*Проект*

Изображение Государственного Герба Республики Казахстан

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

Информационные технологии

Методы и средства обеспечения безопасности

Критерии оценки безопасности информационных технологий

Часть 3

ТРЕБОВАНИЯ ДОВЕРИЯ К БЕЗОПАСНОСТИ

**СТ РК ISO/IEC 15408-3**

*(ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3: Security assurance components, IDT)*

*Настоящий проект стандарта*

*не подлежит применению до его утверждения*

**Комитет технического регулирования и метрологии**

**Министерства торговли и интеграции Республики Казахстан**

**(Госстандарт)**

**Астана**

**Предисловие**

**1 ПОДГОТОВЛЕН И ВНЕСЕН** Республиканским государственным предприятием на праве хозяйственного ведения «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан

**2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ** Приказом Председателя Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан № \_\_ от « » \_\_\_\_ 20\_\_года.

**3** Настоящий стандарт идентичен международному стандарту ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3: Security assurance components (Информационные технологии. Методы и средства обеспечения безопасности. критерии оценки безопасности информационных технологий. Часть 3 Требования доверия к безопасности)

Международный стандарт разработан техническим комитетом ISO/IEC JTC 1/SC 27

Перевод с английского языка (en)

Официальный экземпляр международного стандарта, на основе которого разработан настоящий стандарт, и официальные экземпляры международных стандартов, на которые даны ссылки, имеются в Едином государственном фонде нормативных технических документов

Официальной версией является текст на государственном и русском языке

Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств приведены в Приложении В.А

Степень соответствия – идентичная (IDT)

**4 ВВЕДЕН ВПЕРВЫЕ**

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном каталоге «Документы по стандартизации», а текст изменений и поправок – в периодически издаваемых информационных каталогах «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном каталоге «Национальные стандарты».*

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан.

**Содержание**

Введение

1 Область применения

2 Нормативные ссылки

3 Термины и определения

4 Обзор

5 Парадигма доверия

6 Компоненты обеспечения безопасности

7 Класс АРЕ: Оценка профиля защиты

8 Класс ASE: Оценка задания по безопасности

9 Класс ASE: оценка задачи безопасности

10 Класс ADV: Разработка

11 Класс AGD: Руководства

12 Класс ALC: Поддержка жизненного цикла

13 Класс АТЕ: Тестирование

14 Класс AVA: Оценка уязвимостей

15 Класс АСО: Композиция

Приложение А (*информационное*) Разработка (ADV)

Приложение В (*информационное*) Композиция (АСО)

Приложение С (*информационное*) Перекрестные ссылки между компонентами доверия

Библиография

Приложение В.А (*информационное*) Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств

Введение

Требования доверия безопасности, как установлено в настоящем стандарте, являются основой для требований обеспечения безопасности, выраженных в пакете обеспечения безопасности, профиле защиты (PP), модуле PP, конфигурации PP или задание безопасности (ST).

Данные требования устанавливают стандартный способ выражения требований доверия к TOE. В настоящем стандарте каталогизирован набор компонентов доверия, семейств и классов. Он также определяет критерии оценки для PP, конфигураций PP, модулей PP и ST.

В аудиторию этого документа входят потребители, разработчики, технические рабочие группы, оценщики безопасных ИТ-продуктов и другие. ISO/IEC 15408-1:2022, раздел 5 предоставляет дополнительную информацию о целевой аудитории серии   
ISO/IEC 15408, а также об использовании серии ISO/IEC 15408 группами, составляющими целевую аудиторию. Эти группы могут использовать этот документ следующим образом:

а) Потребители, которые используют этот документ при выборе компонентов для выражения требований доверия для удовлетворения целей безопасности, выраженных в ПЗ или ЗБ, определяют требуемые уровни обеспечения безопасности TOE.

b) Разработчики, которые реагируют на фактические или предполагаемые требования безопасности потребителей при построении TOE, ссылаются на этот документ при интерпретации требований доверия и определении подходов к обеспечению доверия к TOE.

c) Оценщики, которые используют требования доверия, определенные в настоящем документе, в качестве обязательной формулировки критериев оценки при определении доверия к TOE и при оценке ПЗ и ЗБ.

Примечание – В некоторых случаях в этом документе используется жирный шрифт и курсив, чтобы отличать термины от остального текста.

Отношения между компонентами внутри семейства выделены жирным шрифтом. Это соглашение требует использования жирного шрифта для всех новых требований. Для иерархических компонентов требования выделяются жирным шрифтом, если они расширены или изменены сверх требований предыдущего компонента. Кроме того, любые новые или улучшенные разрешенные операции, выходящие за рамки предыдущего компонента, также выделяются жирным шрифтом.

Использование курсива указывает на текст, имеющий точное значение. В требованиях обеспечения безопасности принято использовать специальные глаголы, относящиеся к оценке.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

Информационные технологии

Методы и средства обеспечения безопасности

Критерии оценки безопасности информационных технологий

Часть 3

ТРЕБОВАНИЯ ДОВЕРИЯ К БЕЗОПАСНОСТИ

**Дата введения\_\_\_\_\_\_\_\_\_\_\_\_**

## **1 Область применения**

Настоящий стандарт устанавливает требования к обеспечению качества серии ISO/IEC 15408. Настоящий стандарт включает в себя отдельные компоненты доверия, из которых состоят уровни доверия оценки и другие пакеты, содержащиеся в ISO/IEC 15408-5, а также критерии оценки профилей защиты (PPs), конфигураций PP, модулей PP и целей безопасности (STs).

## **2 Нормативные ссылки**

Для применения настоящего стандарта необходимы, следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения)

ISO/IEC 15408-1:2022 Information security. Evaluation criteria for IT security. Part 1: Introduction and general model (Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 1: Введение и общая модель).

ISO/IEC 15408-2 Information security. Evaluation criteria for IT security. Part 2: Security functional components (Информационные технологии. Методы обеспечения безопасности. Критерии оценки безопасности в IT. Часть 2: Функциональные компоненты безопасности).

ISO/IEC 15408-4 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 4: Framework for the specification of evaluation methods and activities (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности IT. Часть 4. Структура спецификации методов и действий оценки).

ISO/IEC 15408-5 Information security. Evaluation criteria for IT security. Part 5: Pre-defined packages of security requirements (Информационная безопасность. Критерии оценки безопасности IT. Часть 5. Заранее определенные пакеты требований безопасности).

ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Methodology for IT security evaluation (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Методология оценки IT-безопасности).

ISO/IEC IEEE 24765 Systems and software engineering. Vocabulary (Системная и программная инженерия. Словарь).

## **3 Термины и определения**

В настоящем стандарте применяются термины по ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045 и ISO/IEC IEEE 24765, а также следующие термины с соответствующими определениями:

Примечание – ISO и IEC поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

- ISO Онлайн платформа для просмотра: доступна на сайте https://www.iso.org/obp

- Электропедия IEC: доступно на сайте https://www.electropedia.org/

3.1 Процедуры приемки (acceptance procedure):Процедуры, которым следуют в целях приемки вновь созданных или модифицированных элементов конфигурации (3.3) как частей (TOE) или для перевода их на следующий этап жизненного цикла.

Примечания

1 Эти процедуры идентифицируют роли лиц, ответственных за приемку, и критерии, применяемые для принятия решения о приемке.

2 Существует несколько типов ситуаций приемки, некоторые из которых могут частично перекрывать друг друга:

a) приемка элемента под управление системы управления конфигурацией, в частности в рамках процесса интеграции;

b) перевод элементов конфигурации на следующую стадию жизненного цикла на каждом этапе создания TOE.

***Примеры***

1 Модуль, подсистема, контроль качества конечного TOE;

c) приемка после перемещения элементов конфигурации;

2 Части TOE или «Заготовок» продуктов между различными местами разработки (3.15);

d) приемка после поставки (3.14) TOE потребителю;

e) после интеграции TOE.

3 Включение в TOE программного обеспечения, встроенных программ и аппаратных компонентов из других источников.

**3.2 Действие** (action): Элемент действия оценщика или разработчика настоящего стандарта.

Примечание – Данные действия либо однозначно определены как действия оценщика, либо не однозначно вытекают из действий разработчика (подразумеваемые действия оценщика) в компонентах доверия настоящего стандарта.

**3.3 Элемент конфигурации** (configuration item): Объект, находящийся под управлением системы конфигурацией в течение разработки TOE (3.15).

Примечание – Элементами конфигурации могут быть либо части TOE, либо объекты, имеющие отношение к разработке TOE, такие как документы для оценки, инструментальные средства разработки. Элементы управления конфигурацией могут быть напрямую сохранены в системе управления конфигурацией (например файлы) или путем ссылки на них (например, части программного обеспечения) с указанием их версии.

**3.4 Список конфигурации** (configuration list): Документ с выходными данными системы управления конфигурацией (3.8), в котором перечисляются все элементы конфигурации (3.3) для конкретного продукта с указанием точной версии каждого элемента конфигурации, актуальной для конкретной версии продукта в целом.

Примечание – Данный список позволяет отличать элементы, относящиеся к оцененной версии продукта, от других версий этих элементов, относящихся к другим версиям данного продукта. Окончательный список управления конфигурацией является конкретным документом для конкретной версии конкретного продукта. (Данный список может быть документом в электронном виде в рамках инструментальных средств управления конфигурацией. В этом случае он может рассматриваться в качестве определенного представления системы CM или части системы, а не в качестве выходных данных системы. Вместе с тем, для практического использования при оценке список конфигурации будут предположительно поставляться как часть документации для оценки.) Список конфигурации определяет элементы, на которые распространяются требования по управлению конфигурацией из ALC\_CMC.

**3.5 Управление конфигурацией, СМ** (configuration management, CM): Вид деятельности, предусматривающий техническое и административное руководство и контроль, направленные на идентификацию и документирование функциональных и физических характеристик элементов конфигурации (3.3), контроль изменений этих характеристик, регистрацию и представление информации о состоянии обработки и реализации изменений, а также - верификацию соответствия установленным требованиям.

Примечание – Взято из ISO/IEC IEEE 24765:2017, 3.779 1.

**3.6 Документация управления конфигурацией** (configuration management documentation/ CM documentation): Вся документация CM, включая входные данные CM, список CM (список конфигурации), записи системы CM, план CM и документацию по применению CM.

**3.7 Свидетельство управления конфигурацией** (configuration management evidence): Все, что может быть использовано для приобретения уверенности в правильности функционирования системы CM.

***Пример –*** Выходные данные CM (3.8), обоснования, предоставленные разработчиком, результаты контроля, испытаний и интервьюирования, полученные оценщиком в процессе непосредственного посещения места разработки.

**3.8 Выходные данные управления конфигурацией** (configuration management output): Результаты, связанные с управлением конфигурацией, созданные или обеспеченные системой управления конфигурацией.

Примечание ***–*** Эти результаты, связанные с управлением конфигурацией, могут иметь вид документов (например, заполненные бумажные формы, записи системы управления конфигурацией (3.11), данные журналов аудита, выходные данные на бумажном носителе или электронной форме), так и в виде действий (например, меры выполнения человеком инструкций по управлению конфигурацией). Примерами таких выходных данных управления конфигурацией являются списки конфигурации (3.4), план управления конфигурацией (3.9) и/или виды действий в течение жизненного цикла продукта.

**3.9 План управления конфигурацией** (configuration management plan): Описание порядка использования системы управления конфигурацией для конкретного TOE.

Примечание – Цель выпуска плана управления конфигурацией - дать персоналу ясное представление, что он должен делать. С точки зрения системы управления конфигурацией в целом, план можно рассматривать как выходной документ (так как он мог быть создан как один из результатов применения системы управления конфигурацией). С точки зрения конкретного проекта, план представляет собой документ по применению, используемый членами проектной команды для того, чтобы понимать шаги, которые они должны выполнить в ходе проекта. План управления конфигурацией определяет использование системы УК для конкретного продукта; эта же система CM может использоваться в разной степени и для других продуктов. Это означает, что план управления конфигурацией определяет и описывает выходные данные системы управления конфигурации, используемой компанией в процессе разработки TOE (3.15).

***Пример –*** Структура и содержание плана управления конфигурацией представлены в ISO 10007:2017, Приложение А.

**3.10 Система управления конфигурацией** (configuration management system): Совокупность процедур и инструментальных средств (включая их документацию), используемая разработчиком для разработки и поддержки конфигураций его продуктов в течение их жизненных циклов.

Примечание – Системы управления конфигурацией могут обладать различными степенями строгости и функциями. На более высоких уровнях системы управления конфигурацией могут быть автоматизированы и иметь механизмы устранения недостатков, контроля изменений и другие механизмы сопровождения.

**3.11 Записи системы управления конфигурацией** (configuration management system record): Выходные данные, создаваемые в процессе функционирования системы управления конфигурацией и документирующие важные виды деятельности по управлению конфигурацией.

***Пример –*** Записи системы управления конфигурацией являются формы контроля изменений элементов конфигурации или формы санкционирования доступа к элементам конфигурации.

**3.12 Инструментальные средства управления конфигурацией** (configuration management tool): Управляемые вручную или автоматизированные инструментальные средства, реализующие или поддерживающие систему управления конфигурацией.

***Пример –*** Инструментальные средства управления версиями частей TOE.

**3.13 Документация по применению управления конфигурацией** (configuration management usage documentation): Часть системы управления конфигурацией, в которой описаны способы определения и применения системы управления конфигурацией путем использования, например руководств, инструкций и/или документации инструментальных средств и процедур.

**3.14 Поставка** (delivery): Передача завершенного (TOE) из производственной (3.24) среды потребителю.

Примечание – Данный этап жизненного цикла продукта может включать упаковку и хранение в месте разработки (3.15), но не охватывает перемещение незавершенного TOE или частей TOE между различными разработчиками или разными местами разработки.

**3.15 Разработка** (development): Стадия жизненного цикла продукта, связанная с созданием представления реализации TOE.

Примечание – В требованиях класса ALC термин "разработка" и связанные с ним термины (разработчик, разрабатывать) понимаются в более широком смысле и охватывают разработку и производство (3.24).

**3.16 Обнаруженные потенциальные уязвимости** (encountered potential vulnerability): Потенциально слабые места TOE, идентифицированные оценщиком при выполнении видов деятельности по оценке, которые могли бы быть использованы для нарушения SFRs.

**3.17 Результаты оценки** (evaluation deliverable): Ресурс, требуемый от спонсора или разработчика оценщиком или органом по оценке для выполнения одной или нескольких действий по оценке или надзору за оценкой.

**3.18 Пригодная для использования уязвимость** (exploitable vulnerability): Слабое место TOE, которое может быть использовано для нарушения SFRs в среде функционирования TOE.

**3.19 Установка** (installation): Процедура, выполняемая человеком-пользователем, по внедрению TOE в его среду функционирования и приведению его в рабочее состояние.

