «подсистема» используют здесь для выражения идеи декомпозиции ФБО на относительно небольшое число частей. Даже если разработчику не требуется иметь «подсистемы», ожидается, что он представит подобный уровень декомпозиции. Например, проект может быть декомпозирован путем использования «уровней», «доменов» или «серверов».

Выражение «функциональные возможности безопасности» используют, чтобы представить совокупность выполняемых подсистемой действий, которые участвуют в осуществлении функций безопасности, реализуемых ОО. Это разграничение сделано потому, что составные части проекта, такие как подсистемы или модули, не обязательно однозначно отождествляются с конкретными функциями безопасности. В то время как данная подсистема может прямо соответствовать как одной, так и нескольким функциям безопасности, возможно также, что несколько подсистем необходимо объединить для реализации единственной функции безопасности.

Выражение «подсистема, осуществляющая ПБО» относится к подсистеме, которая прямо или косвенно содействует осуществлению ПБО.

Элементы ADV_HLD.*.2E данного семейства определяют требование вынесения оценщиком заключения о том, что проект верхнего уровня является точным и полным отображением функциональных требований безопасности ОО. Это обеспечивает прямое соответствие между функциональными требованиями безопасности ОО и проектом верхнего уровня в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, включенное в ADV_RCR «Соответствие представлений», как основание для этого заключения, а требование полноты предполагает соотнесение с уровнем абстракции проекта верхнего уровня.

ADV_HLD.3.8C содержит требование полного представления интерфейсов подсистем. Этим будет обеспечена необходимая детализация для поддержки как полного тестирования ОО (с использованием компонентов из ATE_DPT«Глубина»), так и оценки уязвимостей.

Применительно к уровню формализации проекта верхнего уровня неформальный, полуформальный и формальный проекты рассматривают как иерархичные по сути. Так, элементы требований ADV_HLD.1.1C и ADV_HLD.2.1C могут быть удовлетворены использованием полуформального или формального проекта верхнего уровня, а элементы требований ADV_HLD.3.1C и ADV_HLD.4.1C — использованием формального проекта верхнего уровня.

В ADV_HLD.*.5C выражение «базовые аппаратные, программно-аппаратные и/или программные средства» относится к виртуальной машине, на базе которой работает ОО (если таковая имеется), а не к механизмам самого ОО (к которым относятся другие части компонента). Как таковые требования ADV_HLD.*.5C являются требованиями к информации о среде ИТ.

14.2.4 ADV_HLD.1 Описательный проект верхнего уровня

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_RCR.1 Неформальная демонстрация соответствия

14.2.4.1 Элементы действий разработчика

14.2.4.1.1 ADV_HLD.1.1D

Разработчик должен представить проект верхнего уровня ФБО.

14.2.4.2 Элементы содержания и представления свидетельств

14.2.4.2.1 ADV_HLD.1.1C

Представление проекта верхнего уровня должно быть неформальным.

14.2.4.2.2 ADV_HLD.1.2C

Проект верхнего уровня должен быть внутренне непротиворечивым.

14.2.4.2.3 ADV_HLD.1.3C

Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

14.2.4.2.4 ADV_HLD.1.4C

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

14.2.4.2.5 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.

14.2.4.2.6 ADV_HLD.1.6C

Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

14.2.4.2.7 ADV_HLD.1.7C

Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

14.2.4.3 Элементы действий оценщика

14.2.4.3.1 ADV_HLD.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.2.4.3.1 ADV_HLD.1.2E

Оценщик должен сделать независимое заключение о том, что проект верхнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.2.5 ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_RCR.1 Неформальная демонстрация соответствия

14.2.5.1 Элементы действий разработчика

14.2.5.1.1 ADV_HLD.2.1D

Разработчик должен представить проект верхнего уровня ФБО.

14.2.5.2 Элементы содержания и представления свидетельств

14.2.5.2.1 ADV_HLD.2.1C

Представление проекта верхнего уровня должно быть неформальным.

14.2.5.2.2 ADV_HLD.2.2C

Проект верхнего уровня должен быть внутренне непротиворечивым.

14.2.5.2.3 ADV_HLD.2.3C

Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

14.2.5.2.4 ADV_HLD.2.4C

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

14.2.5.2.5 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.

14.2.5.2.6 ADV_HLD.2.6C

Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

14.2.5.2.7 ADV_HLD.2.7C

Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

14.2.5.2.8 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.

14.2.5.2.9 ADV_HLD.2.9C

Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

14.2.5.3 Элементы действий оценщика

14.2.5.3.1 ADV_HLD.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.2.5.3.2 ADV_HLD.2.2E

Оценщик должен сделать независимое заключение, что проект верхнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.2.6 ADV_HLD.3 Полуформальный проект верхнего уровня

Зависимости: ADV_FSP.3 Полуформальная функциональная спецификация
ADV_RCR.2 Полуформальная демонстрация соответствия

14.2.6.1 Элементы действий разработчика

14.2.6.1.1 ADV_HLD.3.1D

Разработчик должен представить проект верхнего уровня ФБО.

14.2.6.2 Элементы содержания и представления свидетельств

14.2.6.2.1 ADV_HLD.3.1C

Представление проекта верхнего уровня должно быть **полуформальным**.

14.2.6.2.2 ADV_HLD.3.2C

Проект верхнего уровня должен быть внутренне непротиворечивым.

14.2.6.2.3 ADV_HLD.3.3C

Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

14.2.6.2.4 ADV_HLD.3.4C

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

14.2.6.2.5 ADV_HLD.3.5C

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.

14.2.6.2.6 ADV_HLD.3.6C

Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

14.2.6.2.7 ADV_HLD.3.7C

Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

14.2.6.2.8 ADV_HLD.3.8C

Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

14.2.6.2.9 ADV_HLD.3.9C

Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

14.2.6.3 Элементы действий оценщика

14.2.6.3.1 ADV_HLD.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.2.6.3.2 ADV_HLD.3.2E

Оценщик должен сделать независимое заключение о том, что проект верхнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.2.7 ADV_HLD.4 Пояснения в полуформальном проекте верхнего уровня

Зависимости: ADV_FSP.3 Полуформальная функциональная спецификация
ADV_RCR.2 Полуформальная демонстрация соответствия

14.2.7.1 Элементы действий разработчика

14.2.7.1.1 ADV_HLD.4.1D

Разработчик должен представить проект верхнего уровня ФБО.

14.2.7.2 Элементы содержания и представления свидетельств

14.2.7.2.1 ADV_HLD.4.1C

Представление проекта верхнего уровня должно быть полуформальным.

14.2.7.2.2 ADV_HLD.4.2C

Проект верхнего уровня должен быть внутренне непротиворечивым.

14.2.7.2.3 ADV_HLD.4.3C

Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

14.2.7.2.4 ADV_HLD.4.4C

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

14.2.7.2.5 ADV_HLD.4.5C

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.

14.2.7.2.6 ADV_HLD.4.6C

Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

14.2.7.2.7 ADV_HLD.4.7C

Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

14.2.7.2.8 ADV_HLD.4.8C

Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

14.2.7.2.9 ADV_HLD.4.9C

Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

14.2.7.2.10 ADV_HLD.4.10C

Проект верхнего уровня должен содержать логическое обоснование того, что идентифицированный способ выполнения разделения, в том числе любых механизмов защиты, достаточен для обеспечения четкого и эффективного отделения функций, осуществляющих ПБО, от функций, не участвующих в осуществлении ПБО.

14.2.7.2.11 ADV_HLD.4.11C

Проект верхнего уровня должен содержать логическое обоснование того, что механизмы ФБО достаточны для реализации функций безопасности, идентифицированных в проекте верхнего уровня.

14.2.7.3 Элементы действий оценщика

14.2.7.3.1 ADV_HLD.4.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.2.7.3.2 ADV_HLD.4.2E

Оценщик должен сделать независимое заключение о том, что проект верхнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.2.8 ADV_HLD.5 Формальный проект верхнего уровня

Зависимости: ADV_FSP.4 Формальная функциональная спецификация
ADV_RCR.3 Формальная демонстрация соответствия

14.2.8.1 Элементы действий разработчика

14.2.8.1.1 ADV_HLD.5.1D

Разработчик должен представить проект верхнего уровня ФБО.

14.2.8.2 Элементы содержания и представления свидетельств

14.2.8.2.1 ADV_HLD.5.1C

Представление проекта верхнего уровня должно быть **формальным**.

14.2.8.2.2 ADV_HLD.5.2C

Проект верхнего уровня должен быть внутренне непротиворечивым.

14.2.8.2.3 ADV_HLD.5.3C

Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

14.2.8.2.4 ADV_HLD.5.4C

Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

14.2.8.2.5 ADV_HLD.5.5C

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.

14.2.8.2.6 ADV_HLD.5.6C

Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

14.2.8.2.7 ADV_HLD.5.7C

Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

14.2.8.2.8 ADV_HLD.5.8C

Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

14.2.8.2.9 ADV_HLD.5.9C

Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

14.2.8.2.10 ADV_HLD.5.10C

Проект верхнего уровня должен содержать логическое обоснование того, что идентифицированный способ выполнения разделения, в том числе любых механизмов защиты, достаточен для обеспечения четкого и эффективного отделения функций, осуществляющих ПБО, от функций, не участвующих в осуществлении ПБО.

14.2.8.2.11 ADV_HLD.5.11C

Проект верхнего уровня должен содержать логическое обоснование того, что механизмы ФБО достаточны для реализации функций безопасности, идентифицированных в проекте верхнего уровня.

14.2.8.3 Элементы действий оценщика

14.2.8.3.1 ADV_HLD.5.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.2.8.3.2 ADV_HLD.5.2E

Оценщик должен сделать независимое заключение о том, что проект верхнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.3 Представление реализации (ADV_IMP)

14.3.1 Цели

Описание представления реализации в форме исходного текста программ, микропрограмм, схем аппаратных средств и т. д. фиксирует детализацию выполнения ФБО для поддержки анализа.

14.3.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе полноты и структуры приведенного представления реализации.

14.3.3 Замечания по применению

Представление реализации применяют, чтобы выразить наименее абстрактное представление ФБО, используемое для создания собственно реализации ФБО без дальнейшего уточнения проекта. Исходный текст, который затем компилируют, или чертеж аппаратуры, который используют для построения действующего оборудования, — примеры частей представления реализации.

Возможно, оценщики смогут использовать представление реализации для того, чтобы непосредственно поддерживать другие виды действий при оценке (например анализ уязвимостей, анализ полноты тестирования или идентификацию дополнительных тестов оценщика). Ожидается, что авторы ПЗ/ЗБ выберут компонент, требующий достаточно полной и всесторонней реализации, для удовлетворения всех других требований, включенных в ПЗ/ЗБ.

14.3.4 ADV_IMP.1 Подмножество реализации ФБО

Зависимости: ADV_LLD.1 Описательный проект нижнего уровня
ADV_RCR.1 Неформальная демонстрация соответствия
ALC_TAT.1 Полностью определенные инструментальные средства разработки

14.3.4.1 Замечания по применению

ADV_IMP.1.1D содержит требование, чтобы разработчик обеспечил представление реализации для подмножества ФБО. Целью является доступ, по меньшей мере, к части ФБО, обеспечивающей оценщику возможность провести экспертизу представления реализации тех частей ОО, для которых подобная экспертиза может значительно увеличить понимание применяемых механизмов и доверие к ним. Подготовка выборки представления реализации позволит оценщику выборочно проверить свидетельство прослеживания требований безопасности в представлениях проекта ОО с тем, чтобы получить доверие к подходу, принятому для уточнения, и непосредственно оценить предъявленное представление реализации.

Элемент ADV_IMP.1.2E определяет требование вынесения оценщиком независимого заключения о том, что наименее абстрактное представление ФБО является точным и полным отображением функциональных требований безопасности ОО. Этим обеспечивается прямое соответствие между функциональными требованиями безопасности ОО и наименее абстрактным представлением ФБО в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, предоставляемое в ADV_RCR «Соответствие представлений», как основание для заключения об этом. Наименее абстрактное представление ФБО для этого компонента — совокупность имеющегося представления реализации и той части проекта нижнего уровня, для которой не имеется представления реализации.

14.3.4.2 Элементы действий разработчика

14.3.4.2.1 ADV_IMP.1.1D

Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.

14.3.4.3 Элементы содержания и представления свидетельств

14.3.4.3.1 ADV_IMP.1.1C

Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

14.3.4.3.2 ADV_IMP.1.2C

Представление реализации должно быть внутренне непротиворечивым.

14.3.4.4 Элементы действий оценщика

14.3.4.4.1 ADV_IMP.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.3.4.4.2 ADV_IMP.1.2E

Оценщик должен сделать независимое заключение о том, что наименее абстрактное представление ФБО — точное и полное отображение функциональных требований безопасности ОО.

14.3.5 ADV_IMP.2 Реализация ФБО

Зависимости: ADV_LLD.1 Описательный проект нижнего уровня
ADV_RCR.1 Неформальная демонстрация соответствия
ALC_TAT.1 Полностью определенные инструментальные средства разработки

14.3.5.1 Замечания по применению

Элемент ADV_IMP.2.2E определяет требование вынесения оценщиком независимого заключения о том, что представление ФБО является точным и полным отображением функциональных требований безопасности ОО. Этим обеспечивается прямое соответствие между функциональными требованиями безопасности ОО и представлением реализации в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, предоставляемое в ADV_RCR «Соответствие представлений», как основание при вынесении этого заключения.

14.3.5.2 Элементы действий разработчика

14.3.5.2.1 ADV_IMP.2.1D

Разработчик должен обеспечить представление реализации для всех ФБО.

14.3.5.3 Элементы содержания и представления свидетельств

14.3.5.3.1 ADV_IMP.2.1C

Представление реализации должно однозначно определить ФБО на таком уровне детализации, чтобы ФБО могли быть созданы без дальнейших проектных решений.

14.3.5.3.2 ADV_IMP.2.2C

Представление реализации должно быть внутренне непротиворечивым.

14.3.5.3.3 ADV_IMP.2.3C

Представление реализации должно включать в себя описание взаимосвязей между всеми частями реализации.

14.3.5.4 Элементы действий оценщика

14.3.5.4.1 ADV_IMP.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.3.5.4.2 ADV_IMP.2.2E

Оценщик должен сделать независимое заключение о том, что **представление реализации** — точное и полное отображение функциональных требований безопасности ОО.

14.3.6 ADV_IMP.3Структурированная реализация ФБО

Зависимости: ADV_INT.1 Модульность
ADV_LLD.1 Описательный проект нижнего уровня
ADV_RCR.1 Неформальная демонстрация соответствия
ALC_TAT.1 Полностью определенные инструментальные средства разработки

14.3.6.1 Замечания по применению

Элемент ADV_IMP.3.2E определяет требование вынесения оценщиком независимого заключения о том, что представление ФБО является точным и полным отображением функциональных требований безопасности ОО. Этим обеспечивается прямое соответствие между функциональными требованиями безопасности ОО и представлением реализации в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, предоставляемое в ADV_RCR «Соответствие представлений», как основание при вынесении этого заключения.

14.3.6.2 Элементы действий разработчика

14.3.6.2.1 ADV_IMP.3.1D

Разработчик должен обеспечить представление реализации для всех ФБО.

14.3.6.3 Элементы содержания и представления свидетельств

14.3.6.3.1 ADV_IMP.3.1C

Представление реализации должно однозначно определить ФБО на таком уровне детализации, чтобы ФБО могли быть созданы без дальнейших проектных решений.

14.3.6.3.2 ADV_IMP.3.2C

Представление реализации должно быть внутренне непротиворечивым.

14.3.6.3.3 ADV_IMP.3.3C

Представление реализации должно включать в себя описание взаимосвязей между всеми частями реализации.

14.3.6.3.4 ADV_IMP.3.4C

Представление реализации должно быть структурировано в малые и понятные разделы.

14.3.6.4 Элементы действий оценщика

14.3.6.4.1 ADV_IMP.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.3.6.4.2 ADV_IMP.3.2E

Оценщик должен сделать независимое заключение о том, что представление реализации — точное и полное отображение функциональных требований безопасности ОО.