Примечание – Эту операцию обычно выполняют только один раз после получения и приемки TOE. Как ожидается, TOE приводят к конфигурации, допускаемой ЗБ. Если подобные процессы должны выполняться разработчиком, то они обозначаются как «генерация» в рамках ALC «Поддержка жизненного цикла». Если для TOE требуется первоначальный запуск, который не нужно регулярно повторять, то этот процесс относят к категории «установка».

**3.20 Модель жизненного цикла** (life-cycle model): Структура, содержащая процессы, действия и задачи, связанные с разработкой (3.15), эксплуатацией и обслуживанием продукта, охватывающая срок службы системы от определения ее требований до прекращения ее использования.

Примечание – Взято из ISO/IEC IEEE 24765:2017 3.2219 2.

**3.21 Функционирование (эксплуатация)** (operation): Стадия использования TOE, включающая «обычное использование», администрирование и поддержку TOE после поставки (3.14) и подготовки (3.23).

**3.22 Потенциальная уязвимость** (potential vulnerability): Предполагаемая, но не подтвержденная слабость TOE.

Примечание – Предположение основывают на теоретически допустимой схеме нападения для нарушения SFRs.

**3.23 Подготовка** (preparation): Вид деятельности на стадии жизненного цикла некоторого продукта, включающий приемку потребителем поставленного TOE и его установку (3.19).

Примечание – Подготовка может включать такие действия как загрузка, инициализация и приведение ОО в состояние готовности к функционированию.

**3.24 Производство** (production): Стадия жизненного цикла «производство» следует после стадии «разработка» и заключается в преобразовании представления реализации в реализацию конкретного TOE, т. е. в состояние, приемлемое для поставки (3.14) потребителю.

Примечание – Эта стадия может включать изготовление, интеграцию, генерацию, внутреннюю транспортировку, хранение и маркировку ОО.

**3.25 Остаточная уязвимость** (residual vulnerability): Слабое место TOE, которое не может быть использовано в среде функционирования TOE, но которое может быть использовано для нарушения ФТБ нарушителем с более высоким потенциалом нападения, чем предполагается в среде функционирования TOE.

**3.26 Поддействие** (sub-activity): применение компонента доверия ISO/IEC 15408-3.

Примечание – Ряд доверий не рассматриваются явно в серии стандартов ISO/IEC 15408, поскольку оценки проводятся на одном компоненте доверия из семейства доверия.

**3.27 Период времени до воздействия** (time period to exposure): Интервал времени, в течение которого элемент участвует в ИТ-системе и может быть атакован.

**3.28 Уязвимость** (vulnerability): Слабое место TOE, которое может быть использовано для нарушения ФТБ в некоторой среде.

**3.29 Окно возможности** (window of opportunity): Период времени, в течение которого злоумышленник имеет доступ к цели оценки (TOE).

## **4** **Обзор**

В разделе 5 описывается парадигма, используемая в требованиях обеспечения безопасности данного раздела ISO/IEC 15408.

В разделе 6 описывается структура представления классов доверия, семейств, компонентов, уровней обеспечения доверия вместе с их взаимодействием и структуры составленных пакетов доверия. Также приведена характеристика классов доверия и семейств, описываемых в разделах с 7 по 15.

В разделах с 7 по 15 приводятся подробные определения классов обеспечения качества этого документа.

Приложение А содержит дополнительные пояснения и примеры концепций, лежащих в основе класса Development.

В приложении B приведено объяснение понятий, лежащих в основе объекта оценки (TOE) и класса Компонента.

В приложении C приведена сводка зависимостей между компонентами доверия.

## **5 Парадигма доверия**

**5.1 Общие положения**

Целью данного раздела является определение принципов, лежащих в основе подхода ISO/IEC 15408 к доверию. Понимание данного положения позволит пользователю понять принцип построения требований доверия в ISO/IEC 15408.

**5.2 Основные принципы ISO/IEC 15408**

Принцип ISO/IEC 15408 заключается в том, что угрозы безопасности и обязательства в отношении политики безопасности организации должны быть четко сформулированы, а предлагаемые меры безопасности должны предельно соответствовать их намеченной цели.

Кроме того, следует принять меры, снижающие вероятность уязвимости, способность применять (то есть преднамеренно использовать или ненамеренно запускать) уязвимость и степень ущерба, который может быть причинен в результате уязвимости. Кроме того, должны быть приняты меры, способствующие последующему выявлению уязвимостей и устранению, смягчению и/или уведомлению о том, что уязвимость была использована или запущена.

**5.3 Подход к доверию**

**5.3.1 Общие положения**

Подход стандартов ISO/IEC 15408 заключается в обеспечении доверия на основе оценки (активного расследования) IT-продукта, которому следует доверять. Оценка являлась традиционным средством обеспечения доверия и основой для предыдущих документов оценки. В соответствии с существующими подходами ISO/IEC 15408 придерживается той же философии. Согласно ISO/IEC 15408 экспертам-оценщикам предлагается оценить достоверность документации и IT-продукта, уделяя повышенное внимание масштабам, глубине и строгости.

Серия стандартов ISO/IEC 15408 не исключает, и не разъясняет в отношении других способов получения доверия. Продолжаются исследования в отношении альтернативных путей получения доверия. По мере появления зрелых альтернативных подходов в результате научно-исследовательской деятельности, они будут рассмотрены для включения в ISO/IEC 15408, который построен так, чтобы обеспечить их будущее введение.

**5.3.2 Значение уязвимости**

Предполагается, что есть агенты угроз, которые будут активно стремиться использовать возможности для нарушения безопасности как для незаконной прибыли, так и для благих намерений, но, тем не менее, ненадежных действий. Угрожающие агенты также могут случайно запускать уязвимости безопасности, наносящие ущерб организации. В связи с необходимостью обработки конфиденциальной информации и отсутствием продуктов с достаточно высоким доверием существует значительный риск из-за сбоев IT. Поэтому вполне вероятно, что нарушения информационной безопасности могут привести к значительным потерям.

Нарушения безопасности IT возникают вследствие преднамеренной эксплуатации или непреднамеренного запуска уязвимостей в применении IT в рамках бизнес-задач.

Необходимо принять меры для предотвращения уязвимостей, возникающих в продуктах IT. По мере возможности уязвимости должны быть:

a) устранены - то есть должны быть предприняты активные меры для выявления и устранения или нейтрализации всех проявляемых уязвимостей;

b) минимизированы – то есть должны быть предприняты активные шаги для снижения до приемлемого остаточного уровня потенциального воздействия любого проявления уязвимости;

c) Находиться под наблюдением – должны быть предприняты активные шаги для обеспечения обнаружения любых попыток использовать уязвимость, чтобы можно было предпринять шаги для сокращения ущерба.

**5.3.3 Причина уязвимости**

Уязвимости могут возникать из-за сбоев в:

а) требованиях: IT-продукт может обладать всеми требуемыми от него функциями и возможностями и при этом содержать уязвимости, которые делают его непригодным или неэффективным с точки зрения безопасности;

b) проектированиях: IT-продукт спроектирован плохо. Создание безопасного продукта, системы или приложения требует не только реализации функциональных требований, но и архитектуры, которая позволяет эффективно обеспечивать соблюдение конкретных свойств безопасности, которые продукт, система или приложение должны обеспечивать. Способность противостоять атакам, с которыми продукт, система или приложение могут столкнуться в предполагаемой операционной среде, во многом зависит от архитектуры, которая запрещает эти атаки или, если они не могут быть запрещены, позволяет обнаруживать такие атаки и/или ограничивать ущерб, который может нанести такая атака;

c) разработке: IT-продукт не соответствует своим спецификациям и/или в результате плохих стандартов разработки или неправильного выбора дизайна появились уязвимости;

d) доставка, установка и настройка: IT-продукт имеет уязвимости, появившиеся во время доставки, установки и настройки продукта;

e) эксплуатация: IT-продукт был сконструирован правильно и в соответствии с правильной спецификацией, но в результате неадекватного контроля за его эксплуатацией возникли уязвимости.

f) обслуживание: IT-продукт поддерживается таким образом, что появляются новые уязвимости.

**5.3.4 ISO/IEC 15408 доверие**

Доверие является основанием для уверенности в том, что IT-продукт отвечает целям безопасности. Доверие могло бы быть получено из ссылки на такие источники, как необоснованные утверждения, предшествующий опыт или аналогичный опыт. ISO/IEC 15408 обеспечивает доверие посредством активного расследования. Активное исследование – это оценка IT-продукта с целью определения его свойств безопасности.

**5.3.5 Доверие посредством оценки**

Оценка является традиционным средством получения доверия и является основой подхода ISO/IEC 15408.

Методы оценки могут включать:

а) анализ и проверка процесса(ов) и процедуры(й);

b) проверка того, что процесс(ы) и процедура(ы) применяются;

c) анализ соответствия между представлениями проекта TOE;

d) анализ представления проекта TOE на соответствие требованиям;

e) проверка доказательств;

f) анализ руководящих документов;

g) анализ разработанных функциональных тестов и предоставленных результатов;

h) независимое функциональное тестирование;

i) анализ уязвимостей (включая гипотезы недостатков);

j) испытание на проникновение;

k) анализ процесса доставки;

l) анализ процесса технического обслуживания.

**5.4 Шкала оценки доверия ISO/IEC 15408**

ISO/IEC 15408 утверждает, что большее доверие возникает в результате применения больших усилии при оценке, в то время как цель заключается в применении минимальных усилий, необходимых для обеспечения необходимого уровня доверия.

Увеличение применяемых усилий основано на:

а) объем – применяется больше усилий, при рассмотрении большой части IT-продукта

b) глубина – усилий применяется больше на более тонком уровне детализации проектирования и реализации;

с) строгость – при их применении более структурированным, формальным образом.

## **6 Компоненты обеспечения безопасности**

**6.1 Общие положения**

Подразделы 6.2 – 6.6 описывают конструкции, используемые в представлении классов, семейств и компонентов.

На рисунке 1 показаны требования доверия, установленные в стандарте ISO/IEC 15408. 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 Профиле защиты (ПЗ) и Задании по безопасности (ЗБ).

**6.2 Структура класса доверия**

**6.2.1 Общие положения**

Структура класса доверия показана на рисунке 1.

**6.2.2 Наименование 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.

**6.2.3 Представление класса**

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

**6.2.4 Семейства доверия**

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

**6.3 Структура семейства доверия**

**6.3.1 Имя семейства**

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

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

**6.3.2 Цели**

Подраздел «Цели» семейства доверия представляет назначение семейства доверия.

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



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

**6.3.3 Ранжирование компонентов**

Каждое семейство доверия содержит один или несколько компонентов доверия. Этот подраздел 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 охвата, глубины и/или строгости.

**6.3.4 Замечания по применению**

Необязательный подраздел семейства доверия «Замечания по применению» содержит дополнительную информацию о семействе. Эта информация предназначена непосредственно для пользователей семейства доверия (например, для разработчиков ПЗ и ЗБ, проектировщиков 00, оценщиков).

Представление информации неформально и включает в себя, например, предупреждения об ограничениях использования или областях, требующих особого внимания.

**6.3.5 Компоненты доверия**

Каждое семейство содержит хотя бы один компонент доверия. Структура компонентов доверия представлена в следующем пункте.

**6.4 Структура компонента доверия**

**6.4.1 Общие положения**

На рисунке 2 проиллюстрирована структуру компонента доверия.



**Рисунок 2 – Структура компонента доверия**

Связи между компонентами внутри семейства показаны жирными линиями. Для частей требований, которые являются новыми, расширенными или модифицированными по сравнению с требованиями предыдущего по иерархии компонента, применен полужирный шрифт.

**6.4.2 Идентификация компонента**

Подраздел «Идентификация компонента» содержит описательную информацию, необходимую для идентификации, категорирования, регистрации и ссылок на компонент.

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

Представлена также уникальная краткая форма имени компонента доверия как основной способ ссылки на компонент. Принято, что за краткой формой имени семейства ставится точка, а затем цифра. Цифры для компонентов внутри каждого семейства назначены последовательно, начиная с единицы.

**6.4.3 Цели**

Необязательный подраздел «Цели» компонента доверия содержит конкретные цели для данного компонента. Для компонентов доверия, которые имеют этот подраздел, он включает в себя конкретное назначение данного компонента и более подробное разъяснение целей.

**6.4.4 Замечания по применению**

Необязательный подраздел компонента доверия «Замечания по применению», при его наличии, содержит дополнительную информацию для облегчения использования компонента.

**6.4.5 Зависимости**

Зависимости среди компонентов доверия возникают, когда 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 может указываться: «Зависимости отсутствуют». Компоненты из списка могут, в свою очередь, иметь зависимости от других компонентов.

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

В отдельных ситуациях обозначенные зависимости могут быть неприменимы. Разработчик ПЗ/ЗБ может отказаться от удовлетворения зависимости, представив обоснование, почему данная зависимость неприменима.

**6.4.6 Элементы доверия**

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

Каждый элемент доверия принадлежит к одному из трех типов:

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

b) Элементы содержания и представления свидетельств, определяющие требуемые свидетельства и отражаемую в них информацию. Требования к содержанию и представлению свидетельств обозначены буквой «С» после номера элемента.

c) 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 явные действия и анализ, которые должны выполняться в дополнение к уже проведенным разработчиком. Должны также выполняться неуказанные явно действия оценщика, необходимые вследствие элементов действий разработчика, но не охваченные в требованиях к содержанию и представлению свидетельств.

Требования к действиям оценщика обозначаются буквой «Е» после номера элемента. Действия разработчика, содержание и представление свидетельств определяют требования доверия, которые предъявляются к разработчику при демонстрации доверия к тому, что TOE удовлетворяет ФТБ из ПЗ или ЗБ.

Действия оценщика определяют его ответственность по двум аспектам оценки. Первый аспект состоит в проверке правильности ПЗ/ЗБ в соответствии с требованиями классов АРЕ «Оценка профиля защиты» и ASE «Оценка задания по безопасности». Второй аспект состоит в верификации соответствия TOE его функциональным требованиям и требованиям доверия. Демонстрируя, что ПЗ/ЗБ правильны и их требования выполняются TOE, оценщик может предоставить основание для уверенности в том, что TOE будет отвечать поставленным целям безопасности.

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

**6.5 Элементы доверия**

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

**6.6 Классификация компонентов**

В настоящем стандарте содержатся классы семейств и компонентов, которые сгруппированы на основе, связанной с доверием. В начале каждого класса представлена диаграмма, на которой указываются семейства в классе и компоненты в каждом семействе.



**Рисунок 3 – Образец декомпозиции класса**

На рисунке 3 показан класс, содержащий одно семейство. Семейство содержит три компонента, которые являются линейно иерархичными (т.е. компонент 2 содержит более высокие требования, чем компонент 1, к конкретным действиям, приводимым свидетельствам или строгости действий и/или свидетельств). Все семейства доверия в настоящем стандарте – линейно иерархичные, хотя линейность необязательна для семейств доверия, которые могут быть добавлены в дальнейшем.

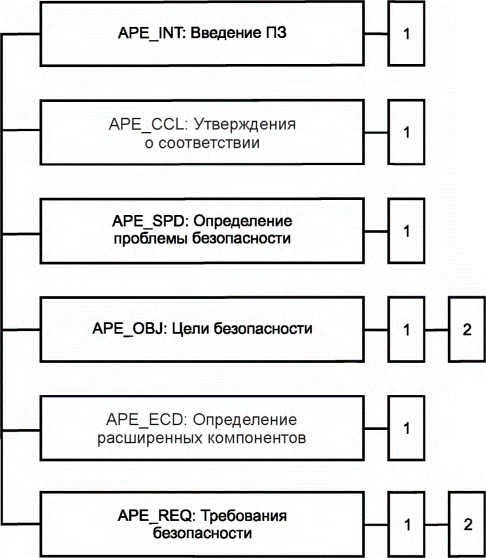
## **7 Класс АРЕ: Оценка профиля защиты**

**7.1 Общие положения**

Оценка PP требуется для демонстрации того, что PP является полным, непротиворечивым и правильным, а в случае, если PP основывается на одном или нескольких других PP или пакетах доверия, что этот PP является корректной реализацией этих PPs и пакетов доверия. Эти свойства необходимы для того, чтобы PP можно было использовать в качестве основы для разработки PPs или другого PP.

ISO/IEC 15408-1:2022 (Раздел 7) следует использовать в совокупности с приложениями А, В, С, в которых разъясняются некоторые принципы и понятия, описанные в данном подразделе, а также приводятся многочисленные примеры.

На рисунке 4 показаны семейства этого класса и иерархия компонентов этих семейств.



**Рисунок 4 – Декомпозиция класса АРЕ «Оценка профиля защиты»**

**7.2 Введение PP (APE\_NT)**

**7.2.1 Цели**

Цель данного семейства состоит в том, чтобы предоставить описание TOE в повествовательной форме.

Оценка «Введения PP» требуется для демонстрации того, что PP правильно идентифицирован, и что «Ссылка на PP» и «Аннотация TOE» не противоречат друг другу.

**7.2.2 APE\_INT.1 Введение PP**

Зависимости: отсутствуют.

Элементы действий разработчика

APE\_INT.1.1D

Разработчик PP должен представить «Введение PP».

Элементы содержания и представления свидетельств

APE\_INT.1.1C

«Введение PP» должно содержать «Ссылку на PP» и «Аннотацию TOE».

APE\_INT.1.2C

«Ссылка на PP» должна уникально идентифицировать PP.

APE\_INT.1.3C

В «Аннотации TOE» должна быть представлена краткая информация об использовании и основных функциональных возможностях безопасности TOE.

APE\_INT.1.4C

В «Аннотации TOE» должен быть идентифицирован тип TOE.

APE\_INT.1.5C

В «Аннотации TOE» должны быть идентифицированы любые не входящие в TOE аппаратные/программные/программно-аппаратные средства, доступные для TOE.

APE\_INT.1.1Е

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

**7.3 Утверждения о соответствии (APE\_CCL)**

**7.3.1 Цели**

Цель данного семейства заключается в том, чтобы сделать заключение об обоснованности утверждений о соответствии. Кроме того, в данном семействе специфицируется, соответствуют ли ЗБ и другие ПЗ данному ПЗ.

**7.3.2 АРЕ\_CCL.1 Утверждения о соответствии**

Зависимости: APE\_INT.1 Введение ПЗ

APE\_ECD.1 Определение расширенных компонентов

APE\_REQ.1 Установленные требования безопасности

Элементы действий разработчика

APE\_CCL.1.1D

Разработчик ПЗ должен представить «Утверждение о соответствии».

APE\_CCL.1.2D

Разработчик ПЗ должен представить «Обоснование утверждения о соответствии».

APE\_CCL.1.3D

Разработчик ПЗ должен представить «Изложение соответствия».

Элементы содержания и представления свидетельств

APE\_CCL\_1.1С

В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ISO/IEC 15408»

Утверждение о соответствии должно указывать издание ISO/IEC 15408, о соответствии которому утверждает ПЗ.

APE\_CCL.1.2C

Утверждение о соответствии должно описывать соответствие ПЗ ISO/IEC 15408-2 либо как соответствующего ISO/IEC 15408-2, либо как расширенного ISO/IEC 15408-2.

APE\_CCL.1.3C

Утверждение о соответствии должно описывать соответствие ПЗ как «соответствующее настоящему стандарту» или «расширенное ISO/IEC 15408-3».

APE\_CCL.1.4C

Утверждение о соответствии должно соответствовать определению расширенных компонентов.

APE\_CCL.1.5C

Утверждение о соответствии должно идентифицировать все ПЗ и упаковки, о соответствии которым утверждает ПЗ.

APE\_CCL.1.6C

Утверждение о соответствии должно описывать любое соответствие ПЗ функциональному пакету как соответствие пакету, расширенному пакету или адаптированному пакету.

APE\_CCL.1.7C

Утверждение о соответствии должно описывать любое соответствие ПЗ пакету гарантий как соответствующее пакету или расширенное пакетом.

APE\_CCL.1.8C

Утверждение о соответствии должно описывать любое соответствие ПЗ другому ПЗ в качестве ПЗ, соответствующего ПЗ.

APE\_CCL.1.9C

Обоснование утверждения о соответствии должно демонстрировать, что тип TOE соответствует типу TOE в ПЗ, о соответствии которому утверждается.

APE\_CCL.1.10C

Обоснование утверждения о соответствии должно демонстрировать, что формулировка определения проблемы безопасности согласуется с формулировкой определения проблемы безопасности в ПЗ и любых функциональных пакетах, для которых утверждается о соответствии.

APE\_CCL.1.11C

Обоснование утверждения о соответствии должно демонстрировать, что изложение целей безопасности согласуется с изложением целей безопасности в ПЗ и любых функциональных пакетах, для которых утверждается о соответствии.

APE\_CCL.1.12C

Обоснование утверждения о соответствии должно демонстрировать, что изложение требований безопасности согласуется с изложением требований безопасности в ПЗ и любых функциональных пакетах, для которых утверждается о соответствии.

APE\_CCL.1.13C

В утверждения о соответствии должно описываться соответствие любых ПЗ/ЗБ ПЗ как точное, строгое или доказуемое соответствие.

APE\_CCL.1.14C

Для ПЗ с точным соответствием утверждения о соответствии должно содержать утверждения о разрешении, которое идентифицирует набор ПЗ (если таковые имеются), для которых в сочетании с оцениваемым ПЗ разрешено утверждать о точном соответствии.

APE\_CCL.1.15C

Для ПЗ с точным соответствием утверждения о соответствии должно содержать утверждение «разрешено с», которое идентифицирует набор Модулей ПП (если таковые имеются), которые разрешено использовать с оцениваемым ПЗ в Конфигурации ПП.

APE\_CCL.1.16C

Утверждение о соответствии должно идентифицировать набор производных методов оценки и действий по оценке (если таковые имеются), которые будут использоваться с оцениваемым ПЗ. Этот список должен содержать:

- любые методы оценки и действия по оценке, указанные для оцениваемого ПЗ;

- любые методы оценки и действия по оценке, указанные в утверждениях о соответствии ПЗ, о соответствии которым заявляет оцениваемый ПЗ;

- любые методы оценки и действия по оценке, указанные в разделах «Требования безопасности» пакетов, о соответствии которым утверждает оцениваемый ПЗ.

Элементы действий оценщика

APE\_CCL.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**7.4 Определение проблемы безопасности (APE\_SPD)**

**7.4.1 Цели**

В данной части ПЗ определяется проблема безопасности, которая должна решаться применением TOE и его средой функционирования.

Оценка «Определения проблемы безопасности» требуется для того, чтобы продемонстрировать, что проблема безопасности данного TOE и среды его функционирования четко определена.

**7.4.2 APE\_SPD.1 Определение проблемы безопасности**

Зависимости: отсутствуют.

Элементы действий разработчика

APE\_SPD.1.1D

Разработчик ПЗ должен представить «Определение проблемы безопасности».

Элементы содержания и представления свидетельств

APE\_SPD.1.1C

«Определение проблемы безопасности» должно включать в себя описание угроз.

APE\_SPD.1.2C

Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного действия.

APE\_SPD.1.3C

В «Определение проблемы безопасности» должно быть включено описание ПБОр.

APE\_SPD.1.4C

«Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования ОО.

Элементы действий оценщика

APE\_SPD.1.1E

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

**7.5 Цели безопасности (APE\_OBJ)**

**7.5.1 Цели**

Цели безопасности являются кратким изложением предполагаемой реакции на проблему безопасности, определенную в семействе доверия «Определение проблемы безопасности» (APE\_SPD).

Оценка целей безопасности требуется для демонстрации того, что цели безопасности достаточно и в полной мере соответствуют «Определению проблемы безопасности», и что эта проблема четко разделена между TOE и средой его функционирования.

**7.5.2 Ранжирование компонентов**

Компоненты этого семейства ранжированы по следующему принципу – либо они описывают только цели безопасности для среды функционирования TOE, либо еще и цели безопасности для TOE.

**7.5.3 APE\_OBJ.1 Цели безопасности для среды функционирования**

Зависимости: отсутствуют.

Элементы действий разработчика

APE\_OBJ.1.1D

Разработчик ПЗ должен представить изложение «Целей безопасности».

Элементы содержания и представления свидетельств

APE\_OBJ.1.1C

Изложение «Целей безопасности» должно включать в себя описание целей безопасности для среды функционирования 00.

Элементы действий оценщика

APE\_0BJ.1.1E

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

**7.5.4 APE\_0BJ.2 Цели безопасности**

Зависимости: APE\_SPD.1 Определение проблемы безопасности

Элементы действий разработчика

APE\_0BJ.2.1D

Разработчик ПЗ должен представить изложение «Целей безопасности».

APE\_OBJ.2.2D

Разработчик ПЗ должен представить «Обоснование целей безопасности».

Элементы содержания и представления свидетельств

APE\_OBJ.2.1C

Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования TOE.

APE\_OBJ.2.2C

В «Обосновании целей безопасности» каждая цель безопасности для TOE должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к ПБОр, на осуществление которых направлена эта цель безопасности.

APE\_OBJ.2.3C

В «Обосновании целей безопасности» каждая цель безопасности для TOE должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.

APE\_OBJ.2.4C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.

APE\_OBJ.2.5C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всех ПБОр.

APE\_OBJ.2.6C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.

Элементы действий оценщика

APE\_OBJ.2.1E

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

**7.6 Определение расширенных компонентов (APE\_ECD)**

**7.6.1 Цели**

Расширенные требования безопасности являются требованиями, которые основываются не на компонентах ISO/IEC 15048-2 или настоящего стандарта, а на расширенных компонентах: компонентах, определяемых разработчиком ПЗ.

Оценка определения расширенных компонентов необходима для того, чтобы сделать заключение, что эти компоненты определены четко и однозначно, и что они необходимы, т. е. не могут быть в полной мере выражены через существующие компоненты ISO/IEC 15048-2 или настоящего стандарта.

**7.6.2 APE\_ECD.1 Определение расширенных компонентов**

Зависимости: отсутствуют.

Элементы действий разработчика

APE\_ECD.1.1D

Разработчик ПЗ должен представить изложение «Требований безопасности».

APE\_ECD.1.2D

Разработчик ПЗ должен представить «Определение расширенных компонентов».

Элементы содержания и представления свидетельств

APE\_ECD.1.1C

В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.

APE\_ECD.1.2C

В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.

APE\_ECD.1.3C

В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ISO/IEC 15408.

APE\_ECD.1.4C

В «Определении расширенных компонентов» в качестве модели представления должны использоваться компоненты, семейства, классы и методология ISO/IEC 15408.

APE\_ECD.1.5C

Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Элементы действий оценщика

APE\_ECD.1.1E

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

APE\_ECD.1.2E

Оценщик должен подтвердить, что ни один из расширенных компонентов не может быть четко выражен с использованием существующих компонентов.

**7.7 Требования безопасности (APE\_REQ)**

**7.7.1 Цели**

ФТБ формируют четкое, однозначное и технически правильное описание ожидаемого режима безопасности 00. ТДБ формируют четкое, однозначное и технически правильное описание ожидаемых действий, которые будут предприняты для достижения доверия к TOE.

Оценка требований безопасности необходима для того, чтобы обеспечить их четкое, однозначное и технически правильное описание.

**7.7.2 Ранжирование компонентов**

Компоненты этого семейства ранжированы по следующему принципу — либо ФТБ устанавливаются «как есть», либо ФТБ являются производными от целей безопасности для TOE.

**7.7.3 APE\_REQ.1 Установленные требования безопасности**

Зависимости: APE\_ECD.1 Определение расширенных компонентов

Элементы действий разработчика

APE\_REQ.1.1D

Разработчик ПЗ должен представить изложение «Требований безопасности».

APE\_REQ.1.2D

Разработчик ПЗ должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

APE\_REQ.1.1C

Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

APE\_REQ.1.2C

Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.

APE\_REQ.1.3C

В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

APE\_REQ.1.4C

Все операции должны выполняться корректно.

APE\_REQ.1.5C

Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения данной зависимости.

APE\_REQ.1.6C

Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий оценщика

APE\_REQ.1.1E

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

**7.7.4 APE\_REQ.2 Производные требования безопасности**

Зависимости: APE\_OBJ.2 Цели безопасности

APE\_ECD.1 Определение расширенных компонентов

Элементы действий разработчика

APE\_REQ.2.1D

Разработчик ПЗ должен представить изложение «Требований безопасности».

APE\_REQ.2.2D

Разработчик ПЗ должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

APE\_REQ.2.1C

Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

APE\_REQ.2.2C

Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.

APE\_REQ.2.3C

В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

APE\_REQ.2.4C

Все операции должны быть выполнены правильно.

APE\_REQ.2.5C

Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.

APE\_REQ.2.6C

В «Обосновании требований безопасности» должно быть представлено прослеживание каждого ФТБ к целям безопасности для TOE.

APE\_REQ.2.7C

В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех целей безопасности для TOE.

APE\_REQ.2.8C

В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.

APE\_REQ.2.9C

Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий оценщика

APE\_REQ.2.1E

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

## **8 Класс ASE: Оценка задания по безопасности**

**8.1 Общие положения**

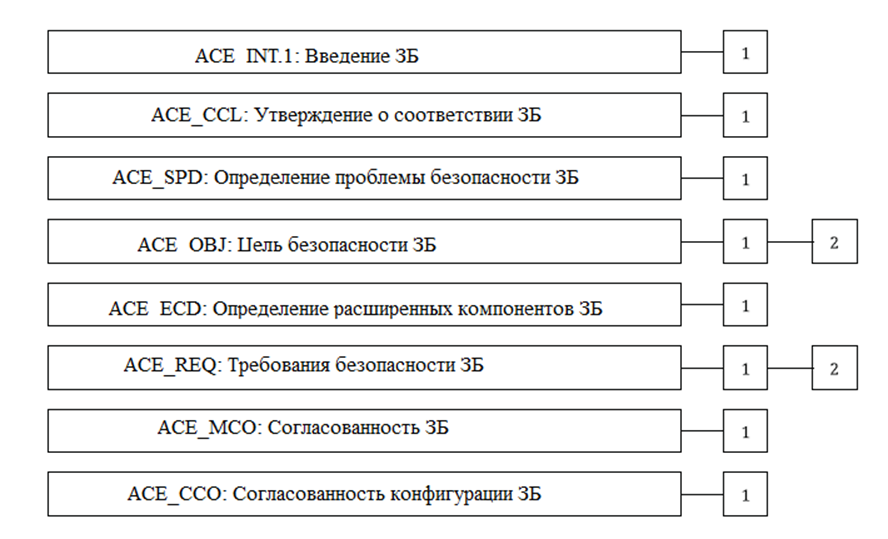
Оценка ЗБ требуется для демонстрации того, что ЗБ является правильным и внутренне непротиворечивым и, если ЗБ основано на одном или более ПЗ или пакетах доверия, что ЗБ является корректной реализацией этих ПЗ и пакетов. Эти свойства необходимы для того, чтобы можно было использовать ЗБ в качестве основы при оценке TOE.