14.4 Внутренняя структура ФБО (ADV_INT)

14.4.1 Цели

Данное семейство связано с внутренней структурой ФБО. Установлены требования для модульности, разбиения на уровни (с тем, чтобы разделить уровни абстракции и минимизировать циклические зависимости), минимизации как сложности механизмов осуществления политик, так и функциональных возможностей ФБО, не участвующих в осуществлении ПБО, для получения ФБО, которые являются достаточно простыми для анализа.

Модульное проектирование уменьшает взаимозависимость между элементами ФБО и, таким образом, уменьшает риск того, что изменение или ошибка в одном модуле повлияет на весь ОО. Таким образом, модульное проектирование предоставляет основу для определения области взаимодействия с другими элементами ФБО, обеспечивает повышение доверия к отсутствию непредвиденных последствий, а также предоставляет основу для проектирования и оценки комплектов тестов.

Использование разбиения на уровни и простой конструкции для функциональных возможностей, осуществляющих ПБО, уменьшает сложность ФБО. Это, в свою очередь, способствует лучшему пониманию ФБО, предоставляя большее доверие, что функциональные требования безопасности ОО точно и полностью отражены в реализации.

Минимизация тех функциональных возможностей в ФБО, которые не участвуют в осуществлении ПБО, уменьшает возможность появления дефектов в ФБО. В сочетании с модульностью и разбиением на уровни, минимизация позволяет оценщику сосредоточиться только на тех функциональных возможностях, которые действительно необходимы для осуществления ПБО.

Минимизация сложности проекта содействует повышению доверия к тому, что код понятен: чем меньше сложность кода ФБО, тем больше вероятность, что проект ФБО постижим. Минимизация сложности проекта является ключевой характеристикой механизма проверки правомочности обращений.

14.4.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе требуемых структурированности и минимизации.

14.4.3 Замечания по применению

Выражение «части ФБО» использовано для представления частей ФБО различной степени детализации, основанной на доступных представлениях ФБО. Функциональная спецификация допускает идентификацию в терминах интерфейсов, проект верхнего уровня — в терминах подсистем, проект нижнего уровня — в терминах модулей и представление реализации — в терминах блоков реализации.

Элементы ADV_INT.2.5C и ADV_INT.3.5C связаны с минимизацией взаимодействий между уровнями иерархии. Взаимодействие между уровнями допустимо, но при этом от разработчика требуется показать, что эти взаимодействия необходимы и их невозможно избежать.

ADV_INT.2.6C относится к концепции монитора обращений, требуя минимизации сложности тех частей ФБО, которые осуществляют политики управления доступом и/или управления информационными потоками, идентифицированные в ПБО. ADV_INT.3.6C развивает далее концепцию монитора обращений, требуя минимизации сложности всех ФБО.

Некоторые элементы в компонентах этого семейства ссылаются на описание архитектуры. Описание архитектуры выполняется на том же уровне абстракции, что и проект нижнего уровня в отношении модулей ФБО. Принимая во внимание, что проект нижнего уровня описывает модульную конструкцию ФБО, назначение описания архитектуры — предоставить при необходимости свидетельство модульности, разбиения на уровни и минимизации сложности ФБО. Требуется согласованность как проекта нижнего уровня, так и представления реализации с описанием архитектуры для обеспечения доверия к тому, что эти представления ФБО обладают требуемой модульностью, разбиением на уровни и минимизацией сложности.

14.4.4 ADV_INT.1 Модульность

Зависимости: ADV_IMP.1 Подмножество реализации ФБО
ADV_LLD.1 Описательный проект нижнего уровня

14.4.4.1 Элементы действий разработчика

14.4.4.1.1 ADV_INT.1.1D

Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.

14.4.4.1.2 ADV_INT.1.2D

Разработчик должен представить описание архитектуры.

14.4.4.2 Элементы содержания и представления свидетельств

14.4.4.2.1 ADV_INT.1.1C

Описание архитектуры должно идентифицировать модули ФБО.

14.4.4.2.2 ADV_INT.1.2C

Описание архитектуры должно содержать изложение назначения, интерфейсов, параметров и результатов применения каждого модуля ФБО.

14.4.4.2.3 ADV_INT.1.3C

Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.

14.4.4.3 Элементы действий оценщика

14.4.4.3.1 ADV_INT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.4.4.3.2 ADV_INT.1.2E

Оценщик должен сделать независимое заключение о том, что и проект нижнего уровня, и представление реализации согласуются с описанием архитектуры.

14.4.5 ADV_INT.2 Уменьшение сложности

Зависимости: ADV_IMP.1 Подмножество реализации ФБО
ADV_LLD.1 Описательный проект нижнего уровня

14.4.5.1 Замечания по применению

Данный компонент обращается к концепции монитора обращений, требуя минимизации сложности тех частей ФБО, которые осуществляют идентифицированные в ПБО политики управления доступом и/или информационными потоками.

14.4.5.2 Элементы действий разработчика

14.4.5.2.1 ADV_INT.2.1D

Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.

14.4.5.2.2 ADV_INT.2.2D

Разработчик должен представить описание архитектуры.

14.4.5.2.3 ADV_INT.2.3D

Разработчик должен проектировать и структурировать ФБО по уровням с минимизацией взаимных связей между уровнями проекта.

14.4.5.2.4 ADV_INT.2.4D

Разработчик должен проектировать и структурировать ФБО способом, минимизирующим сложность тех частей ФБО, которые осуществляют какие-либо политики управления доступом и/или информационными потоками.

14.4.5.3 Элементы содержания и представления свидетельств

14.4.5.3.1 ADV_INT.2.1C

Описание архитектуры должно идентифицировать модули ФБО **и специфицировать, какие части ФБО осуществляют политики управления доступом и/или информационными потоками.**

14.4.5.3.2 ADV_INT.2.2C

Описание архитектуры должно содержать изложение назначения, интерфейсов, параметров и результатов применения каждого модуля ФБО.

14.4.5.3.3 ADV_INT.2.3C

Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.

14.4.5.3.4 ADV_INT.2.4C

Описание архитектуры должно показать ее разбиение на уровни.

14.4.5.3.5 ADV_INT.2.5C

Описание архитектуры должно показать, что взаимные связи были минимизированы, и содержать логическое обоснование оставшихся связей.

14.4.5.3.6 ADV_INT.2.6C

Описание архитектуры должно содержать изложение, каким образом части ФБО, которые осуществляют любые политики управления доступом и/или информационными потоками, структурированы для минимизации сложности.

14.4.5.4 Элементы действий оценщика

14.4.5.4.1 ADV_INT.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.4.5.4.2 ADV_INT.2.2E

Оценщик должен сделать независимое заключение о том, что и проект нижнего уровня, и представление реализации согласуются с описанием архитектуры.

14.4.6 ADV_INT.3 Минимизация сложности

Зависимости: ADV_IMP.2 Реализация ФБО
ADV_LLD.1 Описательный проект нижнего уровня

14.4.6.1 Замечания по применению

Данный компонент содержит требование, чтобы свойство монитора обращений «достаточно простой для анализа» полностью обеспечивалось. Если этот компонент сочетается с функциональными требованиями FPT_RVM.1 и FPT_SEP.3, то концепция монитора обращений будет полностью реализована.

14.4.6.2 Элементы действий разработчика

14.4.6.2.1 ADV_INT.3.1D

Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.

14.4.6.2.2 ADV_INT.3.2D

Разработчик должен представить описание архитектуры.

14.4.6.2.3 ADV_INT.3.3D

Разработчик должен проектировать и структурировать ФБО по уровням с минимизацией взаимных связей между уровнями проекта.

14.4.6.2.4 ADV_INT.3.4D

Разработчик должен проектировать и структурировать ФБО способом, минимизирующим сложность **ФБО в целом**.

14.4.6.2.5 ADV_INT.3.5D

Разработчик должен проектировать и структурировать части ФБО, осуществляющие какие-либо политики управления доступом и/или информационными потоками, так, чтобы они были достаточно простыми для анализа.

14.4.6.2.6 ADV_INT.3.6D

Разработчик должен обеспечить, чтобы функции, цели которых не имеют отношения к безопасности, не включались в модули ФБО.

14.4.6.3 Элементы содержания и представления свидетельств

14.4.6.3.1 ADV_INT.3.1C

Описание архитектуры должно идентифицировать модули ФБО и специфицировать, какие части ФБО осуществляют политики управления доступом и/или управления информационными потоками.

14.4.6.3.2 ADV_INT.3.2C

Описание архитектуры должно содержать изложение назначения, интерфейса, параметров и результатов применения каждого модуля ФБО.

14.4.6.3.3 ADV_INT.3.3C

Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.

14.4.6.3.4 ADV_INT.3.4C

Описание архитектуры должно показать ее разбиение на уровни.

14.4.6.3.5 ADV_INT.3.5C

Описание архитектуры должно показать, что взаимные связи были минимизированы, и содержать логическое обоснование оставшихся связей.

14.4.6.3.6 ADV_INT.3.6C

Описание архитектуры должно содержать изложение, каким образом **все ФБО** структурированы для минимизации сложности.

14.4.6.3.7 ADV_INT.3.7C

Описание архитектуры должно содержать логическое обоснование включения в ФБО каждого модуля, не участвующего в осуществлении ПБО.

14.4.6.4 Элементы действий оценщика

14.4.6.4.1 ADV_INT.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.4.6.4.2 ADV_INT.3.2E

Оценщик должен сделать независимое заключение о том, что и проект нижнего уровня, и представление реализации согласуются с описанием архитектуры.

14.4.6.4.3 ADV_INT.3.3E

Оценщик должен подтвердить, что части ФБО, осуществляющие какие-либо политики управления доступом и/или информационными потоками, достаточно просты для анализа.

14.5 Проект нижнего уровня (ADV_LLD)

14.5.1 Цели

Проект нижнего уровня ОО содержит описание внутреннего содержания ФБО в терминах модулей, их взаимосвязей и зависимостей. Проект нижнего уровня обеспечивает доверие к тому, что подсистемы ФБО были правильно и эффективно уточнены.

Для каждого модуля ФБО проект нижнего уровня описывает назначение, функции, интерфейсы, зависимости и реализацию всех функций, участвующих в осуществлении ПБО.

14.5.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе степени формализации, требуемой для проекта нижнего уровня, и степени детализации, требуемой для спецификаций интерфейсов.

14.5.3 Замечания по применению

Выражение «модуль, осуществляющий ПБО» относится к любому модулю, на который необходимо полагаться для корректного осуществления ПБО.

Выражение «функциональные возможности безопасности» используют, чтобы представить совокупность выполняемых модулем действий, которые участвуют в осуществлении функций безопасности, реализуемых ОО. Данное разграничение сделано потому, что модули не обязательно однозначно отождествляются с конкретными функциями безопасности. В то время как данный модуль может прямо соответствовать как одной, так и нескольким функциям безопасности, возможно также, что несколько модулей необходимо объединить для реализации единственной функции безопасности.

Элементы ADV_LLD.*.6C содержат требование, чтобы проект нижнего уровня содержал описание того, как обеспечивается каждая из функций, осуществляющих ПБО. Смысл этого требования состоит в том, чтобы проект нижнего уровня содержал описание планируемой реализации каждого модуля, исходя из перспективы проекта.

Элементы ADV_LLD.*.2E этого семейства определяют требование вынесения оценщиком независимого заключения о том, что проект нижнего уровня является точным и полным отображением функциональных требований безопасности ОО. Этим обеспечивается прямое соответствие между функциональными требованиями безопасности ОО и проектом нижнего уровня в дополнение к попарным соответствиям, требуемым семейством ADV_RCR «Соответствие представлений». Ожидается, что оценщик использует свидетельство, включенное в ADV_RCR «Соответствие представлений», как основание для этого заключения, а требование полноты предполагает соотнесение с уровнем абстракции проекта нижнего уровня.

ADV_LLD.2.9C содержит требование полного представления интерфейсов модулей. Этим будет обеспечена необходимая детализация для поддержки как полного тестирования ОО (с использованием компонентов из семейства ATE_DPT «Глубина»), так и оценки уязвимостей.

Применительно к уровню формализации проекта нижнего уровня неформальный, полуформальный и формальный проекты рассматривают как иерархичные по сути. Так, элемент ADV_LLD.1.1C может быть удовлетворен использованием полуформального или формального проекта нижнего уровня, а элемент ADV_LLD.2.1C — формального проекта нижнего уровня.

14.5.4 ADV_LLD.1 Описательный проект нижнего уровня

Зависимости: ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_RCR.1 Неформальная демонстрация соответствия

14.5.4.1 Элементы действий разработчика

14.5.4.1.1 ADV_LLD.1.1D

Разработчик должен представить проект нижнего уровня ФБО.

14.5.4.2 Элементы содержания и представления свидетельств

14.5.4.2.1 ADV_LLD.1.1C

Представление проекта нижнего уровня должно быть неформальным.

14.5.4.2.2 ADV_LLD.1.2C

Проект нижнего уровня должен быть внутренне непротиворечивым.

14.5.4.2.3 ADV_LLD.1.3C

Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

14.5.4.2.4 ADV_LLD.1.4C

Проект нижнего уровня должен содержать описание назначения каждого модуля.

14.5.4.2.5 ADV_LLD.1.5C

Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

14.5.4.2.6 ADV_LLD.1.6C

Проект нижнего уровня должен содержать описание того, как предоставляется каждая из функций, осуществляющих ПБО.

14.5.4.2.7 ADV_LLD.1.7C

Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

14.5.4.2.8 ADV_LLD.1.8C

Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

14.5.4.2.9 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.

14.5.4.2.10 ADV_LLD.1.10C

Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

14.5.4.3 Элементы действий оценщика

14.5.4.3.1 ADV_LLD.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.5.4.3.2 ADV_LLD.1.2E

Оценщик должен сделать независимое заключение о том, что проект нижнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.5.5 ADV_LLD.2 Полуформальный проект нижнего уровня

Зависимости: ADV_HLD.3 Полуформальный проект верхнего уровня
ADV_RCR.2 Полуформальная демонстрация соответствия

14.5.5.1 Элементы действий разработчика

14.5.5.1.1 ADV_LLD.2.1D

Разработчик должен представить проект нижнего уровня ФБО.

14.5.5.2 Элементы содержания и представления свидетельств

14.5.5.2.1 ADV_LLD.2.1C

Представление проекта нижнего уровня должно быть **полуформальным**.

14.5.5.2.2 ADV_LLD.2.2C

Проект нижнего уровня должен быть внутренне непротиворечивым.

14.5.5.2.3 ADV_LLD.2.3C

Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

14.5.5.2.4 ADV_LLD.2.4C

Проект нижнего уровня должен содержать описание назначения каждого модуля.

14.5.5.2.5 ADV_LLD.2.5C

Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

14.5.5.2.6 ADV_LLD.2.6C

Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

14.5.5.2.7 ADV_LLD.2.7C

Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

14.5.5.2.8 ADV_LLD.2.8C

Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

14.5.5.2.9 ADV_LLD.2.9C

Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

14.5.5.2.10 ADV_LLD.2.10C

Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

14.5.5.3 Элементы действий оценщика

14.5.5.3.1 ADV_LLD.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.5.5.3.2 ADV_LLD.2.2E

Оценщик должен сделать независимое заключение о том, что проект нижнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.5.6 ADV_LLD.3 Формальный проект нижнего уровня

Зависимости: ADV_HLD.5 Формальный проект верхнего уровня
ADV_RCR.3 Формальная демонстрация соответствия

14.5.6.1 Элементы действий разработчика

14.5.6.1.1 ADV_LLD.3.1D

Разработчик должен представить проект нижнего уровня ФБО.

14.5.6.2 Элементы содержания и представления свидетельств

14.5.6.2.1 ADV_LLD.3.1C

Представление проекта нижнего уровня должно быть **формальным**.

14.5.6.2.2 ADV_LLD.3.2C

Проект нижнего уровня должен быть внутренне непротиворечивым.

14.5.6.2.3 ADV_LLD.3.3C

Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

14.5.6.2.4 ADV_LLD.3.4C

Проект нижнего уровня должен содержать описание назначения каждого модуля.

14.5.6.2.5 ADV_LLD.3.5C

Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

14.5.6.2.6 ADV_LLD.3.6C

Проект нижнего уровня должен содержать описание того, как предоставляется каждая из функций, осуществляющих ПБО.