Класс ACE определен для оценки конфигурации ЗБ, состоящей как минимум из одного ЗБ и одного другого компонента (ЗБ и/или ЗБ-модулей). Оценка PP рассматривается в классе APE. Класс ACE определяет требования к:

– Оценка ЗБ-модулей в рамках их Базы(ов) ЗБ-модулей (компоненты ACE\_INT.1, ACE\_CCL.1, ACE\_SPD.1, ACE\_OBJ.1 или ACE\_OBJ.2, ACE\_REQ.1 или ACE\_REQ.2 и ACE\_MCO.1).

– Оценка согласованности комбинации всех ЗБ и модулей ЗБ, принадлежащих к конфигурации PP (см. ACE\_CCO.1).

Раздел 8 следует использовать вместе с ISO/IEC 15408-1:2022, Приложение C.



**Рисунок 5 – ACE: Декомпозиция класса оценки конфигурации профиля защиты**

**8.2 Введение модуля ЗБ (ACE\_INT)**

**8.2.1 Цели**

Целью этого семейства является описательное описание TOE.

Оценка внедрения модуля ЗБ необходима для демонстрации того, что модуль ПП правильно идентифицирован и что ссылка на модуль ЗБ и обзор TOE согласуются друг с другом.

**8.2.2 ACE\_INT.1 Введение в модуль ЗБ**

Зависимости: Зависимости: отсутствуют.

Элементы действий разработчика

ACE\_INT.1.1D

Разработчик должен предоставить введение в модуль ЗБ.

Элементы контента и презентации

ACE\_INT.1.1C

Введение в модуль ЗБ должно содержать ссылку на модуль ЗБ, идентификацию базы(-ов) модуля ЗБ и обзор TOE.

ACE\_INT.1.2C

Ссылка на модуль ЗБ должна однозначно идентифицировать модуль ЗБ.

ACE\_INT.1.3C

Идентификация Базы ЗБ-Модуля должна состоять из списка, по крайней мере, одного PP и, возможно, других ЗБ и ЗБ-Модулей, от которых зависит ЗБ-Модуль.

ACE\_INT.1.4C

Идентификация Базы(ов) Модуля ЗБ должна описывать структуру зависимостей Баз(ы) Модуля ЗБ.

ACE\_INT.1.5C

Введение в модуль ЗБ должно содержать столько же обзоров TOE, сколько альтернативных баз модулей ЗБ.

ACE\_INT.1.6C

Обзор TOE должен суммировать использование и основные функции безопасности TOE.

ACE\_INT.1.7C

Обзор TOE должен идентифицировать тип TOE.

ACE\_INT.1.8C

Обзор TOE должен идентифицировать любое оборудование/программное обеспечение/микропрограммное обеспечение, не относящееся к TOE, доступное для TOE.

ACE\_INT.1.9C

Обзор TOE должен описывать различия TOE по отношению к TOE, определенным в Базе(ах) модуля PP.

Элементы действий оценщика

ACE\_INT.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.3 Заявления о соответствии модуля ЗБ (ACE\_CCL)**

**8.3.1 Цели**

Целью этого семейства является определение действительности заявления о соответствии и заявления о соответствии. Модуль ЗБ не может заявлять о соответствии какому-либо ЗБ, конфигурации ЗБ или другому модулю ЗБ.

**8.3.2 ACE\_CCL Утверждения о соответствии модуля ЗБ**

Зависимости:

ACE\_INT.1 Введение в модуль ЗБ

ACE\_ECD.1 Определение расширенных компонентов модуля ЗБ

ACE\_REQ.1 Требования безопасности, установленные модулем ЗБ, или требования безопасности, производные ACE\_REQ.2 модуля ЗБ.

Элементы действий разработчика

ACE\_CCL.1.1D

Разработчик должен предоставить утверждение о соответствии.

ACE\_CCL.1.2D

Разработчик должен предоставить утверждение о соответствии.

Элементы контента и презентации

ACE\_CCL.1.1C

Утверждение о соответствии должно указывать издание ISO/IEC 15408, о соответствии которому утверждает модуль ЗБ.

ACE\_CCL.1.2C

Утверждение о соответствии должно описывать соответствие модуля ЗБ стандарту ISO/IEC 15408-2 либо как соответствующего ISO/IEC 15408-2, либо как расширенного ISO/IEC 15408-2.

ACE\_CCL.1.3C

Утверждение о соответствии должно описывать тип соответствия, требуемый от любого ЗБ для модуля ЗБ (как части конфигурации ЗБ), как тип соответствия: точный, строгий или доказуемый.

ACE\_CCL.1.4C

Утверждение о соответствии должно описывать соответствие модуля ЗБ настоящему стандарту либо как «соответствующее ISO/IEC 15408-3», либо как «расширенное   
ISO/IEC 15408-3».

ACE\_CCL.1.5C

Утверждение о соответствии должно соответствовать определению расширенных компонентов.

ACE\_CCL.1.6C

Утверждение о соответствии должно идентифицировать все функциональные пакеты, о соответствии которым утверждает модуль ЗБ.

ACE\_CCL.1.7C

Утверждение о соответствии должно описывать любое соответствие модуля PP функциональному пакету как совместимое с пакетом, дополненное пакетом или адаптированное для пакета.

ACE\_CCL.1.8C

Утверждение о соответствии должно идентифицировать все пакеты обеспечения качества, о соответствии которым утверждает модуль ЗБ.

ACE\_CCL.1.9C

Утверждение о соответствии должно описывать любое соответствие модуля PP пакету обеспечения качества как соответствующего пакету, так и расширенного пакета.

ACE\_CCL.1.10C

Для точного соответствия утверждения о соответствии модуля ЗБ должно содержать заявление «разрешено с», которое идентифицирует набор ЗБ и модулей ЗБ (за исключением тех ЗБ и модулей ЗБ, которые включены в базу модулей ЗБ), к которым в сочетании с оцениваемыми модулями PP допускается утверждать о точном соответствии.

ACE\_CCL.1.11C

Утверждение о соответствии может идентифицировать набор основанных на ISO/IEC 18045 методов оценки и действий по оценке, которые должны использоваться с оцениваемым модулем ЗБ. Этот список должен содержать любые методы оценки и действия по оценке, указанные в модуле ЗБ, а также любые методы оценки и действия по оценке, указанные в базе(ах) модуля ЗБ и/или в пакетах (если таковые имеются), для которых установлено соответствие, оцениваемым модулем ЗБ.

Элементы действий оценщика

ACE\_CCL.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.4 Определение проблемы безопасности модуля PP (ACE\_SPD)**

**8.4.1 Цели**

**Эта часть** модуля PP определяет проблему безопасности, которую должен решать TOE, и операционную среду TOE.

Оценка определения проблемы безопасности необходима для демонстрации того, что проблема безопасности, которую должен решать TOE и его эксплуатационная среда, четко определена.

**8.4.2 ACE\_SPD.1 Определение проблемы безопасности модуля ЗБ**

Зависимости: Зависимости: отсутствуют.

Элементы действий разработчика

ACE\_SPD.1.1D

Разработчик должен предоставить определение проблемы безопасности.

Элементы контента и презентации

ACE\_SPD.1.1C

Определение проблемы безопасности должно описывать угрозы.

ACE\_SPD.1.2C

Все угрозы должны быть описаны с точки зрения агента угрозы, актива и неблагоприятного действия.

ACE\_SPD.1.3C

Определение проблемы безопасности должно описывать OSP.

ACE\_SPD.1.4C

Определение проблемы безопасности должно описывать предположения относительно операционной среды TOE.

Элементы действий оценщика

ACE\_SPD.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.5 Цели безопасности модуля PP (ACE\_OBJ)**

**8.5.1 Цели**

Цели безопасности представляют собой краткое изложение предполагаемого ответа на проблему безопасности, определенную с помощью семейства определений проблем безопасности (APE\_SPD).

Оценка целей безопасности необходима для демонстрации того, что цели безопасности адекватно и полностью соответствуют определению проблемы безопасности и что разделение этой проблемы между TOE и его операционной средой четко определено.

**8.5.2 Ранжирование компонентов**

Компоненты этого семейства ранжируются в зависимости от того, предписывают ли они только цели безопасности для операционной среды (см. ACE\_OBJ.1) или также цели безопасности для TOE (см. ACE\_OBJ.2).

**8.5.3 ACE\_OBJ.1 Цели безопасности модуля ЗБ для операционной среды**

Зависимости: Зависимости: отсутствуют.

Элементы действий разработчика

ACE\_OBJ.1.1D

Разработчик должен предоставить формулировку целей безопасности для операционной среды модулей ЗБ.

ACE\_OBJ.1.2D

Разработчик должен предоставить обоснование целей безопасности среды эксплуатации модулей ЗБ.

Элементы контента и презентации

ACE\_OBJ.1.1C

Заявление о целях безопасности должно описывать цели безопасности для операционной среды.

ACE\_OBJ.1.2C

Обоснование целей безопасности должно прослеживать каждую цель безопасности для операционной среды до угроз, которым противостоит эта цель безопасности, OSP, реализуемых этой целью безопасности, и допущений, поддерживаемых этой целью безопасности.

ACE\_OBJ.1.3C

Обоснование целей безопасности должно демонстрировать, что цели безопасности для операционной среды подтверждают все предположения.

Элементы действий оценщика

ACE\_OBJ.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.5.4 ACE\_OBJ.2 Цели безопасности РР**

Зависимости: ACE\_SPD.1 Определение проблемы безопасности модуля ЗБ.

Элементы действий разработчика

ACE\_OBJ.2.1D

Разработчик должен предоставить формулировку целей безопасности для модулей РР.

ACE\_OBJ.2.2D

Разработчик должен предоставить обоснование целей безопасности модулей РР.

Элементы контента и презентации

ACE\_OBJ.2.1C

В заявлении о целях безопасности должны быть описаны цели безопасности для TOE и цели безопасности для операционной среды.

ACE\_OBJ.2.2C

Обоснование целей безопасности должно прослеживать каждую цель безопасности для TOE до угроз, которым противостоит эта цель безопасности, и OSP, реализуемых этой целью безопасности.

ACE\_OBJ.2.3C

Обоснование целей безопасности должно прослеживать каждую цель безопасности для операционной среды до угроз, которым противостоит эта цель безопасности, OSP, реализуемых этой целью безопасности, и допущений, поддерживаемых этой целью безопасности.

ACE\_OBJ.2.4C

Обоснование целей безопасности должно демонстрировать, что цели безопасности противодействуют всем угрозам.

ACE\_OBJ.2.5C

Обоснование целей безопасности должно демонстрировать, что цели безопасности обеспечивают соблюдение всех OSP.

ACE\_OBJ.2.6C

Обоснование целей безопасности должно демонстрировать, что цели безопасности для операционной среды подтверждают все предположения.

Элементы действий оценщика

ACE\_OBJ.2.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.6 Определение расширенных компонентов модуля PP (ACE\_ECD)**

**8.6.1 Цели**

Расширенные SFR — это требования, которые не основаны на компонентах из ISO/IEC 15408-2 или данного документа, а основаны на расширенных компонентах: компонентах, определенных автором модуля PP.

Оценка определения расширенных функциональных компонентов необходима для определения того, что они ясны и недвусмысленны, а также необходимы, т.е. они могут не быть четко выражены с использованием существующих компонентов ISO/IEC 15408-2 или настоящего документа.

**8.6.2 ACE\_ECD.1 Расширенное определение компонентов модулей PP**

Зависимости: Зависимости: отсутствуют.

Элементы действий разработчика

ACE\_ECD.1.1D

Разработчик должен предоставить изложение требований безопасности к модулям РР.

ACE\_ECD.1.2D

Разработчик должен предоставить расширенное определение компонентов для модулей ПП.

Элементы контента и презентации

ACE\_ECD.1.1C

В заявлении о требованиях безопасности должны быть указаны все расширенные требования безопасности.

ACE\_ECD.1.2C

Определение расширенных компонентов должно определять расширенный компонент для каждого расширенного требования безопасности.

ACE\_ECD.1.3C

Определение расширенных компонентов должно описывать, как каждый расширенный компонент связан с существующими компонентами, семействами и классами серии ISO/IEC 15408.

ACE\_ECD.1.4C

В определении расширенных компонентов в качестве модели для представления должны использоваться существующие компоненты, семейства, классы и методология серии ISO/IEC 15408.

ACE\_ECD.1.5C

Расширенные компоненты должны состоять из измеримых и объективных элементов, чтобы можно было продемонстрировать соответствие или несоответствие этим элементам.

Элементы действий оценщика

ACE\_ECD.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ACE\_ECD.1.2E

Оценщик должен подтвердить, что ни один расширенный компонент не может быть четко выражен с использованием существующих компонентов.

**8.7 Требования безопасности модуля PP (ACE\_REQ)**

**8.7.1 Цели**

SFR формируют ясное, недвусмысленное и четко определенное описание ожидаемого поведения безопасности TOE. SAR образуют ясное, недвусмысленное и четко определенное описание ожидаемых действий, которые будут предприняты для получения уверенности в TOE.

Оценка требований безопасности необходима для обеспечения их ясности, недвусмысленности и четкости.

**8.7.2 Ранжирование компонентов**

Компоненты этого семейства уравниваются в зависимости от того, выводятся ли SFR из SPD (см. ACE\_REQ.1) или из целей безопасности для TOE (см. ACE\_REQ.2.).

**8.7.3 ACE\_REQ.1 Требования безопасности, применяемые к модулю РР**

Зависимости:

APE\_ECD.1 Определение расширенных компонентов

ACE\_SPD.1 Определение проблемы безопасности модуля PP

Элементы действий разработчик

ACE\_REQ.1.1D

Разработчик должен предоставить изложение требований безопасности к модулям РР.

ACE\_REQ.1.2D

Разработчик должен предоставить обоснование требований безопасности модулей РР.

Элементы контента и презентации

ACE\_REQ.1.1C

В заявлении о требованиях безопасности должны быть описаны SFR и SAR (SAR, применимые к модулю PP, могут быть явно указаны или взяты от базы(-й) модуля PP).