14.5.6.2.7 ADV_LLD.3.7C

Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

14.5.6.2.8 ADV_LLD.3.8C

Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

14.5.6.2.9 ADV_LLD.3.9C

Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

14.5.6.2.10 ADV_LLD.3.10C

Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

14.5.6.3 Элементы действий оценщика

14.5.6.3.1 ADV_LLD.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.5.6.3.2 ADV_LLD.3.2E

Оценщик должен сделать независимое заключение, что проект нижнего уровня — точное и полное отображение функциональных требований безопасности ОО.

14.6 Соответствие представлений (ADV_RCR)

14.6.1 Цели

Соответствие между различными представлениями ФБО (то есть краткой спецификацией ОО, функциональной спецификацией, проектом верхнего уровня, проектом нижнего уровня, представлением реализации) связано с правильным и полным отображением требований вплоть до наименее абстрактного из имеющихся представлений ФБО. Это заключение достигают пошаговым уточнением и совокупным результатом определения соответствия между всеми смежными абстракциями представления.

14.6.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе требуемого уровня формализации соответствия между различными представлениями ФБО.

14.6.3 Замечания по применению

Необходимо, чтобы разработчик продемонстрировал оценщику, что наиболее детализированное или наименее абстрактное имеющееся представление ФБО есть точное, непротиворечивое и полное отображение функций, выраженных как функциональные требования в 3Б. Этого достигают, показывая соответствие между смежными представлениями на соразмерном уровне строгости.

Семейство ADV_RCR не связано с требованиями соответствия ПБО или модели ПБО. В этом семействе, как показано на рисунке 10, рассмотрено соответствие между различными представлениями ФБО (то есть краткой спецификацией ОО, функциональной спецификацией, проектом верхнего уровня, проектом нижнего уровня и представлением реализации).

Элементы ADV_RCR.*.1C ссылаются на «все функциональные возможности, относящиеся к безопасности» в определении области уточнения для смежной пары представлений ФБО. При переходе от краткой спецификации ОО к функциональной спецификации этот элемент предусматривает только, чтобы функции безопасности ОО из краткой спецификации ОО были уточнены в функциональной спецификации, и не требует, чтобы функциональная спецификация содержала какие-либо подробности относительно мер доверия (которые представлены в краткой спецификации ОО). Когда представление реализации предоставляется только для некоторого подмножества ФБО (как в ADV_IMP.1 «Подмножество реализации ФБО»), требуемые уточнения при переходе от проекта нижнего уровня к представлению реализации ограничены функциональными возможностями безопасности, которые имеются в представлении реализации. Во всех остальных случаях этот элемент предусматривает, чтобы все части более абстрактного представления ФБО были уточнены в менее абстрактном представлении ФБО.

Применительно к уровню формализации соответствия между смежными представлениями ФБО неформальный, полуформальный и формальный уровни рассматривают как иерархичные по сути. Так, ADV_RCR.2.2C и ADV_RCR.3.2C могут быть удовлетворены формальным доказательством соответствия, а при отсутствии каких-либо требований к уровню формализации демонстрация соответствия может быть неформальной, полуформальной или формальной.

14.6.4 ADV_RCR.1 Неформальная демонстрация соответствия

Зависимости: нет зависимостей.

14.6.4.1 Элементы действий разработчика

14.6.4.1.1 ADV_RCR.1.1D

Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

14.6.4.2 Элементы содержания и представления свидетельств

14.6.4.2.1 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.

14.6.4.3 Элементы действий оценщика

14.6.4.3.1 ADV_RCR.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.6.5 ADV_RCR.2 Полуформальная демонстрация соответствия

Зависимости: нет зависимостей.

14.6.5.1 Элементы действий разработчика

14.6.5.1.1 ADV_RCR.2.1D

Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

14.6.5.2 Элементы содержания и представления свидетельств

14.6.5.2.1 ADV_RCR.2.1C

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.

14.6.5.2.2 ADV_RCR.2.2C

Для каждой смежной пары имеющихся представлений ФБО, где части обоих представлений специфицированы, по меньшей мере, полуформально, демонстрация соответствия между этими частями представлений должна быть полуформальной.

14.6.5.3 Элементы действий оценщика

14.6.5.3.1 ADV_RCR.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.6.6 ADV_RCR.3 Формальная демонстрация соответствия

Зависимости: нет зависимостей.

14.6.6.1 Замечания по применению

Необходимо, чтобы разработчик продемонстрировал либо доказал соответствие представлений, как описано в требованиях ниже, соразмерно с уровнем строгости стиля представления. Например, соответствие необходимо доказать, если используемые представления специфицированы формально.

14.6.6.2 Элементы действий разработчика

14.6.6.2.1 ADV_RCR.3.1D

Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

14.6.6.2.2 ADV_RCR.3.2D

Для тех из соответствующих частей представлений, которые специфицированы формально, разработчик должен доказать это соответствие.

14.6.6.3 Элементы содержания и представления свидетельств

14.6.6.3.1 ADV_RCR.3.1C

Для каждой смежной пары имеющихся представлений ФБО анализ должен **доказать или** демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

14.6.6.3.2 ADV_RCR.3.2C

Для каждой смежной пары имеющихся представлений ФБО, где части **одного** представления **специфицированы полуформально, а другого** — по меньшей мере, полуформально, демонстрация соответствия между этими частями представлений должна быть полуформальной.

14.6.6.3.3 ADV_RCR.3.3C

Для каждой смежной пары имеющихся представлений ФБО, где части обоих представлений специфицированы формально, доказательство соответствия между этими частями представлений должно быть формальным.

14.6.6.4 Элементы действий оценщика

14.6.6.4.1 ADV_RCR.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.6.6.4.2 ADV_RCR.3.2E

Оценщик должен сделать независимое заключение о правильности доказательств соответствия, избирательно верифицируя формальный анализ.

14.7 Моделирование политики безопасности (ADV_SPM)

14.7.1 Цели

Цель этого семейства — повысить доверие к тому, что функции безопасности в функциональной спецификации осуществляют политики ПБО. Эта цель достигается посредством разработки модели политики безопасности, основанной на подмножестве политик ПБО, и установления соответствия между функциональной спецификацией, моделью политики безопасности и этим подмножеством политик ПБО.

14.7.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе степени формализации, требуемой от модели ПБО, и степени формализации, требуемой при установлении соответствия между моделью ПБО и функциональной спецификацией.

14.7.3 Замечания по применению

В то время как ПБО может включать в себя любые политики, модели ПБО традиционно представляют только подмножества этих политик, потому что моделирование некоторых политик в настоящее время не представляется выполнимым. Современное состояние вопроса определяет политики, которые могут быть смоделированы, и автору ПЗ/ЗБ следует идентифицировать конкретные функции и связанные с ними политики, которые можно, и поэтому требуется смоделировать. Как минимум, требуется моделировать политики управления доступом и информационными потоками (если они являются частью ПБО), так как в настоящее время это признается возможным.

В каждом из компонентов этого семейства присутствует требование описания в модели ПБО правил и характеристик применяемых политик ПБО и обеспечения адекватности модели ПБО соответствующим политикам ПБО. «Правила» и «характеристики» модели ПБО предназначены для обеспечения гибкости в выборе типа модели (например переход из одного состояния в другое, невмешательство), которая может быть разработана. Например, правила могут быть представлены как «свойства» (например отдельное свойство безопасности), а характеристики могут быть представлены такими определениями, как «начальное состояние», «безопасное состояние», «субъекты» и «объекты».

Применительно к уровню формализации модели ПБО и соответствия между моделью ПБО и функциональной спецификацией неформальный, полуформальный и формальный уровни рассматривают как иерархичные по сути. Так, ADV_SPM.1.1C может быть удовлетворен полуформальной или формальной моделью ПБО, а ADV_SPM.2.1C — также формальной моделью ПБО. Помимо этого, ADV_SPM.2.5C и ADV_SPM.3.5C могут быть удовлетворены формальным доказательством соответствия. И, наконец, при отсутствии каких-либо требований к уровню формализации демонстрация соответствия может быть неформальной, полуформальной или формальной.

14.7.4 ADV_SPM.1 Неформальная модель политики безопасности ОО

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация

14.7.4.1 Элементы действий разработчика

14.7.4.1.1 ADV_SPM.1.1D

Разработчик должен представить модель ПБО.

14.7.4.1.2 ADV_SPM.1.2D

Разработчик должен демонстрировать соответствие между функциональной спецификацией и моделью ПБО.

14.7.4.2 Элементы содержания и представления свидетельств

14.7.4.2.1 ADV_SPM.1.1C

Модель ПБО должна быть неформальной.

14.7.4.2.2 ADV_SPM.1.2C

Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

14.7.4.2.3 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.

14.7.4.2.4 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.

14.7.4.3 Элементы действий оценщика

14.7.4.3.1 ADV_SPM.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.7.5 ADV_SPM.2 Полуформальная модель политики безопасности ОО

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация

14.7.5.1 Элементы действий разработчика

14.7.5.1.1 ADV_SPM.2.1D

Разработчик должен представить модель ПБО.

14.7.5.1.2 ADV_SPM.2.2D

Разработчик должен демонстрировать соответствие между функциональной спецификацией и моделью ПБО.

14.7.5.2 Элементы содержания и представления свидетельств

14.7.5.2.1 ADV_SPM.2.1C

Модель ПБО должна быть **полуформальной**.

14.7.5.2.2 ADV_SPM.2.2C

Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

14.7.5.2.3 ADV_SPM.2.3C

Модель ПБО должна включать в себя обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

14.7.5.2.4 ADV_SPM.2.4C

Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

14.7.5.2.5 ADV_SPM.2.5C

Там, где функциональная спецификация, по меньшей мере, полуформальна, демонстрация соответствия между моделью ПБО и функциональной спецификацией должна быть полуформальной.

14.7.5.3 Элементы действий оценщика

14.7.5.3.1 ADV_SPM.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

14.7.6 ADV_SPM.3 Формальная модель политики безопасности ОО

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация

14.7.6.1 Элементы действий разработчика

14.7.6.1.1 ADV_SPM.3.1D

Разработчик должен представить модель ПБО.

14.7.6.1.2 ADV_SPM.3.2D

Разработчик должен демонстрировать **или доказать, где это требуется**, соответствие между функциональной спецификацией и моделью ПБО.

14.7.6.2 Элементы содержания и представления свидетельств

14.7.6.2.1 ADV_SPM.3.1C

Модель ПБО должна быть **формальной**.

14.7.6.2.2 ADV_SPM.3.2C

Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

14.7.6.2.3 ADV_SPM.3.3C

Модель ПБО должна включать в себя обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

14.7.6.2.4 ADV_SPM.3.4C

Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

14.7.6.2.5 ADV_SPM.3.5C

Там, где функциональная спецификация **полуформальна**, демонстрация соответствия между моделью ПБО и функциональной спецификацией должна быть полуформальной.

14.7.6.2.6 ADV_SPM.3.6C

Там, где функциональная спецификация формальна, доказательство соответствия между моделью ПБО и функциональной спецификацией должно быть формальным.

14.7.6.3 Элементы действий оценщика

14.7.6.3.1 ADV_SPM.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

15 Класс AGD. Руководства

Класс AGD «Руководства» содержит требования к содержанию «Руководства администратора» и «Руководства пользователя». Для безопасного администрирования и использования ОО необходимо описать все аспекты, относящиеся к безопасному применению ОО. Документация руководств включает в себя руководства пользователя и администратора, а также, когда пакет доверия содержит соответствующие требования, — специфические руководства для пользователей и администраторов, вытекающие из требований класса ADO «Поставка и эксплуатация» и семейства ALC_FLR «Устранение недостатков».

Декомпозиция класса AGD «Руководства» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 12.

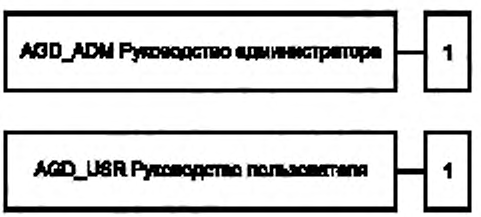


Рисунок 12 — Декомпозиция класса AGD «Руководства»

15.1 Руководство администратора (AGD_ADM)

15.1.1 Цели

Руководство администратора относится к печатным документам, предназначенным для использования лицами, ответственными за правильное конфигурирование, сопровождение и администрирование ОО в целях максимальной безопасности. Так как безопасность эксплуатации ОО зависит от правильного выполнения ФБО, лица, ответственные за выполнение указанных выше функций, являются доверенными для ФБО. Руководство предназначено способствовать пониманию администраторами функций безопасности, предоставляемых ОО, включая как функции, требующие выполнения администратором действий, критичных для безопасности, так и функции, предоставляющие информацию, критичную для безопасности.

15.1.2 Ранжирование компонентов

Данное семейство содержит только один компонент.

15.1.3 Замечания по применению

Требования AGD_ADM.1.3C и AGD_ADM.1.7C касаются того аспекта, что в руководстве администратора соответствующим образом должны быть отражены все упомянутые в ПЗ/ЗБ предупреждения пользователям ОО, относящиеся к среде безопасности и целям безопасности ОО.

Понятие «безопасные значения», как оно используется в AGD_ADM.1.5C, уместно при управлении администратором параметрами безопасности. В руководстве необходимо представить безопасные и опасные устанавливаемые значения для таких параметров. Это понятие связано с применением компонента FMT_MSA.2 из ИСО/МЭК 15408-2.

AGD_ADM.1.6C требует, чтобы руководство администратора содержало описание соответствующей реакции администратора на все относящиеся к безопасности события. Хотя многие относящиеся к безопасности события являются результатом выполнения административных функций, это не всегда должно быть так (например, заполнение журнала аудита, обнаружение вторжения). Кроме того, относящееся к безопасности событие может происходить в результате выполнения определенного ряда функций администратора или, наоборот, несколько относящихся к безопасности событий могут быть вызваны выполнением одной функции.

15.1.4 AGD_ADM.1 Руководство администратора

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация

15.1.4.1 Элементы действий разработчика

15.1.4.1.1 AGD_ADM.1.1D

Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

15.1.4.2 Элементы содержания и представления свидетельств

15.1.4.2.1 AGD_ADM.1.1C

Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

15.1.4.2.2 AGD_ADM.1.2C

Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

15.1.4.2.3 AGD_ADM.1.3C

Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

15.1.4.2.4 AGD_ADM.1.4C

Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

15.1.4.2.5 AGD_ADM.1.5C

Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

15.1.4.2.6 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.

15.1.4.2.7 AGD_ADM.1.7C

Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

15.1.4.2.8 AGD_ADM.1.8C

Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

15.1.4.3 Элементы действий оценщика

15.1.4.3.1 AGD_ADM.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

15.2 Руководство пользователя (AGD_USR)

15.2.1 Цели

Руководство пользователя относится к материалам, предназначенным для применения пользователями ОО, не связанными с администрированием, и другими лицами (например, программистами), использующими внешние интерфейсы ОО. Руководство описывает доступные пользователям функции безопасности, входящие в состав ФБО, и содержит инструкции и предписания, включая предупреждения, по их безопасному использованию.

Руководство пользователя является основой для предположений об использовании ОО и обеспечивает уверенность в том, что лояльные пользователи, поставщики приложений и прочие лица, использующие внешние интерфейсы ОО, поймут, как безопасно эксплуатировать ОО, и будут использовать его в соответствии с назначением.

15.2.2 Ранжирование компонентов

Данное семейство содержит только один компонент.

15.2.3 Замечания по применению

Требования AGD_USR.1.3C и AGD_USR.1.5C касаются того, что в руководстве пользователя соответствующим образом должны быть отражены все упомянутые в ПЗ/ЗБ предупреждения пользователям ОО, относящиеся к среде безопасности и целям безопасности ОО.

Во многих случаях может оказаться целесообразным, чтобы руководство было представлено несколькими различными документами: один для пользователей, а другой для прикладных программистов и/или проектировщиков аппаратных средств, использующих программные или аппаратные интерфейсы.

15.2.4 AGD_USR.1 Руководство пользователя

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация

15.2.4.1 Элементы действий разработчика

15.2.4.1.1 AGD_USR.1.1D

Разработчик должен представить руководство пользователя.

15.2.4.2 Элементы содержания и представления свидетельств

15.2.4.2.1 AGD_USR.1.1C

Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.

15.2.4.2.2 AGD_USR.1.2C

Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.

15.2.4.2.3 AGD_USR.1.3C

Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

15.2.4.2.4 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.

15.2.4.2.5 AGD_USR.1.5C

Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.