ACE\_REQ.1.2C

Должны быть определены все субъекты, объекты, операции, атрибуты безопасности, внешние объекты и другие термины, которые используются в SFR и SAR.

ACE\_REQ.1.3C

Изложение требований безопасности должно идентифицировать все операции по требованиям безопасности.

ACE\_REQ.1.4C

Все операции должны выполняться правильно.

ACE\_REQ.1.5C

Каждая зависимость требований безопасности должна быть либо удовлетворена, либо обоснование требований безопасности должно оправдывать неудовлетворение зависимости.

ACE\_REQ.1.6C

Обоснование требований безопасности должно прослеживать каждое SFR до угроз, которым противостоит это SFR, и OSP, реализуемых этим SFR.

ACE\_REQ.1.7C

Обоснование требований безопасности должно демонстрировать, что SFR (в сочетании с целями безопасности для среды) противодействуют всем угрозам для TOE.

ACE\_REQ.1.8C

Обоснование требований безопасности должно демонстрировать, что SFR (в сочетании с целями безопасности для среды) обеспечивают соблюдение всех OSP для TOE.

ACE\_REQ.1.9C

Обоснование требований безопасности должно объяснять, почему были выбраны SAR.

ACE\_REQ.1.10C

Изложение требований безопасности должно быть внутренне непротиворечивым.

Элементы действий оценщика

ACE\_REQ.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.7.4 ACE\_REQ.2 Требования безопасности, производные от модуля PP**

Зависимости:

ACE\_ECD.1 Определение расширенных компонентов модуля PP

ACE\_OBJ.2 Цели безопасности модуля PP

Элементы действий разработчика

ACE\_REQ.2.1D

Разработчик должен предоставить изложение требований безопасности к модулям РР.

ACE\_REQ.2.2D

Разработчик должен предоставить обоснование требований безопасности модулей РР.

Элементы контента и презентации

ACE\_REQ.2.1C

В заявлении о требованиях безопасности должны быть описаны SFR и SAR (SAR, применимые к модулю PP, могут быть явно указаны или взяты из базы(-й) модуля PP).

ACE\_REQ.2.2C

Должны быть определены все субъекты, объекты, операции, атрибуты безопасности, внешние объекты и другие термины, которые используются в SFR и SAR.

ACE\_REQ.2.3C

Изложение требований безопасности должно идентифицировать все операции по требованиям безопасности.

ACE\_REQ.2.4C

Все операции должны выполняться правильно.

ACE\_REQ.2.5C

Каждая зависимость требований безопасности должна быть либо удовлетворена, либо обоснование требований безопасности должно оправдывать неудовлетворение зависимости.

ACE\_REQ.2.6C

Обоснование требований безопасности должно прослеживать каждое SFR до целей безопасности TOE, реализуемых этим SFR.

ACE\_REQ.2.7C

Обоснование требований безопасности должно демонстрировать, что SFR отвечают всем целям безопасности для TOE.

ACE\_REQ.2.8C

Обоснование требований безопасности должно объяснять, почему были выбраны SAR.

ACE\_REQ.2.9C

Изложение требований безопасности должно быть внутренне непротиворечивым.

Элементы действий оценщика

ACE\_REQ.2.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

**8.8 Согласованность модуля PP (ACE\_MCO)**

**8.8.1 Цели**

Целью этого семейства является определение согласованности модуля PP и установление соответствия между модулем PP и его базой(ами) модуля PP.

**8.8.2 ACE\_MCO.1 Согласованность модуля PP**

Зависимости:

ACE\_INT.1 Введение в модуль PP

ACE\_SPD.1 Определение проблемы безопасности модуля PP

ACE\_OBJ.1 Прямое обоснование Цели безопасности модуля PP для окружающей среды или ACE\_OBJ.2 Цели безопасности модуля PP

ACE\_REQ.1 Прямое обоснование требований безопасности модуля PP или ACE\_REQ.2 Требования безопасности, производные от модуля PP

Элементы действий разработчика

ACE\_MCO.1.1D

Разработчик должен предоставить обоснование согласованности модуля PP для каждой из альтернативных баз модуля PP, указанных во введении к модулю PP.

ACE\_MCO.1.2D

Разработчик должен предоставить обоснование надежности модуля PP для каждой из альтернативных баз модуля PP, указанных во введении к модулю PP.

Элементы контента и презентации

ACE\_MCO.1.1C

Обоснование согласованности должно демонстрировать, что тип TOE модуля PP и типы TOE его базы(ов) модуля PP согласованы.

ACE\_MCO.1.2C

Обоснование согласованности должно идентифицировать активы SPD модуля PP, которые также принадлежат некоторым из его баз модулей PP, и среди них те, для которых модуль PP и база модуля PP определяют разные проблемы безопасности.

ACE\_MCO.1.3C

Обоснование последовательности должно демонстрировать, что:

- формулировка определения проблемы безопасности согласуется с формулировкой определения проблемы безопасности его Базы(ами) Модулей PP;

- формулировка определения проблемы безопасности согласуется с формулировкой определения проблемы безопасности любого функционального пакета, для которого заявляется соответствие.

ACE\_MCO.1.4C

Обоснование последовательности должно демонстрировать, что:

- определение целей безопасности согласуется с целями безопасности его Базы(ами) Модулей PP;

- определение целей безопасности согласуется с целями безопасности любого функционального пакета, соответствие которого заявляется.

ACE\_MCO.1.5C

Обоснование последовательности должно демонстрировать, что:

- определение функциональных требований безопасности соответствует функциональным требованиям безопасности его Базы(ами) Модулей PP;

- определение функциональных требований безопасности согласуется с функциональными требованиями безопасности любого функционального пакета, соответствие которого заявляется.

ACE\_MCO.1.6C

Обоснование доверия должно демонстрировать внутреннюю согласованность набора требований обеспечения безопасности модуля PP в отношении определения проблемы безопасности.

ACE\_MCO.1.7C

Обоснование доверия должно демонстрировать согласованность набора требований обеспечения безопасности Модуля PP с требованиями обеспечения безопасности Базы(ами) Модуля PP.

Элементы действий оценщика

ACE\_MCO.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств. Если в модуле PP указаны альтернативные основы модуля PP, оценщик должен выполнить это действие для каждого обоснования согласованности.

**8.9 Согласованность конфигурации PP (ACE\_CCO)**

**8.9.1 Цели**

Целью этого семейства является определение правильности и согласованности конфигурации PP.

**8.9.2 ACE\_CCO.1 Согласованность конфигурации PP**

Зависимости:

ACE\_INT.1 Введение в модуль PP

Заявления о соответствии модуля ACE\_CCL.1 PP

ACE\_SPD.1 Определение проблемы безопасности модуля PP

ACE\_OBJ.1 Прямое обоснование целей безопасности модуля PP для окружающей среды или ACE\_OBJ.2 Цели безопасности модуля PP

ACE\_ECD.1 Определение расширенного компонента модуля PP

ACE\_REQ.1 Прямое обоснование требований безопасности модуля РР или ACE\_REQ.2 производные требования безопасности модуля РР

Согласованность модуля ACE\_MCO.1 PP

APE\_\* (все компоненты APE)

Элементы действий разработчика

ACE\_CCO.1.1D

Разработчик должен предоставить ссылку на конфигурацию РР.

ACE\_CCO.1.2D

Разработчик должен предоставить описание компонентов.

ACE\_CCO.1.3D

Разработчик должен предоставить обзор TOE.

ACE\_CCO.1.4D

Разработчик должен предоставить утверждение о соответствии.

ACE\_CCO.1.5D

Разработчик должен предоставить утверждение о соответствии в утверждении соответствии.

ACE\_CCO.1.6D

Разработчик должен предоставить обоснование последовательности.

ACE\_CCO.1.7D

Разработчик должен предоставить утверждение SAR.

ACE\_CCO.1.8D

Разработчик должен предоставить набор методов и/или действий оценки, применимых к конфигурации РР.

Элементы контента и презентации

ACE\_CCO.1.1C

Ссылка на конфигурацию PP должна однозначно идентифицировать конфигурацию PP.

ACE\_CCO.1.2C

Заявление о компонентах конфигурации PP должно однозначно идентифицировать PP и модули PP, составляющие конфигурацию PP.

ACE\_CCO.1.3C

Для каждого модуля PP, указанного в описании компонентов конфигурации PP, описание компонентов должно включать базу модуля PP, необходимую для указанного модуля PP. Если в модуле PP указаны альтернативные базы модулей PP, в конфигурации PP должна быть указана только одна из этих баз модулей PP.

ACE\_CCO.1.4C

Для конфигурации PP с множественным доверием описание компонентов должно описывать организацию TSF с точки зрения суб-TSF, определенных в PP, и модулей PP, определенных в конфигурации PP.

ACE\_CCO.1.5C

Обзор TOE должен идентифицировать тип TOE.

ACE\_CCO.1.6C

Обзор TOE должен описывать использование и основные функции безопасности TOE.

ACE\_CCO.1.7C

Обзор TOE должен идентифицировать любое оборудование/программное обеспечение/микропрограммное обеспечение, не относящееся к TOE, доступное для TOE.

ACE\_CCO.1.8C

Утверждение о соответствии должно указывать издание(я) ISO/IEC 15408, о соответствии которому заявляют компоненты конфигурации РР.

ACE\_CCO.1.9C

Утверждение о соответствии должно описывать соответствие конфигурации РР ISO/IEC 15408-2 либо как соответствующее ISO/IEC 15408-2, либо как расширенное ISO/IEC 15408-2.

ACE\_CCO.1.10C

Утверждение о соответствии должно описывать соответствие конфигурации PP настоящему документу либо как «соответствующее ISO/IEC 15408-3», либо как расширенное ISO/IEC 15408-3.

ACE\_CCO.1.11C

Утверждение о соответствии должно соответствовать утверждениям о соответствии компонентов конфигурации РР.

ACE\_CCO.1.12C

Утверждение о соответствии конфигурации PP должно включать заявление о соответствии пакета доверия, состоящее из утверждений, описывающих любое соответствие конфигурации PP пакету доверия как совместимое с пакетом или дополненное пакетом.

ACE\_CCO.1.13C

В утверждении о соответствии должно быть указано требуемое соответствие конфигурации РР как одно из точных, строгих и доказуемых, или же должен быть предоставлен список типов соответствия, которые требуются для каждого из компонентов конфигурации РР.

ACE\_CCO.1.14C

Для случая точного соответствия в заявлении о соответствии каждого РР, включенном в описание компонентов конфигурации РР, должны быть указаны все компоненты конфигурации РР как разрешенные к использованию в сочетании с РР в конфигурации РР.

ACE\_CCO.1.15C

Для случая точного соответствия в утверждении о соответствии каждого модуля PP, включенном в заявление о компонентах конфигурации PP, должны быть указаны все компоненты конфигурации PP, которых нет в базе(ах) модуля PP. для этого конкретного модуля PP как разрешенного к использованию в сочетании с модулем PP в конфигурации PP.

ACE\_CCO.1.16C

Для Конфигураций ПП, которые не относятся к точному типу соответствия (т. е. для Конфигураций ПП со строгим или доказуемым типом соответствия), заявление о соответствии Конфигурации ПП может включать в себя справочное заявление о методах оценки и действиях по оценке, которое идентифицирует серии методов оценки стандартов ISO/IEC 18045, и действия по оценке, применимые к оцениваемой конфигурации PP.

ACE\_CCO.1.17C

Обоснование согласованности должно демонстрировать, что тип TOE, определенный в конфигурации PP, согласуется с типами TOE, определенными в модулях PP и модулях PP, которые принадлежат описанию компонентов конфигурации PP.

ACE\_CCO.1.18C

Обоснование согласованности должно демонстрировать, что объединение всех SPD, целей безопасности и функциональных требований безопасности, определенных в компонентах конфигурации PP, является последовательным.

ACE\_CCO.1.19C

Для конфигурации PP с одним подтверждением в описании SAR должен быть определен один набор SAR, который применяется ко всему TOE. Для строгого и доказуемого соответствия набор SAR должен включать SAR, идентифицированные в каждом из компонентов конфигурации PP. Для точного соответствия набор SAR должен быть идентичен набору SAR, определенному в каждом из компонентов конфигурации PP.

ACE\_CCO.1.20C

Для конфигурации PP с несколькими гарантиями оператор SAR должен определять глобальный набор SAR, который применяется ко всему TOE, и SAR, которые применяются к каждому суб-TSF. Для строгого и доказуемого соответствия глобальный набор SAR должен включать набор общих SAR для компонентов конфигурации PP, а каждый набор SAR, применимый к суб-TSF, должен включать те, которые идентифицированы для компонентов конфигурации PP, связанных с этим суб-TSF. Для точного соответствия глобальный набор SAR обеспечения безопасности должен представлять собой набор общих SAR среди компонентов конфигурации PP, и каждый набор SAR, применимый к суб-TSF, должен быть идентичен наборам, определенным для компонентов конфигурации PP, связанных с этим суб-TSF.

ACE\_CCO.1.21C

Заявление о SAR для конфигурации PP должно включать обоснование доверия, которое демонстрирует соответствие применимого набора SAR с теми, которые определены в компонентах оцениваемой конфигурации PP и связанных с ними методах оценки и действий по оценке. Для конфигурации PP с несколькими гарантиями обоснование доверия должно демонстрировать:

— что глобальный набор SAR соответствует угрозам, определенным в SPD компонентов конфигурации PP, и

— что глобальный набор SAR и наборы SAR для каждого суб-TSF согласуются друг с другом.

Элементы действий оценщика

ACE\_CCO.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ACE\_CCO.1.2E

Оценщик должен проверить, что конфигурация PP, состоящая из всех модулей PP и модулей PP, указанных в описании компонентов, является согласованной.

## **9 Класс ASE: оценка задачи безопасности (ЗБ)**

**9.1 Общие положения**

Оценка ЗБ необходима для демонстрации того, что ЗБ является надежным и внутренне непротиворечивым, и, если ЗБ основано на Конфигурации ПЗ или на одном или нескольких ПЗ или пакетах, что ЗБ является правильным экземпляром Конфигурации ПЗ, ПП и пакеты. Эти свойства необходимы для того, чтобы ЗБ можно было использовать в качестве основы для оценки TOE.

Раздел 9 следует использовать вместе с ISO/IEC 15408-1:2022, приложениями B, C и D, поскольку эти приложения разъясняют концепции и содержат множество примеров.

На рисунке 6 показаны семейства этого класса и иерархия компонентов внутри семейств.



**Рисунок 6 – ASE: Декомпозиция класса оценки задачи безопасности (ST)**

**9.2 Введение ЗБ (ASE\_INT)**

**9.2.1 Цели**

Цель данного семейства состоит в том, чтобы описать TOE в повествовательной форме по трем уровням представления: «Ссылка на TOE», «Аннотация TOE» и «Описание TOE».

Оценка «Введения ЗБ» требуется для демонстрации правильной идентификации ЗБ и TOE, а также правильного описания TOE по трем уровням представления и непротиворечивости этих описаний друг другу.

**9.2.2 ASE\_INT.1 Введение ЗБ**

Зависимости: отсутствуют.

Элементы действий разработчика

ASE\_INT.1.1D

Разработчик ЗБ должен представить «Введение ЗБ».

Элементы содержания и представления свидетельств

ASE\_INT.1.1C

«Введение ЗБ» должно содержать «Ссылку на ЗБ», «Ссылку на TOE», «Аннотацию TOE» и «Описание TOE».

ASE\_INT.1.2C

«Ссылка на ЗБ» должна однозначно идентифицировать ЗБ.

ASE\_INT.1.3C

«Ссылка на TOE» должна однозначно идентифицировать TOE.

ASE\_INT.1.4C

В «Аннотации TOE» должна быть представлена краткая информация о его использовании и основных функциональных возможностях безопасности TOE.

ASE\_INT.1.5C

В «Аннотации TOE» должен быть идентифицирован тип TOE.

ASE\_INT.1.6C

В «Аннотации TOE» должны быть идентифицированы любые не входящие в TOE аппаратные, программные, а также программно-аппаратные средства, требуемые TOE.

ASE\_INT.1.7C

«Описание TOE» должно включать описание физических границ TOE.

ASE\_INT.1.8C

«Описание TOE» должно включать описание логических границ TOE.

Элементы действий оценщика

ASE\_INT.1.1E

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

ASE\_INT.1.2E

Оценщик должен подтвердить, что «Ссылка на TOE», «Аннотация TOE» и «Описание TOE» не противоречат друг другу.

**9.3 Утверждения о соответствии (ASE\_CCL)**

**9.3.1 Цели**

Цель данного семейства состоит в том, чтобы сделать заключение об обоснованности утверждений о соответствии. Кроме того, данное семейство определяет, каким образом утверждается о соответствии ЗБ заданному ПЗ.

**9.3.2 ASE\_CCL.1 Утверждения о соответствии**

Зависимости: ASE\_INT.1 Введение ЗБ

ASE\_ECD.1 Определение расширенных компонентов

ASE\_REQ.1 Установленные требования безопасности

Элементы действий разработчика

ASE\_CCL.1.1D

Разработчик должен представить «Утверждения о соответствии».

ASE\_CCL.1.2D

Разработчик должен представить «Обоснование утверждений о соответствии».

Элементы содержания и представления свидетельств

ASE\_CCL.1.1C

В «Утверждения о соответствии» должно быть включено «Утверждение о соответствии ISO/IEC 15408», которое определяет, для какой редакции ISO/IEC 15408 утверждается соответствие ЗБ и TOE.

ASE\_CCL.1.2C

В «Утверждении о соответствии ISO/IEC 15408» должно приводиться описание соответствия ЗБ; ЗБ либо описывается как соответствующее требованиям ISO/IEC 15408-2, либо как содержащее расширенные по отношению к ISO/IEC 15408-2 требования.

ASE\_CCL.1.3C

В «Утверждении о соответствии ISO/IEC 15408» должно приводиться описание соответствия ПЗ; ЗБ либо описывается как соответствующее требованиям настоящего стандарта, либо как содержащее расширенные по отношению к настоящему стандарту требования.

ASE\_CCL.1.4C

«Утверждение о соответствии» должно согласовываться с «Определением расширенных компонентов».

ASE\_CCL.1.5C

В «Утверждении о соответствии» должны быть идентифицированы все ПЗ и пакеты требований безопасности, о соответствии которым утверждается в ЗБ.

ASE\_CCL.1.6C

В «Утверждении о соответствии ЗБ пакету требований» должно приводиться описание любого соответствия ЗБ некоторому пакету требований; ЗБ либо описывается как соответствующее пакету требований, либо как содержащее расширенные по отношению к пакету требования.

ASE\_CCL.1.7C

В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что тип ОО согласуется с типом TOE в тех ПЗ, о соответствии которым утверждается.

ASE\_CCL.1.8C

В «Обосновании утверждений о соответствии» должно быть продемонстрировано, что изложение «Определения проблемы безопасности» согласуется с изложением «Определения проблемы безопасности» в тех ПЗ, о соответствии которым утверждается.

ASE\_CCL.1.9C

Обоснование заявления о соответствии должно демонстрировать, что формулировка определения проблемы безопасности согласуется с формулировкой определения проблемы безопасности в ПЗ-Конфигурация 1), ПЗ и любых функциональных пакетах, для которых заявляется о соответствии.

ASE\_CCL.1.10C

Обоснование заявления о соответствии должно демонстрировать, что изложение целей безопасности согласуется с изложением целей безопасности в ПЗ-Конфигурация 2), ПЗ и любом функциональном пакете, для которого заявляется о соответствии.

ASE\_CCL.1.11C

Обоснование заявления о соответствии должно демонстрировать, что изложение требований безопасности согласуется с изложением требований безопасности в Конфигурации ПЗ 3), ПЗ и любых функциональных пакетах, для которых заявляется о соответствии.

ASE\_CCL.1.12C

Заявление о соответствии для ПЗ или конфигурации ПЗ должно быть точным, строгим или доказуемым, либо представлять собой список типов соответствия.

ASE\_CCL.1.13C

Если заявление о соответствии идентифицирует набор методов оценки и действий по оценке, полученных из рабочих единиц ISO/IEC 18045, которые должны использоваться для оценки TOE, то этот набор должен включать все те, которые включены в любой пакет, ПЗ или ПЗ-модуль в конфигурация ПЗ, о соответствии которой заявляет ЗБ, и никакая другая.

Элементы действий оценщика

ASE\_CCL.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1) На практике это относится к объединению SPD, определенных в компонентах PP-Configuration.

2) На практике это относится к объединению целей безопасности, определенных в компонентах конфигурации PP.

3) На практике это относится к объединению SFR, определенных в компонентах конфигурации PP.

**9.4 Определение проблемы безопасности (ASE\_SPD)**

**9.4.1 Цели**

В данной части ЗБ определяется проблема безопасности, которая должна решаться применением TOE и его средой функционирования.

Оценка «Определения проблемы безопасности» необходима для демонстрации того, что проблема безопасности конкретного TOE и его среды функционирования четко определена.

**9.4.2 ASE\_SPD.1 Определение проблемы безопасности**

Зависимости: отсутствуют.

Элементы действий разработчика

ASE\_SPD.1.1D

Разработчик должен представить «Определение проблемы безопасности».

Элементы содержания и представления свидетельств

ASE\_SPD.1.1C

«Определение проблемы безопасности» должно включать в себя описание угроз.

ASE\_SPD.1.2C

Описание всех угроз должно проводиться в терминах источника угрозы, активов и негативного действия.

ASE\_SPD.1.3C

В «Определение проблемы безопасности» должно быть включено описание OSPs.

ASE\_SPD.1.4C

«Определение проблемы безопасности» должно содержать описание предположений относительно среды функционирования TOE.

Элементы действий оценщика

ASE\_SPD.1.1E

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

**9.5 Цели безопасности (ASE\_OBJ)**

**9.5.1 Цели**

Цели безопасности являются кратким изложением предполагаемой реакции на проблему безопасности, определенную в семействе доверия «Определение проблемы безопасности» (ASE\_SPD).

Оценка целей безопасности требуется для демонстрации того, что цели безопасности достаточно и в полной мере соответствуют «Определению проблемы безопасности» и что эта проблема четко разделена между TOE и средой его функционирования.

**9.5.2 Ранжирование компонентов**

Компоненты этого семейства ранжированы по следующему принципу – либо они описывают только цели безопасности для среды функционирования TOE, либо еще и цели безопасности для TOE.

**9.5.3 ASE\_OBJ.1 Цели безопасности для среды функционирования**

Зависимости: отсутствуют.

Элементы действий разработчика

ASE\_OBJ.1.1D

Разработчик должен представить изложение «Целей безопасности».

Элементы содержания и представления свидетельств

ASE\_OBJ.1.1C

Изложение «Целей безопасности» должно включать в себя описание целей безопасности для среды функционирования TOE.

Элементы действий оценщика

ASE\_OBJ.1.1E

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

**9.5.4 ASE\_OBJ.2 Цели безопасности**

Зависимости: ASE\_SPD.1 Определение проблемы безопасности

Элементы действий разработчика

ASE\_OBJ.2.1D

Разработчик должен предоставить «Определение целей безопасности».

ASE\_OBJ.2.2D

Разработчик должен предоставить «Обоснование целей безопасности».

Элементы содержания и представления свидетельств

ASE\_OBJ.2.1C

Изложение «Целей безопасности» должно включать в себя описание целей безопасности для ОО и для среды функционирования TOE.

ASE\_OBJ.2.2C

В «Обосновании целей безопасности» каждая цель безопасности для TOE должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, и к ПБОр, на осуществление которых направлена эта цель безопасности.

ASE\_OBJ.2.3C

В «Обосновании целей безопасности» каждая цель безопасности для TOE должна быть прослежена к угрозам, на противостояние которым направлена эта цель безопасности, к ПБОр, на осуществление которых направлена эта цель безопасности, а также к предположениям, поддерживаемым данной целью безопасности.

ASE\_OBJ.2.4C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на противостояние всем идентифицированным угрозам.

ASE\_OBJ.2.5C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности направлены на осуществление всех ПБОр.

ASE\_OBJ.2.6C

В «Обосновании целей безопасности» должно быть продемонстрировано, что цели безопасности для среды функционирования поддерживают все предположения.

Элементы действий оценщика

ASE\_OBJ.2.1E

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

**9.6 Определение расширенных компонентов (ASE\_ECD)**

**9.6.1 Цели**

Расширенные требования безопасности являются требованиями, которые основываются не на компонентах функциональных требований ISO/IEC 15048-2 или на компонентах доверия настоящего стандарта, а на расширенных компонентах: компонентах, определяемых разработчиком ПЗ.

Оценка определения расширенных компонентов необходима для того, чтобы сделать заключение, что эти компоненты определены четко и однозначно, и что они необходимы, т. е. не могут быть в полной мере выражены через существующие компоненты ISO/IEC 15048-2 или настоящего стандарта.

**9.6.2 ASE\_ECD.1 Определение расширенных компонентов**

Зависимости: отсутствуют.

Элементы действий разработчика

ASE\_ECD.1.1D

Разработчик должен представить изложение «Требований безопасности».

ASE\_ECD.1.2D

Разработчик должен представить «Определение расширенных компонентов».

Элементы содержания и представления свидетельств

ASE\_ECD.1.1C

В изложении «Требований безопасности» должны быть идентифицированы все расширенные требования безопасности.

ASE\_ECD.1.2C

В «Определении расширенных компонентов» должен определяться расширенный компонент для каждого расширенного требования безопасности.

ASE\_ECD.1.3C

В «Определении расширенных компонентов» должно указываться, как каждый расширенный компонент связан с существующими компонентами, семействами и классами ISO/IEC 15408.

ASE\_ECD.1.4C

В «Определении расширенных компонентов» должны использоваться в качестве модели представления компоненты, семейства, классы и методология ISO/IEC 15408.

ASE\_ECD.1.5C

Расширенные компоненты должны состоять из измеримых объективных элементов, чтобы была возможность продемонстрировать соответствие или несоответствие этим элементам.

Элементы действий оценщика

ASE\_ECD.1.1E

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

ASE\_ECD.1.2E

Оценщик должен подтвердить, что ни один из расширенных компонентов не может быть четко выражен с использованием существующих компонентов.

**9.7 Требования безопасности (ASE\_REQ)**

**9.7.1 Цели**

ФТБ формируют четкое, однозначное и технически правильное описание ожидаемого режима безопасности TOE. ТДБ представляют четкое, однозначное и технически правильное описание ожидаемых действий, которые будут предприняты для достижения доверия к TOE.

Оценка требований безопасности необходима для того, чтобы обеспечить их четкое, однозначное и технически правильное описание.

**9.7.2 Ранжирование компонентов**

Компоненты данного семейства ранжированы в зависимости от их изложения.

**9.7.3 ASE\_REQ.1 Установленные требования безопасности**

Зависимости: ASE\_ECD.1 Определение расширенных компонентов

Элементы действий разработчика

ASE\_REQ.1.1D

Разработчик должен представить изложение «Требований безопасности».

ASE\_REQ.1.2D

Разработчик должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

ASE\_REQ.1.1C

Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

ASE\_REQ.1.2. С

Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, используемые в ФТБ и ТДБ, должны быть определены.

ASE\_REQ.1.3C

В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

ASE\_REQ.1.4C

Все операции должны выполняться правильно.

ASE\_REQ.1.5C

Каждая зависимость от требований безопасности должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения данной зависимости.

ASE\_REQ.1.6C

Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий оценщика

ASE\_REQ.1.1E

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

**9.7.4 ASE\_REQ.2 Производные требования безопасности**

Зависимости: ASE\_OBJ.2 Цели безопасности

ASE\_ECD.1 Определение расширенных компонентов

Элементы действий разработчика

ASE\_REQ.2.1D

Разработчик должен представить «Определение требований безопасности».

ASE\_REQ.2.2D

Разработчик должен представить «Обоснование требований безопасности».

Элементы содержания и представления свидетельств

ASE\_REQ.2.1C

Изложение «Требований безопасности» должно содержать описание ФТБ и ТДБ.

ASE\_REQ.2.2C

Все субъекты, объекты, операции, атрибуты безопасности, внешние сущности и другие понятия, использующиеся в ФТБ и ТБД, должны быть определены.

ASE\_REQ.2.3C

В изложении «Требований безопасности» должны быть идентифицированы все выполненные над требованиями безопасности операции.

ASE\_REQ.2.4C

Все операции должны выполняться правильно.

ASE\_REQ.2.5C

Каждая зависимость от «Требований безопасности» должна быть либо удовлетворена, либо должно приводиться обоснование неудовлетворения зависимости.

ASE\_REQ.2.6C

В «Обосновании требований безопасности» должно быть представлено прослеживание каждого ФТБ к целям безопасности для TOE.

ASE\_REQ.2.7C

В «Обосновании требований безопасности» должно быть продемонстрировано, что ФТБ обеспечивают выполнение всех целей безопасности для TOE.

ASE\_REQ.2.8C

В «Обосновании требований безопасности» должно приводиться пояснение того, почему выбраны определенные ТДБ.

ASE\_REQ.2.9C

Изложение «Требований безопасности» должно быть внутренне непротиворечивым.

Элементы действий оценщика

ASE\_REQ.2.1E

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

**9.8 Краткая спецификация ОО (ASE\_TSS)**

**9.8.1 Цели**

Краткая спецификация TOE позволяет оценщикам и потенциальным потребителям получить общее представление о реализации TOE.

Оценка краткой спецификации TOE необходима для того, чтобы сделать заключение о том, в достаточной ли мере в ней описано, каким образом TOE:

- выполняет ФТБ;

- защищает себя от вмешательства, логического искажения и обхода;

а также согласуется ли краткая спецификация TOE с другими словесными описаниями TOE.