15.2.4.2.6 AGD_USR.1.6C

Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.

15.2.4.3 Элементы действий оценщика

15.2.4.3.1 AGD_USR.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16 Класс ALC. Поддержка жизненного цикла

Поддержка жизненного цикла является аспектом установления дисциплины и контроля в процессе уточнения ОО во время его разработки и сопровождения. Уверенность в соответствии ОО требованиям безопасности к ОО будет больше, если анализ безопасности и формирование свидетельств проводятся на регулярной основе как неотъемлемая часть деятельности при разработке и сопровождении.

Декомпозиция класса ALC «Поддержка жизненного цикла» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 13.



Рисунок 13 — Декомпозиция класса ALC
«Поддежка жизненного цикла»

16.1 Безопасность разработки (ALC_DVS)

16.1.1 Цели

Безопасность разработки связана с физическими, процедурными, относящимися к персоналу и другими мерами безопасности, которые могут применяться в среде разработки для защиты ОО. Безопасность разработки включает в себя физическую безопасность места разработки и любые процедуры, связанные с отбором персонала разработчиков.

16.1.2 Ранжирование компонентов

Компоненты в данном семействе ранжированы на основе наличия логического обоснования достаточности мер безопасности.

16.1.3 Замечания по применению

Семейство ALC_DVS связано с мерами по устранению или ослаблению угроз, существующих в месте разработки. Напротив, угрозы, противостоять которым необходимо по месту эксплуатации ОО, обычно учитывают в разделе «Среда безопасности» ПЗ или ЗБ.

Оценщику следует сделать заключение, необходимо ли ему посетить место разработки для подтверждения выполнения требований этого семейства.

Известно, что конфиденциальность не всегда может включаться в задачи защиты ОО в среде его разработки. Использование слова «необходимый» в ALC_DVS.1.1C и ALC_DVS.2.1C предусматривает возможность выбора соответствующих мер защиты.

16.1.4 ALC_DVS.1 Идентификация мер безопасности

Зависимости: нет зависимостей.

16.1.4.1 Элементы действий разработчика

16.1.4.1.1 ALC_DVS.1.1D

Разработчик должен разработать документацию по безопасности разработки.

16.1.4.2 Элементы содержания и представления свидетельств

16.1.4.2.1 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.

16.1.4.2.2 ALC_DVS.1.2C

Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

16.1.4.3 Элементы действий оценщика

16.1.4.3.1 ALC_DVS.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.1.4.3.2 ALC_DVS.1.2E

Оценщик должен подтвердить применение мер безопасности.

16.1.5 ALC_DVS.2 Достаточность мер безопасности

Зависимости: нет зависимостей.

16.1.5.1 Элементы действий разработчика

16.1.5.1.1 ALC_DVS.2.1D

Разработчик должен разработать документацию по безопасности разработки.

16.1.5.2 Элементы содержания и представления свидетельств

16.1.5.2.1 ALC_DVS.2.1C

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.

16.1.5.2.2 ALC_DVS.2.2C

Документация по безопасности разработки должна предоставить свидетельство того, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

16.1.5.2.3 ALC_DVS.2.3C

Свидетельство должно содержать логическое обоснование того, что меры безопасности обеспечивают необходимый уровень защиты конфиденциальности и целостности ОО.

16.1.5.3 Элементы действий оценщика

16.1.5.3.1 ALC_DVS.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.1.5.3.2 ALC_DVS.2.2E

Оценщик должен подтвердить применение мер безопасности.

16.2 Устранение недостатков (ALC_FLR)

16.2.1 Цели

Семейство ALC_FLR содержит требование, чтобы обнаруженные недостатки безопасности были отслежены и исправлены разработчиком. Хотя при оценке ОО не может быть сделано заключение о его соответствии процедурам устранения недостатков в будущем, можно оценить политики и процедуры, которые предусмотрены разработчиком для отслеживания и исправления недостатков, а также распространения информации о недостатках и их исправлении.

16.2.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе расширения области применения процедур устранения недостатков и повышения строгости политик устранения недостатков.

16.2.3 Замечания по применению

Данное семейство обеспечивает доверие к сопровождению и поддержке ОО в будущем, требуя от разработчика ОО отслеживать и исправлять недостатки в ОО. Кроме того, имеются требования по распространению сведений об исправлениях недостатков. Однако данное семейство не налагает требований, выходящих за рамки текущей оценки.

Пользователь ОО считается основным лицом в организации, ответственным за получение и применение исправлений недостатков безопасности. Таким лицом необязательно должен являться отдельный пользователь, им может быть представитель организации, ответственный за обработку недостатков безопасности. Использование термина «пользователь ОО» предполагает, что в различных организациях имеются различные процедуры обработки сообщений о недостатках, которые могут выполняться пользователями индивидуально либо централизовано административным лицом.

В процедурах устранения недостатков следует описать методы реагирования на все типы встречающихся недостатков. Некоторые недостатки не могут быть исправлены немедленно. Об этих недостатках могут сообщить разработчик ОО, пользователи ОО, другие стороны, знакомые с ОО. Не исключено, что недостаток вообще не может быть исправлен, и необходимо применить другие (например, процедурные) меры. Представленная документация должна охватывать процедуры по обеспечению исправлений в местах эксплуатации, а также предоставление информации о недостатках, для которых исправление отложено (и что делать в этой ситуации) или невозможно.

После того как оценка ОО завершена, он больше не является объектом оценки. Более того, любые изменения, вносимые в оцененный ОО, приводят к тому, что первоначальные результаты оценки не являются больше применимыми к измененной версии. Поэтому термин «релиз ОО», используемый в данном семействе, относится к версии продукта или системы, являющейся релизом сертифицированного ОО, в который были внесены изменения.

16.2.4 ALC_FLR.1 Базовое устранение недостатков

Зависимости: нет зависимостей.

16.2.4.1 Элементы действий разработчика

16.2.4.1.1 ALC_FLR.1.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

16.2.4.2 Элементы содержания и представления свидетельств

16.2.4.2.1 ALC_FLR.1.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

16.2.4.2.2 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.

16.2.4.2.3 ALC_FLR.1.3C

Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

16.2.4.2.4 ALC_FLR.1.4C

Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

16.2.4.3 Элементы действий оценщика

16.2.4.3.1 ALC_FLR.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.2.5 ALC_FLR.2 Процедуры сообщений о недостатках

Зависимости: нет зависимостей.

16.2.5.1 Цели

Для того чтобы разработчик имел возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности и знал, кому посылать исправления, пользователям ОО необходимо иметь представление о том, каким образом представлять сообщения о недостатках безопасности разработчику. Руководство по исправлению недостатков, предоставляемое разработчиком пользователям ОО, обеспечивает знание пользователями ОО этой важной информации.

16.2.5.2 Элементы действий разработчика

16.2.5.2.1 ALC_FLR.2.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

16.2.5.2.2 ALC_FLR.2.2D

Разработчик должен установить процедуру приема и отработки всех сообщений пользователей о недостатках безопасности и запросов на их исправление.

16.2.5.2.3 ALC_FLR.2.3D

Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

16.2.5.3 Элементы содержания и представления свидетельств

16.2.5.3.1 ALC_FLR.2.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

16.2.5.3.2 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.

16.2.5.3.3 ALC_FLR.2.3C

Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

16.2.5.3.4 ALC_FLR.2.4C

Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

16.2.5.3.5 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.

16.2.5.3.6 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.

16.2.5.3.7 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.

16.2.5.3.8 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.

16.2.5.4 Элементы действий оценщика

16.2.5.4.1 ALC_FLR.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.2.6 ALC_FLR.3 Систематическое устранение недостатков

Зависимости: нет зависимостей.

16.2.6.1 Цели

Для того чтобы разработчик имел возможность соответствующим образом реагировать на сообщения от пользователей ОО о недостатках безопасности и знал, кому посылать исправления, пользователям ОО необходимо иметь представление о том, каким образом представлять сообщения о недостатках безопасности на рассмотрение разработчику и каким образом регистрироваться у разработчика для того, чтобы получать исправления. Руководство по исправлению недостатков, предоставляемое разработчиком пользователям ОО, обеспечивает знание пользователями ОО этой важной информации.

16.2.6.2 Элементы действий разработчика

16.2.6.2.1 ALC_FLR.3.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

16.2.6.2.2 ALC_FLR.3.2D

Разработчик должен установить процедуру приема и отработки всех сообщений пользователей о недостатках безопасности и запросов на исправление этих недостатков.

16.2.6.2.3 ALC_FLR.3.3D

Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

16.2.6.3 Элементы содержания и представления свидетельств

16.2.6.3.1 ALC_FLR.3.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

16.2.6.3.2 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.

16.2.6.3.3 ALC_FLR.3.3C

Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

16.2.6.3.4 ALC_FLR.3.4C

Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

16.2.6.3.5 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.

16.2.6.3.6 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.

16.2.6.3.7 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.

16.2.6.3.8 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.

16.2.6.3.9 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.

16.2.6.3.10 ALC_FLR.3.10C

Руководство по устранению недостатков должно описывать средства, с помощью которых пользователи ОО могут регистрироваться у уразработчика, чтобы иметь право получать сообщения о недостатках безопасности и исправления.

16.2.6.3.11 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.

16.2.6.4 Элементы действий оценщика

16.2.6.4.1 ALC_FLR.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.3 Определение жизненного цикла (ALC_LCD)

16.3.1 Цели

Плохо управляемые разработка и сопровождение ОО могут приводить к неправильной реализации ОО (или к ОО, который отвечает не всем требованиям безопасности). Это, в свою очередь, приводит к нарушениям безопасности. Поэтому важно, чтобы в жизненном цикле ОО была как можно раньше установлена модель разработки и сопровождения ОО.

Использование модели разработки и сопровождения ОО не гарантирует, что ОО не будет содержать недостатки и будет отвечать всем функциональным требованиям безопасности. Может оказаться, что выбранная модель будет недостаточной или неадекватной, и поэтому выигрыш в качестве ОО не будет заметен. Использование модели жизненного цикла, одобренной некоторой группой экспертов (например, специалистами-теоретиками, органами стандартизации), повышает вероятность, что модель разработки и сопровождения будет содействовать достижению требуемого качества ОО.

16.3.2 Ранжирование компонентов

Компоненты в данном семействе ранжированы на основе повышения требований к стандартности и измеримости модели жизненного цикла, а также к согласованности с этой моделью.

16.3.3 Замечания по применению

Модель жизненного цикла объединяет процедуры, инструментальные средства и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают в себя методы проектирования, процедуры проверки, средства управления проектом, процедуры контроля изменений, методы тестирования и процедуры приемки. Эффективная модель жизненного цикла позволяет включить аспекты процесса разработки и сопровождения в общую структуру управления, которая устанавливает обязанности и контролирует развитие.

Оценка аспектов сопровождения ОО повышает доверие к ОО за счет анализа информации о жизненном цикле ОО, представленной во время оценки до начала сопровождения.

Стандартизованная модель жизненного цикла — это модель, которая была одобрена некоторой группой экспертов (например, специалистами-теоретиками, органами стандартизации).

Измеримая модель жизненного цикла — это модель с количественными параметрами и/или метриками, используемыми для измерения характеристик разработки ОО (например, метрикой сложности исходного текста).

Модель жизненного цикла обеспечивает необходимый контроль за разработкой и сопровождением ОО, если разработчик может предоставить информацию, которая показала бы, что модель приемлемым образом минимизирует риск нарушений безопасности в ОО. При определении модели для части жизненного цикла после поставки ОО может быть полезна информация о предполагаемой среде ОО и целях безопасности ОО, приведенная в ЗБ.

16.3.4 ALC_LCD.1 Определение модели жизненного цикла разработчиком

Зависимости: нет зависимостей.

16.3.4.1 Элементы действий разработчика

16.3.4.1.1 ALC_LCD.1.1D

Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

16.3.4.1.2 ALC_LCD.1.2D

Разработчик должен представить документацию по определению жизненного цикла.

16.3.4.2 Элементы содержания и представления свидетельств

16.3.4.2.1 ALC_LCD.1.1C

Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

16.3.4.2.2 ALC_LCD.1.2C

Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

16.3.4.3 Элементы действий оценщика

16.3.4.3.1 ALC_LCD.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.3.5 ALC_LCD.2 Стандартизованная модель жизненного цикла

Зависимости: нет зависимостей.

16.3.5.1 Элементы действий разработчика

16.3.5.1.1 ALC_LCD.2.1D

Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

16.3.5.1.2 ALC_LCD.2.2D

Разработчик должен представить документацию по определению жизненного цикла.

16.3.5.1.3 ALC_LCD.2.3D

Разработчик должен использовать стандартизованную модель жизненного цикла для разработки и сопровождения ОО.

16.3.5.2 Элементы содержания и представления свидетельств

16.3.5.2.1 ALC_LCD.2.1C

Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

16.3.5.2.2 ALC_LCD.2.2C

Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

16.3.5.2.3 ALC_LCD.2.3C

Документация по определению жизненного цикла должна объяснить выбор модели.

16.3.5.2.4 ALC_LCD.2.4C

Документация по определению жизненного цикла должна объяснить, как модель используется при разработке и сопровождении ОО.

16.3.5.2.5 ALC_LCD.2.5C

Документация по определению жизненного цикла должна демонстрировать согласованность со стандартизованной моделью жизненного цикла.

16.3.5.3 Элементы действий оценщика

16.3.5.3.1 ALC_LCD.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.3.6 ALC_LCD.3 Измеримая модель жизненного цикла

Зависимости: нет зависимостей.

16.3.6.1 Элементы действий разработчика

16.3.6.1.1 ALC_LCD.3.1D

Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

16.3.6.1.2 ALC_LCD.3.2D

Разработчик должен представить документацию по определению жизненного цикла.

16.3.6.1.3 ALC_LCD.3.3D

Разработчик должен использовать стандартизованную и измеримую модель жизненного цикла для разработки и сопровождения ОО.

16.3.6.1.4 ALC_LCD.3.4D

Разработчик должен количественно оценить процесс разработки ОО, используя стандартизованную и измеримую модель жизненного цикла.

16.3.6.2 Элементы содержания и представления свидетельств

16.3.6.2.1 ALC_LCD.3.1C

Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО, **включая детализацию ее количественных параметров и/или метрик, используемых для оценки соответствия процесса разработки ОО принятой модели.**

16.3.6.2.2 ALC_LCD.3.2C

Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

16.3.6.2.3 ALC_LCD.3.3C

Документация по определению жизненного цикла должна объяснить выбор модели.

16.3.6.2.4 ALC_LCD.3.4C

Документация по определению жизненного цикла должна объяснить, как модель используется при разработке и сопровождении ОО.

16.3.6.2.5 ALC_LCD.3.5C

Документация по определению жизненного цикла должна демонстрировать согласованность со стандартизованной **и измеримой** моделью жизненного цикла.

16.3.6.2.6 ALC_LCD.3.6C

Документация по жизненному циклу должна представить результаты количественной оценки процесса разработки ОО с использованием стандартизованной и измеримой модели жизненного цикла.

16.3.6.3 Элементы действий оценщика

16.3.6.3.1 ALC_LCD.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.4 Инструментальные средства и методы (ALC_TAT)

16.4.1 Цели

Семейство ALC_TAT связано с выбором инструментальных средств, используемых для разработки, анализа и реализации ОО. Семейство содержит требования по предотвращению использования плохо определенных, несогласованных или неподходящих инструментальных средств разработки ОО. Это относится, в частности, к языкам программирования, документации, стандартам реализации и некоторым частям ОО, например, вспомогательным динамическим библиотекам.

16.4.2 Ранжирование компонентов

Компоненты в данном семействе ранжированы на основе повышения требований к описанию и области применения стандартов реализации и документации по опциям, зависимым от реализации.

16.4.3 Замечания по применению

Полностью определенными называют инструментальные средства разработки, которые применимы без необходимости подробных дополнительных пояснений. Например, принято считать полностью определенными языки программирования и системы автоматизации проектирования (САПР), которые основаны на стандартах.

В данном семействе различают стандарты реализации, которые применялись разработчиком (ALC_TAT.2.3D), и стандарты реализации для «всех частей ОО» (ALC_TAT.3.3D), в которые дополнительно включены программные, аппаратные или программно-аппаратные средства сторонних разработчиков.

Требование в ALC_TAT.1.2C применяют, главным образом, к языкам программирования для обеспечения однозначности всех операторов исходного текста.

16.4.4 ALC_TAT.1 Полностью определенные инструментальные средства разработки

Зависимости: ADV_IMP.1 Подмножество реализации ФБО

16.4.4.1 Элементы действий разработчика

16.4.4.1.1 ALC_TAT.1.1D

Разработчик должен идентифицировать инструментальные средства разработки ОО.

16.4.4.1.2 ALC_TAT.1.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

16.4.4.2 Элементы содержания и представления свидетельств

16.4.4.2.1 ALC_TAT.1.1C

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

16.4.4.2.2 ALC_TAT.1.2C

Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

16.4.4.2.3 ALC_TAT.1.3C

Документация инструментальных средств разработки должна однозначно определить значения всех опций, обусловленных реализацией.

16.4.4.3 Элементы действий оценщика

16.4.4.3.1 ALC_TAT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.4.5 ALC_TAT.2 Соответствие стандартам реализации

Зависимости: ADV_IMP.1 Подмножество реализации ФБО

16.4.5.1 Элементы действий разработчика

16.4.5.1.1 ALC_TAT.2.1D

Разработчик должен идентифицировать инструментальные средства разработки ОО.

16.4.5.1.2 ALC_TAT.2.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

16.4.5.1.3 ALC_TAT.2.3D

Разработчик должен привести описание применявшихся стандартов реализации.

16.4.5.2 Элементы содержания и представления свидетельств

16.4.5.2.1 ALC_TAT.2.1C

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

16.4.5.2.2 ALC_TAT.2.2C

Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

16.4.5.2.3 ALC_TAT.2.3C

Документация инструментальных средств разработки должна однозначно определить значения всех опций, обусловленных реализацией.

16.4.5.3 Элементы действий оценщика

16.4.5.3.1 ALC_TAT.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.4.5.3.2 ALC_TAT.2.2E

Оценщик должен подтвердить, что стандарты реализации применялись.

16.4.6 ALC_TAT.3 Соответствие всех частей ОО стандартам реализации

Зависимости: ADV_IMP.1 Подмножество реализации ФБО

16.4.6.1 Элементы действий разработчика

16.4.6.1.1 ALC_TAT.3.1D

Разработчик должен идентифицировать инструментальные средства разработки ОО.

16.4.6.1.2 ALC_TAT.3.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

16.4.6.1.3 ALC_TAT.3.3D

Разработчик должен привести описание стандартов реализации **для всех частей ОО.**

16.4.6.2 Элементы содержания и представления свидетельств

16.4.6.2.1 ALC_TAT.3.1C

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

16.4.6.2.2 ALC_TAT.3.2C

Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

16.4.6.2.3 ALC_TAT.3.3C

Документация инструментальных средств разработки должна однозначно определить значения всех опций, обусловленных реализацией.

16.4.6.3 Элементы действий оценщика

16.4.6.3.1 ALC_TAT.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

16.4.6.3.2 ALC_TAT.3.2E

Оценщик должен подтвердить, что стандарты реализации применялись.

17 Класс ATE. Тестирование

Класс ATE «Тестирование» включает в себя четыре семейства: ATE_COV «Покрытие», ATE_DPT «Глубина», ATE_FUN «Функциональное тестирование» и ATE_IND «Независимое тестирование» (например, функциональное тестирование, проводимое оценщиками). Тестирование помогает установить, что функциональные требования безопасности ОО выполнены. Тестирование обеспечивает доверие к тому, что ОО удовлетворяет, по меньшей мере, функциональным требованиям безопасности ОО, хотя оно и не может установить, что ОО не обладает большими возможностями, чем определено спецификациями. Тестирование также может быть направлено на внутреннюю структуру ФБО, например, тестирование подсистем и модулей на соответствие их спецификациям.

Аспекты покрытия и глубины отделены от функционального тестирования для повышения гибкости при применении компонентов семейств. Тем не менее, требования этих трех семейств предназначены для совместного применения.

Компоненты семейства «Независимое тестирование» имеют зависимости от компонентов других семейств, позволяющие получить необходимую информацию для поддержки требований, но при этом относятся в первую очередь к независимым действиям оценщика.

Основное внимание в этом классе уделено подтверждению того, что ФБО выполняются согласно их спецификациям. Для этого применяют и позитивное тестирование, основанное на функциональных требованиях, и негативное тестирование, чтобы проверить отсутствие нежелательных режимов выполнения. Этот класс не распространяется на тестирование проникновения, которое направлено на поиск уязвимостей, дающих пользователю возможность нарушить политику безопасности. Тестирование проникновения базируется на анализе ОО, направленном специально на идентификацию уязвимостей в проекте и реализации ФБО, и рассматривается отдельно как аспект оценки уязвимостей в классе AVA «Оценка уязвимостей».

Декомпозиция класса ATE «Тестирование» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 14.

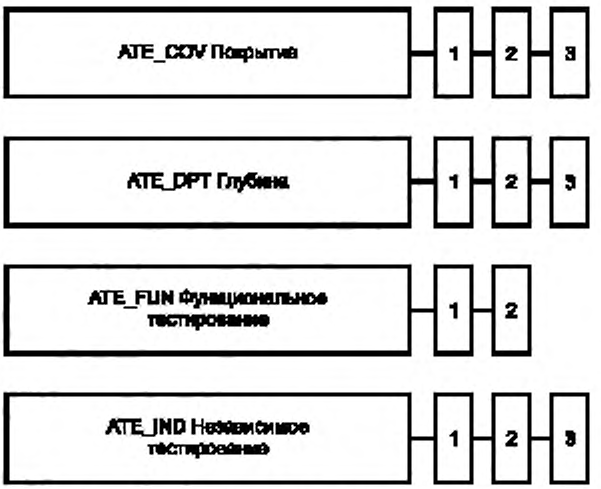


Рисунок 14 — Декомпозиция класса «Тестирование»

17.1 Покрытие (ATE_COV)

17.1.1 Цели

Семейство ATE_COV направлено на те аспекты тестирования, которые имеют отношение к полноте охвата (покрытия) тестами. Таким образом, семейство связано с объемом тестирования ФБО, а также с выяснением, является ли тестирование достаточно всесторонним, чтобы продемонстрировать выполнение ФБО в соответствии со спецификациями.

17.1.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе повышения строгости тестирования интерфейсов и строгости анализа достаточности тестов для демонстрации, что ФБО выполняются в соответствии с их функциональной спецификацией.

17.1.3 ATE_COV.1 Свидетельство покрытия

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ATE_FUN.1 Функциональное тестирование

17.1.3.1 Цели

Цель данного компонента состоит в том, чтобы установить, что ФБО были проверены на соответствие их функциональной спецификации. Эта цель достигается путем экспертизы представленного разработчиком свидетельства соответствия.

17.1.3.2 Замечания по применению

Хотя цель тестирования состоит в полном покрытии ФБО, для верификации этого утверждения достаточно неформального сопоставления тестов с функциональной спецификацией и собственно данных тестирования.

В данном компоненте от разработчика требуется показать, насколько идентифицированные тесты соответствуют описанию ФБО в функциональной спецификации. Это может быть достигнуто представлением соответствия (возможно, с использованием таблицы). Такая информация необходима оценщику для подготовки программы тестирования при оценке. На рассматриваемом уровне нет требований полного покрытия разработчиком каждого аспекта ФБО, поэтому оценщику следует принять во внимание возможные пробелы в этой области.

17.1.3.3 Элементы действий разработчика

17.1.3.3.1 ATE_COV.1.1D

Разработчик должен представить свидетельство покрытия тестами.

17.1.3.4 Элементы содержания и представления свидетельств

17.1.3.4.1 ATE_COV.1.1C

Свидетельство покрытия тестами должно показать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

17.1.3.5 Элементы действий оценщика

17.1.3.5.1 ATE_COV.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.1.4 ATE_COV.2 Анализ покрытия

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ATE_FUN.1 Функциональное тестирование

17.1.4.1 Цели

Цель данного компонента состоит в том, чтобы установить, что ФБО были проверены на соответствие их функциональной спецификации систематическим методом. Эта цель достигается путем экспертизы представленного разработчиком анализа соответствия.

17.1.4.2 Замечания по применению

От разработчика требуется продемонстрировать, что идентифицированные тесты включают в себя проверку всех функций безопасности, представленных в функциональной спецификации. При анализе следует не только показать соответствие между тестами и функциями безопасности, но также предоставить оценщику достаточную информацию для вынесения независимого заключения о том, насколько функции были проверены. Эта информация может быть использована при планировании дополнительных тестов оценщика. Хотя на этом уровне разработчик должен продемонстрировать, что каждая из функций в функциональной спецификации была проверена, исчерпывающее тестирование каждой функции не обязательно.

17.1.4.3 Элементы действий разработчика

17.1.4.3.1 ATE_COV.2.1D

Разработчик должен представить **анализ** покрытия тестами.

17.1.4.4 Элементы содержания и представления свидетельств

17.1.4.4.1 ATE_COV.2.1C

Анализ покрытия тестами должен **демонстрировать** соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

17.1.4.4.2 ATE_COV.2.2C

Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

17.1.4.5 Элементы действий оценщика

17.1.4.5.1 ATE_COV.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.1.5 ATE_COV.3 Строгий анализ покрытия

Зависимости: ADV_FSP.2 Полностью определенные внешние интерфейсы
ATE_FUN.1 Функциональное тестирование

17.1.5.1 Цели

Цель данного компонента состоит в том, чтобы установить, что ФБО были проверены систематическим и исчерпывающим образом на соответствие их функциональной спецификации. Эта цель достигается путем экспертизы анализа соответствия, представленного разработчиком.

17.1.5.2 Замечания по применению

От разработчика требуется предоставить убедительные аргументы того, что идентифицированные тесты покрывают все функции безопасности, а тестирование каждой функции безопасности является полным. Оценщику остается мало возможностей для разработки дополнительных функциональных тестов интерфейсов ФБО, основанных на функциональной спецификации, поскольку они будут исчерпывающе проверены. Тем не менее оценщику следует разрабатывать такие тесты.

17.1.5.3 Элементы действий разработчика

17.1.5.3.1 ATE_COV.3.1D

Разработчик должен представить анализ покрытия тестами.

17.1.5.4 Элементы содержания и представления свидетельств

17.1.5.4.1 ATE_COV.3.1C

Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

17.1.5.4.2 ATE_COV.3.2C

Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

17.1.5.4.3 ATE_COV.3.3C

Анализ покрытия тестами должен убедительно демонстрировать, что все внешние интерфейсы ФБО, идентифицированные в функциональной спецификации, полностью проверены.

17.1.5.5 Элементы действий оценщика

17.1.5.5.1 ATE_COV.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.2 Глубина (ATE_DPT)

17.2.1 Цели

Компоненты данного семейства имеют отношение к уровню детализации тестирования ФБО. Тестирование функций безопасности основано на детализации информации, полученной из анализа представлений.

Цель тестирования — противостоять риску пропуска ошибки при разработке ОО. Дополнительно компоненты этого семейства позволяют с большей вероятностью обнаружить любой внесенный злонамеренный код, особенно потому, что тестирование в большей степени касается внутренней структуры ФБО.

Тестирование конкретных внутренних интерфейсов может обеспечивать доверие не только к тому, что ФБО внешне соответствуют желательному режиму безопасности, но также к тому, что этот режим является следствием корректного функционирования внутренних механизмов.

17.2.2 Ранжирование компонентов

Компоненты в данном семействе ранжированы на основе увеличения степени детализации в представлениях ФБО, от проекта верхнего уровня до представления реализации. Такое ранжирование отражает представления ФБО, рассмотренные в классе ADV.

17.2.3 Замечания по применению

Конкретный объем, а также типы документации и свидетельств будут определяться, в основном, выбранным из семейства ATE_FUN «Функциональное тестирование» компонентом.

Тестирование на уровне функциональной спецификации рассмотрено в ATE_COV «Покрытие».

В данном семействе принят принцип соответствия уровня тестирования искомому уровню доверия. Там, где применяют более высокие по иерархии компоненты, от результатов тестирования требуется демонстрация того, что реализация ФБО не противоречит проекту ФБО. Например, в проекте верхнего уровня следует описать с достаточной детализацией каждую из подсистем, а также интерфейсы для взаимодействия этих подсистем. В свидетельстве тестирования необходимо показать, что были проверены внутренние интерфейсы для взаимодействия подсистем. Это может быть достигнуто тестированием через внешние интерфейсы ФБО либо автономной проверкой интерфейсов подсистем, возможно, с использованием средств и среды автономного тестирования. В случаях, если некоторые аспекты внутреннего интерфейса не могут быть проверены через внешние интерфейсы, следует иметь логическое обоснование того, что эти аспекты проверять необязательно, либо проверить этот внутренний интерфейс непосредственно. В последнем случае необходимо, чтобы проект верхнего уровня был достаточно детализированным для облегчения прямого тестирования. Иерархичные компоненты в этом семействе нацелены на проверку правильности использования внутренних интерфейсов, которые становятся видимыми по мере того, как проект становится менее абстрактным. Когда применяют эти компоненты, сложнее обеспечить адекватное свидетельство глубины тестирования, используя только внешние интерфейсы ФБО, поэтому, как правило, необходимо тестирование на уровне модулей.

17.2.4 ATE_DPT.1 Тестирование: проект верхнего уровня

Зависимости: ADV_HLD.1 Описательный проект верхнего уровня
ATE_FUN.1 Функциональное тестирование

17.2.4.1 Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутреннего устройства ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие к тому, что подсистемы ФБО были правильно реализованы.

17.2.4.2 Замечания по применению

Разработчик, как ожидается, представит описание процесса тестирования в контексте проекта верхнего уровня ФБО в терминах «подсистем». Термин «подсистема» используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

17.2.4.3 Элементы действий разработчика

17.2.4.3.1 ATE_DPT.1.1D

Разработчик должен представить анализ глубины тестирования.

17.2.4.4 Элементы содержания и представления свидетельств

17.2.4.4.1 ATE_DPT.1.1C

Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации того, что ФБО выполняются в соответствии с проектом верхнего уровня.

17.2.4.5 Элементы действий оценщика

17.2.4.5.1 ATE_DPT.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.2.5 ATE_DPT.2 Тестирование: проект нижнего уровня

Зависимости: ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_LLD.1 Описательный проект нижнего уровня
ATE_FUN.1 Функциональное тестирование

17.2.5.1 Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутреннего устройства ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие к тому, что подсистемы ФБО были правильно реализованы.

Модули ФБО обеспечивают описание внутренних действий ФБО. Тестирование на уровне модулей для демонстрации наличия любых недостатков обеспечивает доверие к тому, что модули ФБО были правильно реализованы.

17.2.5.2 Замечания по применению

Разработчик, как ожидается, представит описание процесса тестирования в контексте проекта верхнего уровня ФБО в терминах «подсистем». Термин «подсистема» используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

Разработчик, как ожидается, опишет тестирование проекта нижнего уровня ФБО в терминах «модулей». Термин «модуль» используют, чтобы отразить декомпозицию каждой из подсистем ФБО на относительно малое число частей.

17.2.5.3 Элементы действий разработчика

17.2.5.3.1 ATE_DPT.2.1D

Разработчик должен представить анализ глубины тестирования.

17.2.5.4 Элементы содержания и представления свидетельств

17.2.5.4.1 ATE_DPT.2.1C

Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня **и проектом нижнего уровня.**

17.2.5.5 Элементы действий оценщика

17.2.5.5.1 ATE_DPT.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.2.6 ATE_DPT.3 Тестирование на уровне реализации

Зависимости: ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_IMP.2 Реализация ФБО
ADV_LLD.1 Описательный проект нижнего уровня
ATE_FUN.1 Функциональное тестирование

17.2.6.1 Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутреннего устройства ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие к тому, что подсистемы ФБО были правильно реализованы.

Модули ФБО обеспечивают описание внутренних действий ФБО. Тестирование на уровне модулей для демонстрации наличия любых недостатков обеспечивает доверие к тому, что модули ФБО были правильно реализованы.

Представление реализации ФБО обеспечивает детализированное описание внутреннего устройства ФБО. Тестирование на уровне реализации для демонстрации наличия любых недостатков обеспечивает доверие к тому, что реализация ФБО была выполнена правильно.