**9.8.2 Ранжирование компонентов**

Компоненты этого семейства ранжированы в зависимости от того, требуется ли в краткой спецификации указать только то, каким образом TOE выполняет ФТБ, или в ней необходимо указать также, каким образом TOE защищает себя от логического искажения и обхода. Это дополнительное описание может использоваться в особых случаях, когда имеется особая проблема архитектуры безопасности TOE.

**9.8.3 ASE\_TSS.1 Краткая спецификация** TOE

Зависимости: ASE\_INT.1 Введение ЗБ

ASE\_REQ.1 Установленные требования безопасности

ADV\_FSP.1 Базовая функциональная спецификация

Элементы действий разработчика

ASE\_TSS.1.1D

Разработчик должен представить краткую спецификацию TOE.

Элементы содержания и представления свидетельств

ASE\_TSS.1.1C

Краткая спецификация TOE должна описывать, каким образом TOE выполняет каждое ФТБ.

Элементы действий оценщика

ASE\_TSS.1.1E

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

ASE\_TSS.1.2E

Оценщик должен подтвердить, что краткая спецификация TOE не противоречит «Аннотации TOE» и «Описанию TOE».

**9.8.4 ASE\_TSS.2 Краткая спецификация TOE** **с аннотацией проекта архитектуры**

Зависимости: ASE\_INT.1 Введение ЗБ

ASE\_REQ.1 Установленные требования безопасности

ADV\_ARC.1 Описание архитектуры безопасности

Элементы действий разработчика

ASE\_TSS.2.1D

Разработчик должен представить краткую спецификацию TOE.

Элементы содержания и представления свидетельств

ASE\_TSS.2.1C

Краткая спецификация TOE должна описывать, каким образом TOE выполняет каждое ФТБ.

ASE\_TSS.2.2C

Краткая спецификация TOE должна описывать, каким образом TOE противостоит попыткам вмешательства и логического искажения.

ASE\_TSS.2.3C

Краткая спецификация TOE должна описывать, каким образом TOE противостоит попыткам обхода защиты.

Элементы действий оценщика

ASE\_TSS.2.1E

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

ASE\_TSS.2.2E

Оценщик должен подтвердить, что краткая спецификация TOE не противоречит «Аннотации TOE» и «Описанию TOE».

**9.9 Согласованность цели безопасности составного продукта (ASE\_COMP)**

**9.9.1 Цели**

Целью этого семейства является определение того, не противоречит ли ЗБ составного продукта 4) ЗБ соответствующего базового компонента 5),6).

**9.9.2 Ранжирование компонентов**

Данное семейство содержит только один компонент.

**9.9.3 Замечания по применению**

ЗБ на составное продукта должно быть записано и оценено.

Оценщик составного продукта должен проверить, не противоречит ли ЗБ составной продукции ЗБ соответствующего базового компонента. В частности, это означает, что оценщик составного продукта должен проверить ЗБ составного продукта и ЗБ базового компонента на наличие противоречивых предположений, совместимости целей безопасности, требований безопасности и функциональных возможностей безопасности, необходимых зависимому компоненту.

Спонсор оценки составного продукта должен обеспечить доступность ЗБ базового компонента для разработчика зависимого компонента, для оценщика составного продукта и для органа по оценке составного продукта. Информации, доступной в общедоступной версии базового компонента ЗБ, может быть недостаточно.

Эти указания по применению помогают разработчику создать, а оценщику проанализировать ЗБ составного продукта и описать общую методологию для него.

Для создания составного изделия ЗБ разработчику необходимо выполнить следующие действия:

Шаг 1: Разработчик формулирует предварительное ЗБ для составного продукта (композитное ЗБ), используя стандартный свод правил. Композитное ЗБ может быть составлено независимо от ЗБ соответствующего базового компонента составного продукта (базового ЗБ), по крайней мере, до тех пор, пока нет официальных заявлений о соответствии ПЗ.

Шаг 2: Разработчик определяет перекрытие между базовым и составным ЗБ путем анализа и сравнения их соответствующих функциональных возможностей безопасности TOE (ФБО) 7) 8).

Шаг 3: Разработчик определяет, при каких условиях он может доверять и полагаться на базовый компонент ФБО, используемый составным ЗБ без новой проверки.

Выполнив эти действия, разработчик завершает предварительное ЗБ на композитное изделие.

\_\_\_\_\_\_\_\_\_\_\_\_\_

4) В дальнейшем обозначается как составной продукт ЗБ или составное ЗБ.

5) В дальнейшем обозначается базовым компонентом ЗБ или базовым ЗБ.

6) Как правило, цель безопасности выражает политику безопасности для определенного TOE.

7) Потому что ФБО обеспечивают реализацию цели безопасности (вместе с организационными мерами, обеспечивающими реализацию целей безопасности для операционной среды TOE).

8) Сравнение должно выполняться на уровне абстракции ФТБ. Если разработчик определяет функциональные группы безопасности (TSF-группы) в части TSS своей цели по безопасности, оценщику следует также рассмотреть их, чтобы лучше понять контекст услуг безопасности, предлагаемых TOE.

Не обязательно, чтобы составной продукт и связанный с ним базовый компонент оценивались в соответствии с одним и тем же изданием ISO/IEC 15408. Это связано с тем, что зависимый компонент составного продукта может полагаться на некоторые службы безопасности базового продукта. компонента, если (i) уровень доверия базового компонента соответствует предполагаемому уровню доверия составного продукта и (ii) оценка базового компонента действительна (т. е. принята органом по оценке базового компонента) и актуальна. Эквивалентность отдельных компонентов доверия (и, следовательно, уровней доверия), принадлежащих разным изданиям серии ISO/IEC 15408, должна быть установлена/признана органом по оценке составного продукта.

Если заявлено соответствие ПЗ, например. ЗБ составного продукта заявляет о соответствии ПЗ (который, возможно, заявляет о соответствии другому ПЗ), проверка согласованности может быть сведена к элементам ЗБ, которые еще не охвачены этими ПЗ. Однако в целом факта соблюдения ПЗ недостаточно, чтобы избежать несоответствий. Предположим следующую ситуацию, где → означает «соответствует»:

составное ST → РР 1 → РР2 ← базовое ST

ПЗ 1 может требовать любого вида соответствия 9), но это не влияет на «дополнительные элементы», которые базовое ЗБ может вводить помимо ПП 2. В заключение следует отметить, что эти дополнения не обязательно согласуются с дополнениями составного ЗБ, выбранными за пределами ПП 1. Не существует сценария, обеспечивающего их согласованность «по конструкции».

Обратите внимание, что согласованность может не заключаться в прямом сопоставлении: цели для среды базового компонента могут стать целями для составного TOE.

**9.9.4 ASE\_COMP.1 Согласованность цели безопасности (ЗБ)**

Зависимости: Зависимости: отсутствуют.

Элементы действий разработчика

ASE\_COMP.1.1D

Разработчик должен предоставить заявление о совместимости между составным продуктом ЗБ и базовым компонентом ЗБ. Это заявление может быть предоставлено в составе составного продукта ЗБ.

Элементы контента и презентации

ASE\_COMP.1.1C

Заявление о совместимости должно описывать разделение базового компонента-ФБО на соответствующие базовые компоненты-ФБО, используемые составным объектом безопасности продукта и другими.

ASE\_COMP.1.2C

Заявление о совместимости между целью безопасности составного продукта и задачей безопасности базового компонента должно показывать (например, в форме сопоставления), что цели безопасности составного продукта и соответствующего базового компонента совпадают, т.е. что не существует конфликта между средами безопасности, целями безопасности и требованиями безопасности составного продукта ЗБ и базового компонента ЗБ. Это может быть обеспечено путем указания соответствующих элементов непосредственно в составном задании безопасности продукта с последующим, при необходимости, пояснительным текстом.

Элементы действий оценщика

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

9) Например. «строгий», «точный» или «демонстрируемый» в соответствии с серией ISO/IEC 15408.

ASE\_COMP.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

## **10 Класс ADV: Разработка**

**10.1 Общие положения**

Требования класса «Разработка» предоставляют информацию об объекте оценки. Сведения, по лученные путем изучения этой информации, служат основой для проведения анализа уязвимостей и тестирования TOE в соответствии с описанием, представленным в классах AVA «Анализ уязвимостей» и АТЕ «Тестирование».

Класс «Разработка» содержит шесть семейств доверия для структурирования и представления ФБО на различных уровнях детализации. Эти семейства включают в себя:

- требования к описанию (на различных уровнях детализации) проекта и реализации ФТБ (ADV\_FSP «Функциональная спецификация», ADV\_TDS «Проект 00», ADV\_INT «Представление реализации»);

- требования к описанию архитектурно-ориентированных особенностей разделения доменов, обеспечения собственной защиты ФБО и невозможности обхода ФБО (ADV\_ARC «Архитектура безопасности);

- требования к модели политики безопасности и к прослеживанию соответствия между моделью политики безопасности и функциональной спецификацией (ADV\_SPM «Моделирование политики безопасности»);

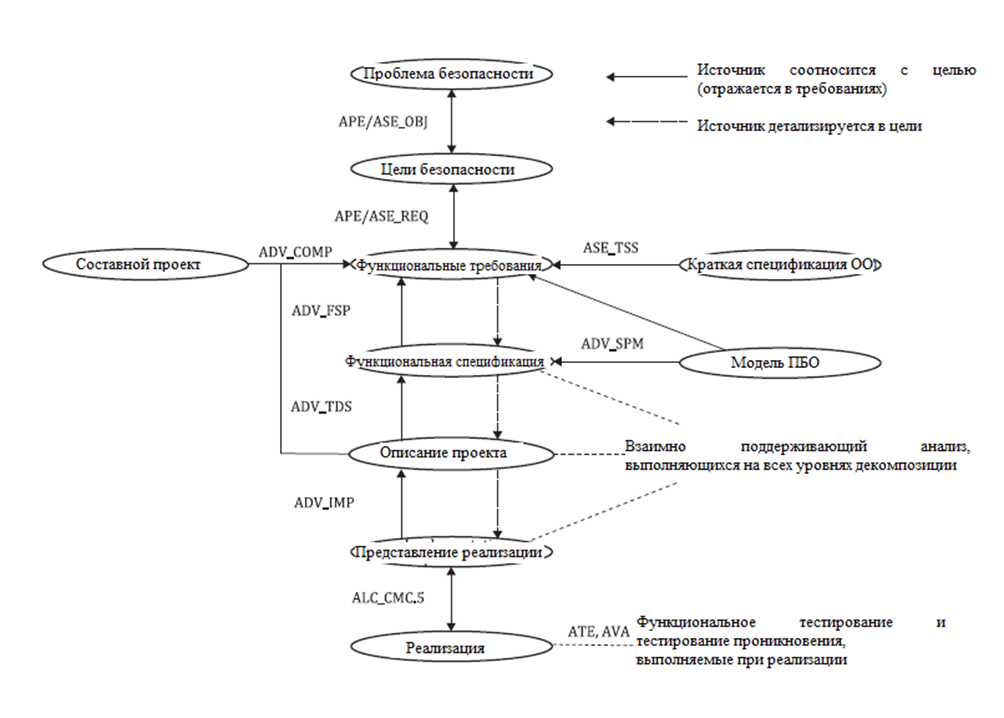
- требования к внутренней структуре ФБО, которые охватывают такие аспекты, как модульность,

деление на уровни и минимизацию сложности (ADV\_INT «Внутренняя структура ФБО»).

При документировании функциональных возможностей безопасности TOE необходимо продемонстрировать два основных свойства. Первое свойство заключается в том, что определенная функциональная возможность выполняется правильно, согласно спецификации. Второе свойство, которое несколько сложнее продемонстрировать, заключается в том, что невозможно использовать TOE так, чтобы это привело к искажению или обходу функциональных возможностей безопасности. Два этих свойства требуют применения различных подходов к их анализу, поэтому семейства класса ADV «Разработка» структурированы таким образом, чтобы поддерживать реализацию этих подходов. Семейства «Функциональная спецификация» (ADV\_FSP), «Проект TOE» (ADV\_TDS), «Представление реализации» (ADV\_IMP) и «Моделирование политики безопасности» (ADV\_SPM) направлены на представление первого свойства: спецификации функциональных возможностей безопасности. Семейства «Архитектура безопасности» (ADV\_ARC) и «Внутренняя структура ФБО» (ADV\_INT) направлены на представление второго свойства: спецификации проекта TOE, показывающей, что определенную функциональную возможность безопасности невозможно исказить или обойти. Следует отметить, что необходимо реализовать оба этих свойства: чем больше уверенности в том, что эти свойства реализованы, тем больше уровень доверия к TOE, приведенного на рисунке 7. Компоненты в этих семействах организованы таким образом, что при использовании компонентов, находящихся выше по иерархии, обеспечивается больший уровень доверия.

Парадигма для семейств данного класса, связанных с первым свойством, заключается в декомпозиции проекта. На самом верхнем уровне — функциональная спецификация ФБО в терминах интерфейсов ФБО (описывающая, что именно выполняют ФБО в части запросов к сервисам ФБО и реакции на эти запросы), которая проводит декомпозицию ФБО на подсистемы (в зависимости от сложности TOE и от того, какой уровень доверия необходим) и описывает то, каким образом ФБО выполняет свои функциональные возможности (на уровне детализации, соответствующем уровню доверия), а также демонстрирует реализацию ФБО. Также может быть представлена формальная модель режима безопасности. Все уровни декомпозиции используются для того, чтобы сделать заключение о полноте и точности всех прочих уровней, что обеспечивает их взаимную поддержку. Требования для различных представлений ФБО выделены в разные семейства, чтобы позволить разработчику ПЗ/ЗБ определить, какие именно представления ФБО необходимы. В соответствии с выбранным уровнем будет устанавливаться, какое доверие требуется/достигается.

На рисунке 7 показаны взаимосвязи между различными представлениями ФБО по классу ADV «Разработка», а также их взаимосвязи с другими классами. Как показано на этом рисунке, классы АРЕ «Оценка ПЗ» и ASE «Оценка ЗБ» определяют требования соответствия между ФТБ и целями безопасности для TOE. Класс ASE «Оценка ЗБ» также определяет требования к соответствию между целями безопасности, функциональными требованиями и краткой спецификацией TOE, в которой объясняется, каким образом TOE соответствует функциональным требованиям. Действия оценщика в соответствии с элементом ALC\_CMC.5.2.E включают в себя верификацию того, что ФБО, тестируемые по классам АТЕ «Тестирование» и AVA «Оценка уязвимостей», являются фактически теми же ФБО, которые описаны на всех уровнях декомпозиции в классе доверия ADV «Разработка».