17.2.6.2 Замечания по применению

Разработчик, как ожидается, представит описание процесса тестирования в контексте проекта верхнего уровня ФБО в терминах «подсистем». Термин «подсистема» используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

Разработчик, как ожидается, представит описание процесса тестирования в контексте проекта нижнего уровня ФБО в терминах «модулей». Термин «модуль» используют, чтобы отразить декомпозицию каждой из подсистем ФБО на относительно малое число частей.

Представление реализации используют непосредственно для генерации реализации ФБО (например исходный текст, который затем компилируют).

17.2.6.3 Элементы действий разработчика

17.2.6.3.1 ATE_DPT.3.1D

Разработчик должен представить анализ глубины тестирования.

17.2.6.4 Элементы содержания и представления свидетельств

17.2.6.4.1 ATE_DPT.3.1C

Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня, проектом нижнего уровня и представлением реализации.

17.2.6.5 Элементы действий оценщика

17.2.6.5.1 ATE_DPT.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.3 Функциональное тестирование (ATE_FUN)

17.3.1 Цели

Функциональное тестирование, выполняемое разработчиком, устанавливает, что ФБО проявляют свойства, необходимые для удовлетворения функциональных требований ПЗ/ЗБ. Такое функциональное тестирование обеспечивает доверие к тому, что ОО, по меньшей мере, соответствует функциональным требованиям безопасности ОО, хотя и не может установить, что ОО не обладает большими возможностями, чем определено спецификациями. Семейство «Функциональное тестирование» сосредоточено на типе и объеме необходимой документации или требуемых инструментальных средств поддержки, а также на том, что будет демонстрировать тестирование, проведенное разработчиком. Функциональное тестирование не ограничено позитивным подтверждением предоставления требуемых функций безопасности, но может также включать в себя негативное тестирование (часто основанное на инверсии функциональных требований) для проверки отсутствия нежелательных режимов функционирования.

Данное семейство способствует обеспечению доверия к тому, что вероятность наличия незамеченных недостатков относительно мала.

Семейства ATE_COV «Покрытие», ATE_DPT «Глубина» и ATE_FUN «Функциональное тестирование» используют совместно для определения свидетельства тестирования, представляемого разработчиком. Независимое функциональное тестирование, выполняемое оценщиком, рассмотрено в ATE_IND «Независимое тестирование».

17.3.2 Ранжирование компонентов

Данное семейство содержит два компонента. Иерархичный компонент содержит требование анализа зависимости от порядка выполнения процедур тестирования.

17.3.3 Замечания по применению

Как ожидается, процедуры выполнения тестов будут содержать инструкции по использованию тестовых программ и комплектов тестов, включая среду, условия тестирования, параметры и значения тестовых данных. Необходимо также, чтобы процедуры тестирования показывали, как результаты тестирования получаются из входных данных тестирования.

Данное семейство определяет требования для представления всех планов, процедур и результатов тестирования. Поэтому объем информации, которая должна быть представлена, будет меняться в зависимости от использования ATE_COV «Покрытие» и ATE_DPT «Глубина».

Зависимость от порядка выполнения актуальна, если успешное выполнение конкретного теста зависит от существования конкретного состояния. Например, можно потребовать, чтобы тест А выполнялся непосредственно перед тестом В, так как состояние, следующее из успешного выполнения теста А, — предпосылка для успешного выполнения теста В. Таким образом, неудача теста В может быть связана с проблемой зависимости от порядка выполнения. В приведенном примере тест В может закончиться неудачно, потому что тест С (а не А) был выполнен непосредственно перед ним, или же неудача теста В связана с неудачей теста А.

17.3.4 ATE_FUN.1 Функциональное тестирование

Зависимости: нет зависимостей.

17.3.4.1 Цели

Цель разработчика — продемонстрировать, что все функции безопасности выполняются в соответствии со спецификациями. От разработчика требуется выполнить тестирование и представить тестовую документацию.

17.3.4.2 Элементы действий разработчика

17.3.4.2.1 ATE_FUN.1.1D

Разработчик должен протестировать ФБО и задокументировать результаты.

17.3.4.2.2 ATE_FUN.1.2D

Разработчик должен представить тестовую документацию.

17.3.4.3 Элементы содержания и представления свидетельств

17.3.4.3.1 ATE_FUN.1.1C

Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

17.3.4.3.2 ATE_FUN.1.2C

Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей проводимых тестов.

17.3.4.3.3 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.

17.3.4.3.4 ATE_FUN.1.4C

Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

17.3.4.3.5 ATE_FUN.1.5C

Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

17.3.4.4 Элементы действий оценщика

17.3.4.4.1 ATE_FUN.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.3.5 ATE_FUN.2 Упорядоченное функциональное тестирование

Зависимости: нет зависимостей.

17.3.5.1 Цели

Цель разработчика — продемонстрировать, что все функции безопасности выполняются в соответствии со спецификациями. От разработчика требуется выполнить тестирование и представить тестовую документацию.

Дополнительная цель данного компонента — обеспечить, чтобы зависимости между тестами были идентифицированы и понятны. Понимание зависимостей между тестами уменьшает вероятность того, что результаты тестов, выполненных различными сторонами или в разное время, будут отличаться из-за различной последовательности выполнения данных тестов.

17.3.5.2 Замечания по применению

Хотя процедуры тестирования могут устанавливать необходимые начальные условия тестирования на основе упорядочения тестов, они могут не содержать какого-либо обоснования этого упорядочения. Анализ упорядочения тестов — важный фактор в определении адекватности тестирования, так как имеется возможность сокрытия ошибок как следствие конкретного порядка выполнения тестов.

17.3.5.3 Элементы действий разработчика

17.3.5.3.1 ATE_FUN.2.1D

Разработчик должен протестировать ФБО и задокументировать результаты.

17.3.5.3.2 ATE_FUN.2.2D

Разработчик должен представить тестовую документацию.

17.3.5.4 Элементы содержания и представления свидетельств

17.3.5.4.1 ATE_FUN.2.1C

Тестовая документация должна состоять из планов и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

17.3.5.4.2 ATE_FUN.2.2C

Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей проводимых тестов.

17.3.5.4.3 ATE_FUN.2.3C

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.

17.3.5.4.4 ATE_FUN.2.4C

Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

17.3.5.4.5 ATE_FUN.2.5C

Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

17.3.5.4.6 ATE_FUN.2.6C

Тестовая документация должна включать в себя анализ зависимостей от порядка выполнения процедуры тестирования.

17.3.5.5 Элементы действий оценщика

17.3.5.5.1 ATE_FUN.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.4 Независимое тестирование (ATE_IND)

17.4.1 Цели

Главная цель — продемонстрировать, что функции безопасности выполняются в соответствии со спецификациями.

Дополнительная цель — противостоять риску неправильной оценки разработчиком выходных данных тестов, приводящей к неправильной реализации спецификаций или пропуска кода, который не согласуется со спецификациями.

17.4.2 Ранжирование компонентов

Ранжирование компонентов основано на объеме тестовой документации и поддержки тестирования, а также на объеме тестирования оценщиком.

17.4.3 Замечания по применению

Тестирование, рассматриваемое в данном семействе, может проводиться с привлечением, помимо оценщика, других квалифицированных исполнителей (например, независимой лаборатории, организации конечных потребителей). При этом тестирование требует понимания ОО с учетом выполнения других действий по установлению доверия к ОО, а оценщик по-прежнему отвечает за обеспечение удовлетворения требований данного семейства, если такое привлечение имеет место.

Это семейство имеет отношение к степени выполнения независимого функционального тестирования ФБО. Независимое функциональное тестирование может приобретать форму полного или частичного повторения функциональных тестов, выполненных разработчиком. Оно может также проводиться в дополнение к функциональным тестам, выполненным разработчиком, как для увеличения области покрытия или глубины тестов, так и для проверки очевидных, известных из общедоступных источников слабых мест безопасности, которые могут быть в ОО. Эти действия дополняют друг друга, и для каждого ОО необходимо планировать приемлемое их сочетание с учетом применимости и области покрытия результатов тестов, а также функциональной сложности ФБО. Следует разработать план тестирования, согласующийся с уровнем других действий по установлению доверия к ОО, который, если требуется более высокое доверие, включает в себя повторение большей выборки тестов и большего объема независимых позитивных и негативных функциональных тестов, выполняемых оценщиком.

Повторение выборки тестов, выполненных разработчиком, предназначено для обеспечения подтверждения, что разработчик выполнил свою запланированную программу тестирования ФБО и правильно зафиксировал результаты. На объем установленной выборки будут влиять детализация и качество результатов функционального тестирования разработчиком. Необходимо также, чтобы оценщик рассмотрел возможности разработки дополнительных тестов и относительную пользу, которая может быть получена от их использования. Повторение всех тестов, выполненных разработчиком, может быть осуществимо и желательно в некоторых случаях, но весьма затруднено и менее продуктивно в других. Поэтому самый высокий по иерархии компонент данного семейства следует использовать осторожно. При формировании выборки рассматривается весь диапазон применения результатов тестирования, включая обеспечение выполнения требований семейств ATE_COV «Покрытие» и ATE_DPT «Глубина».

Необходимо также принять во внимание, что при оценке могут использоваться разные конфигурации ОО. Оценщику необходимо будет проанализировать применимость предоставленных результатов и в соответствии с этим планировать собственное тестирование.

Независимое функциональное тестирование отличается от тестирования проникновения, основанного на целенаправленном и систематическом поиске уязвимостей в проекте и/или реализации. Тестирование проникновения рассмотрено в семействе AVA_VLA «Анализ уязвимостей».

Пригодность ОО для тестирования основана на доступности ОО и поддержке документацией и информацией, необходимыми для выполнения тестов (включая любое тестовое программное обеспечение или инструментальные средства тестирования). Необходимость в такой поддержке отражена в зависимостях от других семейств доверия.

Кроме того, пригодность ОО для тестирования может основываться на других соображениях. Например, версия ОО, представленная разработчиком, может быть не окончательной.

Ссылки на подмножество ФБО предназначены для того, чтобы позволить оценщику проектировать приемлемую совокупность тестов, согласованную с целями проводимой оценки.

17.4.4 ATE_IND.1 Независимое тестирование на соответствие

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

17.4.4.1 Цели

Целью является демонстрация выполнения функций безопасности в соответствии со спецификациями.

17.4.4.2 Замечания по применению

Данный компонент не ориентирован на использование результатов тестирования разработчиком. Он применим, если такие результаты недоступны, а также в случае, если тестирование, выполненное разработчиком, принимается без проверки. От оценщика требуется разработать и выполнить тесты с целью подтверждения того, что функциональные требования безопасности ОО удовлетворены. При этом подходе уверенность в правильном функционировании приобретается через репрезентативное тестирование, а не через выполнение всех возможных тестов. Объем тестирования, планируемый для этой цели, является методологической проблемой, и его необходимо рассматривать в контексте конкретного ОО и в сопоставлении с другими действиями оценки.

17.4.4.3 Элементы действий разработчика

17.4.4.3.1 ATE_IND.1.1D

Разработчик должен представить ОО для тестирования.

17.4.4.4 Элементы содержания и представления свидетельств

17.4.4.4.1 ATE_IND.1.1C

ОО должен быть пригоден для тестирования.

17.4.4.5 Элементы действий оценщика

17.4.4.5.1 ATE_IND.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.4.4.5.2 ATE_IND.1.2E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

17.4.5 ATE_IND.2 Выборочное независимое тестирование

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя
ATE_FUN.1 Функциональное тестирование

17.4.5.1 Цели

Целью является демонстрация выполнения функций безопасности в соответствии со спецификациями. Тестирование, проводимое оценщиком, включает в себя отбор и повторение тестов, выполненных разработчиком.

17.4.5.2 Замечания по применению

Разработчику следует предоставить оценщику материалы, необходимые для эффективного воспроизведения тестов, выполненных разработчиком. В состав этих материалов могут быть включены такие материалы, как машиночитаемая тестовая документация, тест-программы и т.д.

Данный компонент содержит требование о том, чтобы оценщику были доступны результаты тестирования разработчиком для дополнения программы тестирования. Оценщик должен повторить выборку из тестов, выполненных разработчиком, чтобы получить уверенность в полученных результатах. Получив такую уверенность, оценщик расширит тестирование, выполненное разработчиком, проводя дополнительные испытания ОО способом, отличающимся от примененного разработчиком. Основываясь на подтверждении достоверности результатов тестов, выполненных разработчиком, оценщик будет способен убедиться в том, что ОО функционирует правильно, в более широком диапазоне условий, чем это было бы возможно для разработчика, ограниченного уровнем его ресурсов. Убедившись в том, что разработчик протестировал ОО, оценщик будет также иметь больше свободы выбора для концентрации тестирования в тех направлениях, где экспертиза документации или специальные знания вызвали определенную настороженность.

17.4.5.3 Элементы действий разработчика

17.4.5.3.1 ATE_IND.2.1D

Разработчик должен представить ОО для тестирования.

17.4.5.4 Элементы содержания и представления свидетельств

17.4.5.4.1 ATE_IND.2.1C

ОО должен быть пригоден для тестирования.

17.4.5.4.2 ATE_IND.2.2C

Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

17.4.5.5 Элементы действий оценщика

17.4.5.5.1 ATE_IND.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.4.5.5.2 ATE_IND.2.2E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

17.4.5.5.3 ATE_IND.2.3E

Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

17.4.6 ATE_IND.3 Полное независимое тестирование

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя
ATE_FUN.1 Функциональное тестирование

17.4.6.1 Цели

Целью является демонстрация выполнения всех функций безопасности в соответствии со спецификациями. Тестирование, проводимое оценщиком, включает в себя повторное выполнение всех тестов, выполненных разработчиком.

17.4.6.2 Замечания по применению

Разработчику следует предоставить оценщику материалы, необходимые для эффективного воспроизведения тестов, выполненных разработчиком. В состав этих материалов могут быть включены такие материалы, как машиночитаемая тестовая документация, тест-программы и т. д.

В данном компоненте требуется, чтобы оценщик повторил все тесты, выполненные разработчиком, как часть программы тестирования. Как и в предыдущем компоненте, оценщик должен провести дополнительные испытания, стремясь проверить ОО способом, отличным от использованного разработчиком. В случае, если тестирование, выполненное разработчиком, было исчерпывающим, для этого могут оставаться небольшие возможности.

17.4.6.3 Элементы действий разработчика

17.4.6.3.1 ATE_IND.3.1D

Разработчик должен представить ОО для тестирования.

17.4.6.4 Элементы содержания и представления свидетельств

17.4.6.4.1 ATE_IND.3.1C

ОО должен быть пригоден для тестирования.

17.4.6.4.2 ATE_IND.3.2C

Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

17.4.6.5 Элементы действий оценщика

17.4.6.5.1 ATE_IND.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

17.4.6.5.2 ATE_IND.3.2E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

17.4.6.5.3 ATE_IND.3.3E

Оценщик должен выполнить **все** тесты из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

18 Класс AVA. Оценка уязвимостей

Класс AVA «Оценка уязвимостей» связан с наличием пригодных для использования скрытых каналов и возможностью неправильного применения или конфигурирования ОО, а также возможностью преодоления вероятностных или перестановочных механизмов безопасности и использованием уязвимостей, вносимых при разработке или эксплуатации ОО.

Декомпозиция класса AVA «Оценка уязвимостей» на составляющие его семейства и иерархия компонентов этих семейств показаны на рисунке 15.

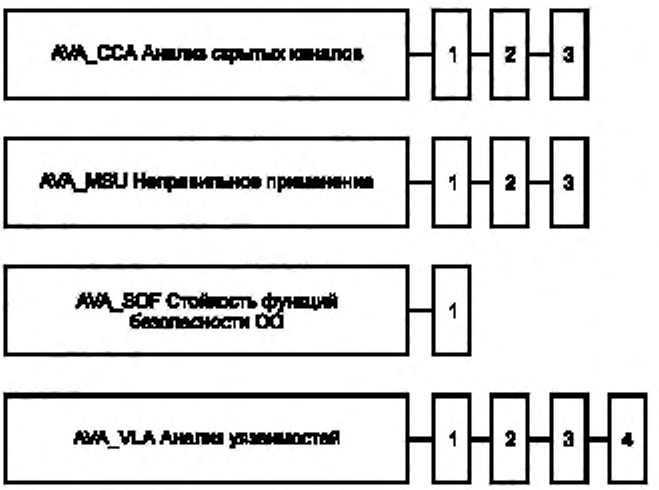


Рисунок 15 — Декомпозиция класса AVA: «Оценка уязвимостей»

18.1 Анализ скрытых каналов (AVA_CCA)

18.1.1 Цели

Анализ скрытых каналов выполняют с целью сделать заключение о существовании и потенциальной пропускной способности непредусмотренных каналов передачи сигналов (то есть неразрешенных информационных потоков), которые могут быть использованы.

Требования доверия связаны с угрозой существования непредусмотренных и пригодных для использования путей передачи сигналов, которые могут быть применены для нарушения ПФБ.

18.1.2 Ранжирование компонентов

Компоненты ранжированы по повышению строгости анализа скрытых каналов.

18.1.3 Замечания по применению

Оценка пропускной способности канала основана на неформальных технических оценках, а также на фактических результатах выполнения тестов.

Примеры предположений, на которых основан анализ скрытых каналов, могут включать в себя быстродействие процессора, системную или сетевую конфигурацию, размер памяти, размер кэш-памяти.

Выборочное подтверждение правильности анализа скрытых каналов путем тестирования дает оценщику возможность верифицировать любые аспекты анализа (такие как идентификация, оценка пропускной способности, удаление, мониторинг, сценарии применения). Это не требует демонстрации всех результатов анализа скрытых каналов.

Если в ЗБ не содержатся ПФБ управления информационными потоками, данное семейство требований доверия не применяется, поскольку оно относится только к ПФБ управления информационными потоками.

18.1.4 AVA_CCA.1 Анализ скрытых каналов

Зависимости: ADV_FSP.2 Полностью определенные внешние интерфейсы
ADV_IMP.2 Реализация ФБО
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.1.4.1 Цели

Цель состоит в том, чтобы идентифицировать скрытые каналы, которые можно обнаружить путем их неформального поиска.

18.1.4.2 Элементы действий разработчика

18.1.4.2.1 AVA_CCA.1.1D

Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

18.1.4.2.2 AVA_CCA.1.2D

Разработчик должен представить документацию анализа скрытых каналов.

18.1.4.3 Элементы содержания и представления свидетельств

18.1.4.3.1 AVA_CCA.1.1C

Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.

18.1.4.3.2 AVA_CCA.1.2C

Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

18.1.4.3.3 AVA_CCA.1.3C

Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.

18.1.4.3.4 AVA_CCA.1.4C

Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.

18.1.4.3.5 AVA_CCA.1.5C

Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.

18.1.4.4 Элементы действий оценщика

18.1.4.4.1 AVA_CCA.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.1.4.4.2 AVA_CCA.1.2E

Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО соответствует функциональным требованиям.

18.1.4.4.3 AVA_CCA.1.3E

Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.

18.1.5 AVA_CCA.2 Систематический анализ скрытых каналов

Зависимости: ADV_FSP.2 Полностью определенные внешние интерфейсы
ADV_IMP.2 Реализация ФБО
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.1.5.1 Цели

Цель состоит в том, чтобы идентифицировать скрытые каналы, которые можно обнаружить путем их систематического поиска.

18.1.5.2 Замечания по применению

Для систематического анализа скрытых каналов требуется, чтобы разработчик идентифицировал скрытые каналы структурированным и повторяемым образом, в противоположность идентификации скрытых каналов частным методом, применимым для конкретной ситуации.

18.1.5.3 Элементы действий разработчика

18.1.5.3.1 AVA_CCA.2.1D

Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

18.1.5.3.2 AVA_CCA.2.2D

Разработчик должен представить документацию анализа скрытых каналов.

18.1.5.4 Элементы содержания и представления свидетельств

18.1.5.4.1 AVA_CCA.2.1C

Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.

18.1.5.4.2 AVA_CCA.2.2C

Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

18.1.5.4.3 AVA_CCA.2.3C

Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.

18.1.5.4.4 AVA_CCA.2.4C

Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.

18.1.5.4.5 AVA_CCA.2.5C

Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.

18.1.5.4.6 AVA_CCA.2.6C

Документация анализа должна содержать свидетельство, что метод, использованный для идентификации скрытых каналов, является систематическим.

18.1.5.5 Элементы действий оценщика

18.1.5.5.1 AVA_CCA.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.1.5.5.2 AVA_CCA.2.2E

Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО соответствует функциональным требованиям.

18.1.5.5.3 AVA_CCA.2.3E

Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.

18.1.6 AVA_CCA.3 Исчерпывающий анализ скрытых каналов

Зависимости: ADV_FSP.2 Полностью определенные внешние интерфейсы
ADV_IMP.2 Реализация ФБО
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.1.6.1 Цели

Цель состоит в том, чтобы идентифицировать скрытые каналы, которые можно обнаружить путем их исчерпывающего поиска.

18.1.6.2 Замечания по применению

Для исчерпывающего анализа скрытых каналов требуется представление дополнительного свидетельства о том, что план идентификации скрытых каналов достаточен для утверждения и испробованы все возможные пути их исследования.

18.1.6.3 Элементы действий разработчика

18.1.6.3.1 AVA_CCA.3.1D

Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

18.1.6.3.2 AVA_CCA.3.2D

Разработчик должен представить документацию анализа скрытых каналов.

18.1.6.4 Элементы содержания и представления свидетельств

18.1.6.4.1 AVA_CCA.3.1C

Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.

18.1.6.4.2 AVA_CCA.3.2C

Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

18.1.6.4.3 AVA_CCA.3.3C

Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.

18.1.6.4.4 AVA_CCA.3.4C

Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.

18.1.6.4.5 AVA_CCA.3.5C

Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.

18.1.6.4.6 AVA_CCA.3.6C

Документация анализа должна содержать свидетельство того, что метод, использованный для идентификации скрытых каналов, является **исчерпывающим.**

18.1.6.5 Элементы действий оценщика

18.1.6.5.1 AVA_CCA.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.1.6.5.2 AVA_CCA.3.2E

Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО соответствует функциональным требованиям.

18.1.6.5.3 AVA_CCA.3.3E

Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.

18.2 Неправильное применение (AVA_MSU)

18.2.1 Цели

Семейство AVA_MSU позволяет установить, может ли ОО быть сконфигурирован или использован опасным образом так, чтобы администратор или пользователь ОО обоснованно считал бы его безопасным.

Целями являются:

a) минимизация вероятности конфигурирования или установки ОО опасным образом, исключающим возможность обнаружения пользователем или администратором;

b) минимизация риска ошибок, обусловленных человеческим фактором или иными причинами, в операциях, которые могут блокировать, отключить или помешать активизировать функции безопасности, приводя к необнаруженному опасному состоянию.

18.2.2 Ранжирование компонентов

Компоненты ранжированы по возрастанию числа свидетельств, представляемых разработчиком, и повышению строгости анализа.

18.2.3 Замечания по применению

Противоречивое, вводящее в заблуждение, неполное или необоснованное руководство может убедить пользователя в безопасности ОО при ее отсутствии, что может привести к уязвимостям.

Примером противоречия является наличие двух инструкций руководства, которые подразумевают различные выходные результаты при одних и тех же входных данных.

Примером введения в заблуждение является такая формулировка инструкции руководства, которую можно трактовать неоднозначно, причем одна из трактовок может привести к опасному состоянию.

Примером неполноты является список существенных физических требований безопасности, в котором опущен важный пункт, что приведет к игнорированию соответствующего требования администратором, считающим список полным.

Примером необоснованности является рекомендация следовать процедуре, приводящей к чрезмерной нагрузке по администрированию.

Требуется наличие документации руководств. Она может быть включена в руководства пользователя и администратора или представляться отдельно. При отдельном представлении оценщику следует подтвердить, что данная документация поставляется вместе с ОО.

18.2.4 AVA_MSU.1 Экспертиза руководств

Зависимости: ADO_IGS.1 Процедуры установки, генерации и запуска
ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.2.4.1 Цели

Цель состоит в том, чтобы обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться.

18.2.4.2 Элементы действий разработчика

18.2.4.2.1 AVA_MSU.1.1D

Разработчик должен представить руководства по применению ОО.

18.2.4.3 Элементы содержания и представления свидетельств

18.2.4.3.1 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.

18.2.4.3.2 AVA_MSU.1.2C

Руководства должны быть полными, понятными, непротиворечивыми и обоснованными.

18.2.4.3.3 AVA_MSU.1.3C

Руководства должны содержать список всех предположений относительно среды эксплуатации.

18.2.4.3.4 AVA_MSU.1.4C

Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль над процедурами, физическими мерами и персоналом).

18.2.4.4 Элементы действий оценщика

18.2.4.4.1 AVA_MSU.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.2.4.4.2 AVA_MSU.1.2E

Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения того, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

18.2.4.4.3 AVA_MSU.1.3E

Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

18.2.5 AVA_MSU.2 Подтверждение правильности анализа

Зависимости: ADO_IGS.1 Процедуры установки, генерации и запуска
ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.2.5.1 Цели

Цель состоит в том, чтобы обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться. В данном компоненте требуется анализ разработчиком руководств для повышения доверия к тому, что цель достигнута.

18.2.5.2 Элементы действий разработчика

18.2.5.2.1 AVA_MSU.2.1D

Разработчик должен представить руководства по применению ОО.

18.2.5.2.2 AVA_MSU.2.2D

Разработчик должен задокументировать анализ руководств.

18.2.5.3 Элементы содержания и представления свидетельств

18.2.5.3.1 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.

18.2.5.3.2 AVA_MSU.2.2C

Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

18.2.5.3.3 AVA_MSU.2.3C

Руководства должны содержать список всех предположений относительно среды эксплуатации.

18.2.5.3.4 AVA_MSU.2.4C

Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

18.2.5.3.5 AVA_MSU.2.5C

Документация анализа должна демонстрировать, что руководства полны.

18.2.5.4 Элементы действий оценщика

18.2.5.4.1 AVA_MSU.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.2.5.4.2 AVA_MSU.2.2E

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.

18.2.5.4.3 AVA_MSU.2.3E

Оценщик должен сделать независимое заключение о том, что использование руководств позволяет выявить все опасные состояния.

18.2.5.4.4 AVA_MSU.2.4E

Оценщик должен подтвердить, что документация анализа показывает, что руководства по безопасной эксплуатации предоставлены для всех режимов эксплуатации ОО.

18.2.6 AVA_MSU.3 Анализ и тестирование опасных состояний

Зависимости: ADO_IGS.1 Процедуры установки, генерации и запуска
ADV_FSP.1 Неформальная функциональная спецификация
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.2.6.1 Цели

Цель состоит в том, чтобы обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться. В данном компоненте требуется анализ разработчиком руководств для повышения доверия к тому, что цель достигнута, и этот анализ проверяется и подтверждается оценщиком путем тестирования.

18.2.6.2 Замечания по применению

В данном компоненте от оценщика требуется выполнить тестирование, позволяющее удостовериться в том, что при переходе ОО в опасное состояние последнее может быть легко выявлено. Указанное тестирование может рассматриваться как специфический аспект тестирования проникновения.

18.2.6.3 Элементы действий разработчика

18.2.6.3.1 AVA_MSU.3.1D

Разработчик должен представить руководства по применению ОО.

18.2.6.3.2 AVA_MSU.3.2D

Разработчик должен задокументировать анализ руководств.

18.2.6.4 Элементы содержания и представления свидетельств

18.2.6.4.1 AVA_MSU.3.1C

Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

18.2.6.4.2 AVA_MSU.3.2C

Руководства должны быть полными, понятными, непротиворечивыми и обоснованными.

18.2.6.4.3 AVA_MSU.3.3C

Руководства должны содержать список всех предположений относительно среды эксплуатации.

18.2.6.4.4 AVA_MSU.3.4C

Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

18.2.6.4.5 AVA_MSU.3.5C

Документация анализа должна демонстрировать, что руководства полны.

18.2.6.5 Элементы действий оценщика

18.2.6.5.1 AVA_MSU.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.2.6.5.2 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.

18.2.6.5.3 AVA_MSU.3.3E

Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

18.2.6.5.4 AVA_MSU.3.4E

Оценщик должен подтвердить, что документация анализа показывает, что руководства по безопасной эксплуатации предоставлены для всех режимов эксплуатации ОО.

18.2.6.5.5 AVA_MSU.3.5E

Оценщик должен выполнить независимое тестирование, чтобы сделать заключение, будет ли администратор или пользователь способен установить, руководствуясь документацией, что ОО конфигурирован и используется опасным образом.

18.3 Стойкость функций безопасности ОО (AVA_SOF)

18.3.1 Цели

Даже если функцию безопасности ОО нельзя обойти, отключить или исказить, в некоторых случаях существует возможность ее преодоления из-за уязвимости в концепции реализующих ее базовых механизмов безопасности. Для этих функций квалификация режима безопасности может быть проведена с использованием результатов количественного или статистического анализа режима безопасности указанных механизмов, а также усилий, требуемых для их преодоления. Квалификацию осуществляют в виде утверждения о стойкости функции безопасности ОО.

18.3.2 Ранжирование компонентов

В данном семействе имеется только один компонент.

18.3.3 Замечания по применению

Функции безопасности реализуются механизмами безопасности. Например, механизм пароля может использоваться при реализации функций идентификации и аутентификации.

Оценку стойкости функции безопасности ОО выполняют на уровне механизма безопасности, но ее результаты позволяют определить способность соответствующей функции безопасности противостоять идентифицированным угрозам.

При анализе стойкости функции безопасности ОО следует рассматривать, по меньшей мере, содержание всех поставляемых материалов ОО, включая ЗБ, с учетом намеченного оценочного уровня доверия.

18.3.4 AVA_SOF.1 Оценка стойкости функции безопасности ОО

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_HLD.1 Описательный проект верхнего уровня

18.3.4.1 Элементы действий разработчика

18.3.4.1.1 AVA_SOF.1.1D

Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.

18.3.4.2 Элементы содержания и представления свидетельств

18.3.4.2.1 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.

18.3.4.2.2 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.

18.3.4.3 Элементы действий оценщика

18.3.4.3.1 AVA_SOF.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.3.4.3.2 AVA_SOF.1.2E

Оценщик должен подтвердить, что утверждения относительно стойкости корректны.

18.4 Анализ уязвимостей (AVA_VLA)

18.4.1 Цели

Анализ уязвимостей позволяет сделать заключение, могут ли уязвимости, идентифицированные в процессе оценки устройства ОО и его ожидаемого функционирования или другими методами (например, из гипотезы о недостатках), быть использованы пользователями для нарушения ПБО.

При анализе уязвимостей рассматривают угрозы того, что пользователь будет в состоянии обнаружить недостатки, позволяющие получить несанкционированный доступ к ресурсам (например, данным), препятствовать выполнению ФБО и искажать их или же ограничивать санкционированные возможности других пользователей.

18.4.2 Ранжирование компонентов

Ранжирование основано на повышении строгости анализа уязвимостей разработчиком и оценщиком.

18.4.3 Замечания по применению

Разработчик выполняет анализ уязвимостей с тем, чтобы установить присутствие уязвимостей безопасности; при этом следует рассматривать, по меньшей мере, содержание всех поставляемых материалов ОО, включая ЗБ, с учетом намеченного оценочного уровня доверия. От разработчика требуется задокументировать решение по идентифицированным уязвимостям, чтобы позволить оценщику использовать эту информацию (если ее признают полезной) для поддержки независимого анализа уязвимостей оценщиком.

Анализ, проводимый разработчиком, предназначен для подтверждения невозможности использования идентифицированных уязвимостей безопасности в предполагаемой среде ОО и стойкости ОО к явным нападениям проникновения.

Под явными уязвимостями понимают те уязвимости, которые открыты для использования, требующего минимума понимания ОО, умений, технического опыта и ресурсов. Такие уязвимости могут быть подсказаны описанием интерфейса ФБО. К явным уязвимостям относятся известные из общедоступных источников (разработчику следует детально знать их) или полученные от органа оценки.

Систематический поиск уязвимостей требует, чтобы разработчик идентифицировал уязвимости структурированным и повторяемым способом, в противоположность их идентификации частными методами. Необходимо, чтобы свидетельство того, что поиск уязвимостей был систематическим, включало в себя идентификацию всей документации ОО, на которой был основан поиск недостатков.

Независимый анализ уязвимостей не ограничивается уязвимостями, идентифицированными разработчиком. Основная цель анализа, проводимого оценщиком, — сделать заключение, что ОО является стойким к нападениям проникновения со стороны нарушителя, обладающего низким (для AVA_VLA.2 «Независимый анализ уязвимостей»), умеренным (для AVA_VLA.3 «Умеренно стойкий») или высоким (для AVA_VLA.4 «Высоко стойкий») потенциалом нападения. Для достижения этой цели оценщик сначала проверяет возможности использования всех идентифицированных уязвимостей. Это осуществляется посредством тестирования проникновения. Оценщику следует принять на себя роль нарушителя с одним из указанных выше потенциалов нападения при попытке проникновения в ОО. Любое использование

уязвимостей таким нарушителем оценщику следует рассматривать как «явное нападение проникновения» (в отношении элементов AVA_VLA.*.2C в контексте компонентов AVA_VLA.2 «Независимый анализ уязвимостей», AVA_VLA.3 «Умеренно стойкий», AVA_VLA.4 «Высоко стойкий»).

18.4.4 AVA_VLA.1 Анализ уязвимостей разработчиком

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_HLD.1 Описательный проект верхнего уровня
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.4.4.1 Цели

Разработчик выполняет анализ уязвимостей с тем, чтобы установить присутствие явных уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

18.4.4.2 Замечания по применению

Оценщику следует предусмотреть выполнение дополнительных тестов для уязвимостей, выявленных при выполнении других частей оценки и потенциально пригодных для использования.

18.4.4.3 Элементы действий разработчика

18.4.4.3.1 AVA_VLA.1.1D

Разработчик должен выполнить анализ уязвимостей.

18.4.4.3.2 AVA_VLA.1.2D

Разработчик должен предоставить документацию анализа уязвимостей.

18.4.4.4 Элементы содержания и представления свидетельств

18.4.4.4.1 AVA_VLA.1.1C

Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска явных способов, которыми пользователь может нарушить ПБО.

18.4.4.4.2 AVA_VLA.1.2C

Документация анализа уязвимостей должна содержать описание решения в отношении явных уязвимостей.

18.4.4.4.3 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.

18.4.4.5 Элементы действий оценщика

18.4.4.5.1 AVA_VLA.1.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.4.4.5.2 AVA_VLA.1.2E

Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета явных уязвимостей.

18.4.5 AVA_VLA.2 Независимый анализ уязвимостей

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_IMP.1 Подмножество реализации ФБО
ADV_LLD.1 Описательный проект нижнего уровня
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.4.5.1 Цели

Разработчик выполняет анализ уязвимостей с тем, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, для того чтобы сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими низким потенциалом нападения.

18.4.5.2 Элементы действий разработчика

18.4.5.2.1 AVA_VLA.2.1D

Разработчик должен выполнить анализ уязвимостей.

18.4.5.2.2 AVA_VLA.2.2D

Разработчик должен предоставить документацию анализа уязвимостей.

18.4.5.3 Элементы содержания и представления свидетельств

18.4.5.3.1 AVA_VLA.2.1C

Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска способов, которыми пользователь может нарушить ПБО.

18.4.5.3.2 AVA_VLA.2.2C

Документация анализа уязвимостей должна содержать описание решения в отношении **идентифицированных** уязвимостей.

18.4.5.3.3 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.

18.4.5.3.4 AVA_VLA.2.4C

Документация анализа уязвимостей должна содержать логическое обоснование того, что ОО с идентифицированными уязвимостями устойчив по отношению к очевидным атакам проникновения.

18.4.5.4 Элементы действий оценщика

18.4.5.4.1 AVA_VLA.2.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.4.5.4.2 AVA_VLA.2.2E

Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета **идентифицированных** уязвимостей.

18.4.5.4.3 AVA_VLA.2.3E

Оценщик должен выполнить независимый анализ уязвимостей.

18.4.5.4.4 AVA_VLA.2.4E

Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

18.4.5.4.5 AVA_VLA.2.5E

Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим низким потенциалом нападения.

18.4.6 AVA_VLA.3 Умеренно стойкий

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_IMP.1 Подмножество реализации ФБО
ADV_LLD.1 Описательный проект нижнего уровня
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.4.6.1 Цели

Разработчик выполняет анализ уязвимостей с тем, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, для того чтобы сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими умеренным потенциалом нападения.

18.4.6.2 Элементы действий разработчика

18.4.6.2.1 AVA_VLA.3.1D

Разработчик должен выполнить анализ уязвимостей.

18.4.6.2.2 AVA_VLA.3.2D

Разработчик должен предоставить документацию анализа уязвимостей.

18.4.6.3 Элементы содержания и представления свидетельств

18.4.6.3.1 AVA_VLA.3.1C

Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска способов, которыми пользователь может нарушить ПБО.

18.4.6.3.2 AVA_VLA.3.2C

Документация анализа уязвимостей должна содержать описание решения в отношении идентифицированных уязвимостей.

18.4.6.3.3 AVA_VLA.3.3C

Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

18.4.6.3.4 AVA_VLA.3.4C

Документация анализа уязвимостей должна содержать логическое обоснование, что ОО с идентифицированными уязвимостями устойчив по отношению к очевидным атакам проникновения.

18.4.6.3.5 AVA_VLA.3.5C

Документация анализа уязвимостей должна показывать, что поиск уязвимостей является систематическим.

18.4.6.4 Элементы действий оценщика

18.4.6.4.1 AVA_VLA.3.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.4.6.4.2 AVA_VLA.3.2E

Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

18.4.6.4.3 AVA_VLA.3.3E

Оценщик должен выполнить независимый анализ уязвимостей.

18.4.6.4.4 AVA_VLA.3.4E

Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

18.4.6.4.5 AVA_VLA.3.5E

Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

18.4.7 AVA_VLA.4 Высокостойкий

Зависимости: ADV_FSP.1 Неформальная функциональная спецификация
ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
ADV_IMP.1 Подмножество реализации ФБО
ADV_LLD.1 Описательный проект нижнего уровня
AGD_ADM.1 Руководство администратора
AGD_USR.1 Руководство пользователя

18.4.7.1 Цели

Разработчик выполняет анализ уязвимостей с тем, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, для того чтобы сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими высоким потенциалом нападения.

18.4.7.2 Элементы действий разработчика

18.4.7.2.1 AVA_VLA.4.1D

Разработчик должен выполнить анализ уязвимостей.

18.4.7.2.2 AVA_VLA.4.2D

Разработчик должен предоставить документацию анализа уязвимостей.

18.4.7.3 Элементы содержания и представления свидетельств

18.4.7.3.1 AVA_VLA.4.1C

Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска способов, которыми пользователь может нарушить ПБО.

18.4.7.3.2 AVA_VLA.4.2C

Документация анализа уязвимостей должна содержать описание решения в отношении идентифицированных уязвимостей.

18.4.7.3.3 AVA_VLA.4.3C

Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

18.4.7.3.4 AVA_VLA.4.4C

Документация анализа уязвимостей должна содержать логическое обоснование, что ОО с идентифицированными уязвимостями устойчив по отношению к очевидным атакам проникновения.

18.4.7.3.5 AVA_VLA.4.5C

Документация анализа уязвимостей должна показывать, что поиск уязвимостей является систематическим.

18.4.7.3.6 AVA_VLA.4.6C

Документация анализа уязвимостей должна содержать логическое обоснование, что анализ полностью учитывает все поставляемые материалы ОО.

18.4.7.4 Элементы действий оценщика

18.4.7.4.1 AVA_VLA.4.1E

Оценщик должен подтвердить, что представленная информация соответствует всем требованиям к содержанию и представлению свидетельств.

18.4.7.4.2 AVA_VLA.4.2E

Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

18.4.7.4.3 AVA_VLA.4.3E

Оценщик должен выполнить независимый анализ уязвимостей.

18.4.7.4.4 AVA_VLA.4.4E

Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

18.4.7.4.5 AVA_VLA.4.5E

Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **высоким** потенциалом нападения.

Приложение А
(справочное)

Перекрестные ссылки между компонентами доверия

Зависимости между компонентами, приведенные в разделах 8 — 18, являются прямыми зависимостями между компонентами доверия.

Прямые и косвенные зависимости между компонентами доверия по классам доверия представлены в таблицах А.1 — А.9. Компоненты, от которых зависят какие-либо другие компоненты доверия, указаны в заголовках столбцов. Кроме того, каждый компонент доверия указан в заголовке какой-либо строки. Конкретное значение в ячейке таблицы указывает на то, требуется ли прямо (символ «X») или косвенно (символ «—») компонент, указанный в заголовке столбца, для компонента, указанного в заголовке строки. Если в ячейке нет никаких символов, то компонент, указанный в заголовке строки, не зависит от компонента, указанного в заголовке столбца.

Таблица А.1 — Таблица зависимостей класса ACM «Управление конфигурацией»

	ACM_CAP.3	ALC_DVS.1	ALC_DVS.2
ACM_AUT.1	X	—	
ACM_AUT.2	X	—	
ACM_CAP.1			
ACM_CAP.2			
ACM_CAP.3		X	
ACM_CAP.4		X	
ACM_CAP.5			X
ACM_SCP.1	X	—	
ACM_SCP.2	X	—	
ACM_SCP.3	X	—	

Таблица А.2 — Таблица зависимостей класса ADO «Поставка и эксплуатация»

	ACM_CAP.3	ADV_FSP.1	ADV_RCR.1	AGD_ADM.1	ALC_DVS.1
ADO_DEL.1					
ADO_DEL.2	X				—
ADO_DEL.3	X				—
ADO_IGS.1		—	—	X	
ADO_IGS.2		—	—	X	

Таблица А.3 — Таблица зависимостей класса ADV «Разработка»

	ADV_FSP.1	ADV_FSP.3	ADV_FSP.4	ADV_HLD.2	ADV_HLD.3	ADV_HLD.5	ADV_IMP.1	ADV_IMP.2	ADV_INT.1	ADV_LLD.1	ADV_RCR.1	ADV_RCR.2	ADV_RCR.3	ALC_TAT.1
ADV_FSP.1											X			
ADV_FSP.2											X			
ADV_FSP.3											X			
ADV_FSP.4											X			
ADV_HLD.1	X										X			
ADV_HLD.2	X										X			
ADV_HLD.3		X									—	X		
ADV_HLD.4		X									—	X		
ADV_HLD.5			X								—		X	
ADV_IMP.1	—			—			—			X	X			X
ADV_IMP.2	—			—			—			X	—			X
ADV_IMP.3	—			—			—		X	X	X			X

Окончание таблицы А. 3

	ADV_FSP.1	ADV_FSP.3	ADV_FSP.4	ADV_HLD.2	ADV_HLD.3	ADV_HLD.5	ADV_IMP.1	ADV_IMP.2	ADV_INT.1	ADV_LLD.1	ADV_RCR.1	ADV_RCR.2	ADV_RCR.3	ALC_TAT.1
ADV_INT.1	—			—			X			X	—			—
ADV_INT.2	—			—			X			X	—			—
ADV_INT.3	—			—			—	X		X	—			—
ADV_LLD.1	—			X							X			
ADV_LLD.2		—			X						—	X		
ADV_LLD.3			—			X					—		X	
ADV_RCR.1														
ADV_RCR.2														
ADV_RCR.3														
ADV_SPM.1	X										—			
ADV_SPM.2	X										—			
ADV_SPM.3	X										—			

Таблица А.4 — Таблица зависимостей класса AGD «Руководства»

	ADV_FSP.1	ADV_RCR.1
AGD_ADM.1	X	—
AGD_USR.1	X	—

Таблица А.5 — Таблица зависимостей класса ALC «Поддержка жизненного цикла»

	ADV_FSP.1	ADV_HLD.2	ADV_IMP.1	ADV_LLD.1	ADV_RCR.1	ALC_TAT.1
ALC_DVS.1						
ALC_DVS.2						
ALC_FLR.1						
ALC_FLR.2						
ALC_FLR.3						
ALC_LCD.1						
ALC_LCD.2						
ALC_LCD.3						
ALC_TAT.1	—	—	X	—	—	—
ALC_TAT.2	—	—	X	—	—	—
ALC_TAT.3	—	—	X	—	—	—

Таблица А.6 — Таблица зависимостей класса APE «Оценка профиля защиты»

	APE_DES.1	APE_ENV.1	APE_INT.1	APE_OBJ.1	APE_REQ.1
APE_DES.1	—	X	X	X	X
APE_ENV.1					
APE_INT.1	X	X	—	X	X
APE_OBJ.1		X			
APE_REQ.1		—		X	
APE_SRE.1		—		—	X

Таблица А.7 — Таблица зависимостей класса ASE «Оценка задания по безопасности»

	ASE_DES.1	ASE_ENV.1	ASE_INT.1	ASE_OBJ.1	ASE_PPC.1	ASE_REQ.1	ASE_TSS.1
ASE_DES.1	—	X	X	X	X	X	X
ASE_ENV.1							
ASE_INT.1	X	X	—	X	X	X	X
ASE_OBJ.1		X					
ASE_OBJ.1		—		X		X	
ASE_REQ.1		—		X			
ASE_SRE.1		—		—		X	
ASE_TSS.1		—		—		X	

Таблица А.8 — Таблица зависимостей класса ATE «Тестирование»

	ADV_FSP.1	ADV_FSP.2	ADV_HLD.1	ADV_HLD.2	ADV_IMP.1	ADV_IMP.2	ADV_LLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_TAT.1	ATE_FUN.1
ATE_COV.1	X							—				X
ATE_COV.2	X							—				X
ATE_COV.3		X						—				X
ATE_DPT.1	—		X					—				X
ATE_DPT.2	—			X			X	—				X
ATE_DPT.3	—			X	—	X	X	—			—	X
ATE_FUN.1												
ATE_FUN.2												
ATE_IND.1	X							—	X	X		
ATE_IND.2	X							—	X	X		X
ATE_IND.3	X							—	X	X		X

Таблица А.9 — Таблица зависимостей класса AVA «Оценка уязвимостей»

	ADO_IGS.1	ADV_FSP.1	ADV_FSP.2	ADV_HLD.1	ADV_HLD.2	ADV_IMP.1	ADV_IMP.2	ADV_LLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ALC_TAT.1
AVA_CCA.1		—	X		—	—	X	—	—	X	X	—
AVA_CCA.2		—	X		—	—	X	—	—	X	X	—
AVA_CCA.3		—	X		—	—	X	—	—	X	X	—
AVA_MSU.1	X	X							—	X	X	
AVA_MSU.2	X	X							—	X	X	
AVA_MSU.3	X	X							—	X	X	
AVA_SOF.1		X		X					—			
AVA_VLA.1		X		X					—	X	X	
AVA_VLA.2		X			X	X		X	—	X	X	—
AVA_VLA.3		X			X	X		X	—	X	X	—
AVA_VLA.4		X			X	X		X	—	X	X	—

Приложение В
(справочное)

Перекрестные ссылки ОУД и компонентов доверия

Сводка оценочных уровней доверия, показывающая взаимосвязь между оценочными уровнями доверия и классами, семействами и компонентами доверия, приведена в таблице В.1.

Таблица В.1 — Сводка оценочных уровней доверия

Класс доверия	Семейство доверия	Компоненты доверия из оценочного уровня доверия						
		ОУД1	ОУД2	ОУД3	ОУД4	ОУД5	ОУД6	ОУД7
Управление конфигурацией	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Поставка и эксплуатация	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Разработка	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Руководства	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Поддержка жизненного цикла	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Тестирование	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Оценка уязвимостей	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	4

Приложение С
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица С.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 (IDT)
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 (IDT)
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичный стандарт.	

УДК 681.324:006.354 ОКС 35.040 П85

Ключевые слова: информационная технология, задание по безопасности, профиль защиты, объект оценки, критерии оценки безопасности, функция безопасности, требования доверия к безопасности

Редактор *В. Н. Колысов*
Технический редактор *Н. С. Гришанова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *В. Н. Романовой*

Сдано в набор 13.03.2009. Подписано в печать 16.06.2009. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 13,49. Уч.-изд. л. 13,90. Тираж 278 экз. Зак. 502.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва. Гранатный пер., 4.
gost.e-ecolog.ru @gostinfo.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.

gost.e-ecolog.ru