**Рисунок 7 — Взаимосвязи между компонентами класса ADV и с другими семействами**

Требования для всех других соответствий, показанных на рисунке 7, определены в классе ADV «Разработка». Семейство ADV\_SPM «Моделирование политики безопасности» определяет требования к выбранным ФТБ формальной модели и предоставляет соответствие между функциональной спецификацией и формальной моделью. Каждое семейство, относящееся к конкретному представлению ФБО (т.е. ADV\_FSP «Функциональная спецификация», ADV\_TDS «Проект 00» и ADV\_IMP «Представление реализации»), определяет требования, относящиеся к соответствию между представлением ФБО и ФТБ. Каждый элемент декомпозиции должен точно отображать все прочие элементы (т.е. все элементы декомпозиции должны быть взаимоподдерживающими); разработчик обеспечивает прослеживание между представлениями ФБО и ФТБ в последних элементах компонентов под рубрикой «Элементы содержания и представления свидетельств». Доверие относительно этого фактора достигается в процессе анализа каждого из уровней декомпозиции путем ссылки конкретного уровня на другие уровни декомпозиции (рекурсивным образом) в процессе анализа этого конкретного уровня декомпозиции; оценщик верифицирует их соответствие как часть выполнения второго элемента группы компонентов «Элементы действий оценщика». Полученная от этих уровней декомпозиции информация служит основой для усилий по функциональному тестированию и тестированию проникновения.

Семейство ADV\_INT «Внутренняя структура ФБО» не представлено на рисунке 10, поскольку оно связано с внутренней структурой ФБО и имеет лишь косвенное отношение к процессу уточнения представлений ФБО. Также не представлено и семейство ADV\_RCR «Архитектура безопасности», которое имеет большее отношение к целостности архитектуры, чем к представлению ФБО. Оба этих семейства, ADV\_INT «Внутренняя структура» и ADV\_RCR «Архитектура безопасности», относятся к анализу свойства TOE, которое заключается в невозможности искажения или обхода функциональных возможностей безопасности TOE.

Функциональные возможности безопасности ОО (ФБО) представляют собой совокупность всех функциональных возможностей различных частей TOE, на которых полагаются с целью осуществления ФТБ. ФБО включают в себя как функции, которые непосредственно осуществляют ФТБ, так и функции, которые, не осуществляя ФТБ непосредственно, косвенно содействуют осуществлению ФТБ. Сюда же включаются и функциональные возможности, при недостаточности или отсутствии которых возможны нарушения ФТБ. К таким функциональным возможностям относятся и те части TOE, которые на стадии запуска TOE должны привести ФБО в первоначальное безопасное состояние.

При разработке компонентов семейств класса ADV «Разработка» применялось несколько важных принципов. Эти принципы кратко рассматриваются в данном разделе, а более подробно объясняются в замечаниях по применению для семейств.

Самый важный принцип заключается в том, что при получении большего объема информации можно получить большее доверие тому, что функциональные возможности безопасности: a) правильно реализованы, b) не могут быть искажены, c) не могут быть подвержены обходу. Это осуществляется путем верификации того, что документация составлена верно и не противоречит иной документации, а также посредством представления информации, которую можно использовать для подтверждения того, что проводимые тестовые испытания (как функциональное тестирование, так и тестирование проникновения) являются исчерпывающими. Это отражается в ранжировании компонентов семейств. В общем случае компоненты ранжированы в зависимости от того, какой объем информации должен быть представлен (и впоследствии проанализирован).

Хотя это справедливо не для всех TOE, но в большинстве случаев документ, описывающий функциональные возможности безопасности, является достаточно сложным, и некоторые его части требуют более тщательного изучения, чем другие. Выявление таких частей осуществляется, к сожалению, субъективным образом, поэтому терминология и компоненты доверия определяются так, что при увеличении уровня доверия ответственность за выявление тех частей ФБО, которые нужно проанализировать детально, переходит от разработчика к оценщику. Для описания данного принципа вводится специальная терминология, представленная далее. Следует отметить, что в семействах класса эта терминология используется для описания связанных с ФТБ частями TOE (т.е. для элементов и шагов оценивания семейств ADV\_FSP «Функциональная спецификация», ADV\_TDS «Проект TOE», ADV\_IMP «Представление реализации»). Хотя общий принцип (о том, что некоторые части TOE являются более интересными для анализа) применим и к другим семействам, критерии излагаются по-разному для получения требуемого уровня доверия.

Все части ФБО являются значимыми для безопасности, что означает, что они должны обеспечивать безопасность TOE согласно ФТБ и требованиям разделения доменов и невозможности обхода ФБО. Один из аспектов важности ФБО для безопасности — в какой степени ФБО обеспечивают выполнение требований безопасности. Так как различные части TOE выполняют различные роли (или вовсе не играют никакой явной роли) в осуществлении требований безопасности, значимость этих функциональных возможностей для выполнения ФТБ можно представить в виде определенного ряда. В начале его находятся те части TOE, которые осуществляют выполнение ФТБ. Такие части непосредственно участвуют в реализации тех или иных ФТБ в TOE. Такие ФТБ относятся ко всем функциональным возможностям, которые представлены одним из ФТБ, содержащимся в ЗБ. Следует отметить, что значимость функциональных возможностей для обеспечения выполнения ФТБ невозможно выразить количественно. Например, в механизме реализации Дискреционного управления доступом (ДУД), в узком смысле к осуществлению выполнения ФТБ можно отнести несколько строк кода, которые обеспечивают проверку соответствия атрибутов безопасности субъекта атрибутам объекта. При более широком рассмотрении к этой же категории можно добавить объект программного обеспечения (например, функцию на языке программирования Си), содержащий несколько строк программного кода. При еще более широком рассмотрении туда же включаются операторы вызова функции языка программирования Си, так как именно они отвечают за обеспечение принятия решения о доступе после проверки атрибутов. Еще более широкое рассмотрение включает любой фрагмент кода в дереве вызовов (или программный эквивалент в зависимости от используемого языка программирования) данной функции языка программирования Си (например, функции сортировки, которая проводит сортировку списка контроля и управления доступом по алгоритму первого совпадения). Иногда компонент является не столько осуществляющим выполнение политики безопасности, сколько играющим роль поддержки] такие компоненты называются поддерживающими выполнение ФТБ. Одна из характеристик функциональных возможностей, поддерживающих ФТБ, заключается в том, что они должны обеспечивать стабильную правильность реализации ФТБ посредством функционирования без ошибок. Такие функциональные возможности могут зависеть от функций, осуществляющих ФТБ, но в основном на функциональном уровне, например: управление памятью, управление буферизацией и т.д. Далее по ряду значимости для безопасности находятся функциональные возможности, называемые не влияющими на выполнение ФТБ. Они не участвуют в реализации ФТБ, а частью ФБО являются, скорее всего, из-за среды их функционирования. Это, например, любой программный код, запущенный в операционной системе в привилегированном аппаратном режиме. Его следует рассматривать как часть ФБО потому, что в случае искажения (или в случае замены вредоносным кодом) он может нарушить правильность выполнения ФТБ в силу того, что выполнялся в привилегированном режиме. Примером функциональных возможностей, не влияющих на выполнение ФТБ, может быть набор математических операций над числами с плавающей запятой, выполняемый для быстроты вычислений в режиме ядра ОС.

Семейство «Архитектура безопасности» (ADV\_ARC) служит для описания требований и анализа TOE на основе свойств разделения доменов, собственной защиты ФБО и невозможности обхода ФБО. Эти свойства имеют значение для выполнения ФТБ, так как их отсутствие приведет, скорее всего, к сбою механизмов, осуществляющих реализацию ФТБ. Функциональные возможности этих свойств и проект, относящийся к ним, при этом рассматриваются не как часть описанного выше ряда значимости, а отдельно — в силу того, что они совершенно иные по сути и к их анализу предъявляются другие требования.

Разница в анализе реализации ФТБ (функциональных возможностей, осуществляющих и поддерживающих выполнение ФТБ) и реализации некоторых фундаментальных свойств безопасности TOE (к которым относится инициализация, собственная защита ФБО и невозможность обхода ФБО) заключается в том, что функциональные возможности, имеющие отношение к ФТБ, являются более или менее явными и относительно легко тестируемыми, а вышеупомянутые свойства требуют анализа гораздо более широкого набора функций на различных уровнях. Кроме того, глубина требуемого анализа данных свойств будет варьироваться в зависимости от проекта TOE. Семейства класса ADV «Разработка» обеспечивают выполнение этого отдельным семейством (ADV\_ARC «Архитектура безопасности»), которое посвящено анализу требований инициализации, собственной защиты ФБО и невозможности обхода ФБО, в то время как другие семейства связаны с анализом функций, обеспечивающих поддержку выполнения ФТБ.

Даже в тех случаях, когда необходимы различные описания на разных уровнях детализации, совсем необязательно каждое представление ФБО оформлять в виде отдельного документа. Возможна ситуация, когда в одном документе выполняются 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, когда несколько представлений ФБО объединены в одном документе, разработчику следует указать, какие части документа удовлетворяют определенным требованиям.

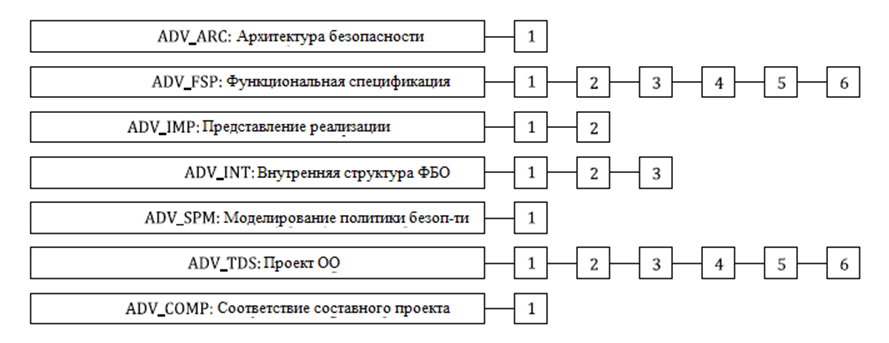
Этим классом узаконены три типа стиля изложения спецификаций: неформальный, полуформальный и формальный. Функциональная спецификация и документация по проекту TOE всегда излагаются с применением либо неформального, либо полуформального стиля изложения. Применение полуформального стиля изложения уменьшает неоднозначность в спецификациях по сравнению с неформальным стилем изложения. Кроме того, в дополнение к полуформальному представлению может потребоваться и предоставление формальной спецификации; преимущество такого требования в том, что описание ФБО несколькими способами увеличивает доверие к тому, что ФБО полно и точно определены.

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

Разница между документами неформального и полуформального стиля изложения заключается только в форматировании и способе представления: в документах полуформального стиля приводится подробный глоссарий используемых терминов и определений, применяется стандартизованная структура документа и т.д. Документы полуформального стиля изложения составляются по стандартному шаблону. В случае, если документ составляется на естественном языке, в нем следует использовать соответствующие данному языку термины и определения. Кроме того, в представление могут включаться более структурированные языковые средства или схемы (например, диаграммы потока данных, диаграммы переходных состояний, диаграммы вида «объекты-отношения», схемы представления структур данных, процессов или программ). Независимо оттого, основывается ли представление на диаграммах и схемах или на средствах естественного языка, при его составлении необходимо соблюдение определенных правил. Приводимый глоссарий должен содержать полные, подробные, точные и однозначные определения использованных в документе слов и словосочетаний; стандартизованная структура документа должна подразумевать, что при методологическом составлении документа особое внимание было уделено тому, чтобы он был максимально понятен. Следует отметить, что совершенно разные части ФБО могут описываться с использованием различных правил полуформального стиля изложения, касающихся оформления и систем обозначений (по крайней мере, пока количество различных полуформальных систем обозначений невелико), это не противоречит принципам полуформального изложения.

Формальную спецификацию излагают с использованием обозначений, основанных на известных математических понятиях, и обычно сопровождают вспомогательным пояснительным (неформальным) текстом. Эти математические понятия используются для определения синтаксиса и семантики системы обозначений и правил доказательства, поддерживающих логическое обоснование. Следует, чтобы в синтаксических и семантических правилах, регламентирующих формальную нотацию, определялось, как однозначно распознавать конструкции и определять их значение. Требуется свидетельство невозможности получения противоречивых выводов, а все правила, регламентирующие систему обозначений, необходимо определить или на них необходимо ссылаться.

На рисунке 8 показаны семейства данного класса и иерархия компонентов в семействах.



**Рисунок 8 – Декомпозиция класса ADV «Разработка»**

В случае оценки множественного доверия требования к описанию (на различных уровнях абстракции) проектирования и реализации ФТБ (ADV\_FSP, ADV\_TDS, ADV\_IMP и ADV\_COMP) будут представлены для суб-ФБО TOE. Семейство архитектур (Архитектура безопасности (ADV\_ARC)) обеспечивает требования и анализ TOE на основе свойств разделения доменов, самозащиты и невозможности обхода, которые также могут применяться к границам между суб-ФБО.

**10.2 Архитектура безопасности (ADV\_ARC)**

**10.2.1 Цели**

В настоящем семействе разработчик предоставляет «Описание архитектуры безопасности» ФБО, что позволяет провести анализ информации, который, в совокупности с другими представленными свидетельствами по ФБО, послужит подтверждением того, что ФБО обладают необходимыми свойствами. «Описание архитектуры безопасности» поддерживает выполнение неявного требования возможности анализа безопасности TOE путем изучения ФБО; в ином случае, при отсутствии полного описания архитектуры, для анализа безопасности потребуется изучение всех функциональных возможностей TOE.

**10.2.2 Ранжирование компонентов**

Семейство содержит только один компонент.

**10.2.3 Замечания по применению**

Свойства собственной защиты ФБО, разделения доменов, невозможности обхода ФБО отличаются от функций безопасности, отраженных в ФТБ ISO/IEC 15408-2, так как собственная защита и невозможность обхода не имеют непосредственно видимого интерфейса в ФБО. Они относятся к свойствам ФБО, которые достигаются посредством проекта TOE и ФБО и осуществляются правильной реализацией этих проектов.

Подход, использующийся в данном семействе, заключается в том, что разработчик проектирует и предоставляет ФБО, которые соответствуют вышеупомянутым свойствам, а также предоставляет свидетельства (в форме документации), объясняющие эти свойства ФБО. Объяснение приводится с тем же уровнем детализации, что и описание осуществляющих выполнение ФТБ элементов TOE в проекте TOE. В обязанности оценщика входит изучение представленных свидетельств в совокупности с другими свидетельствами по TOE и ФБО и вынесение заключения о том, достигается ли реализация заявленных свойств.

В спецификации функциональных возможностей безопасности, осуществляющих выполнение ФТБ (представленных в семействах ADV\_FSP «Функциональная спецификация» и ADV\_TDS «Проект TOE») не обязательно содержится описание механизмов, обеспечивающих свойства собственной защиты и невозможности обхода (например, механизмов управления памятью). Поэтому сведения, необходимые для получения доверия тому, что эти свойства выполняются, предпочтительнее представить отдельно от декомпозиции проекта ФБО, как это представлено в семействах ADV\_FSP «Функциональная спецификация» и ADV\_TDS «Проект TOE». Это не подразумевает, что в «Описании архитектуры безопасности», требуемом для данного компонента, не могут использоваться сведения, представленные в проекте декомпозиции или ссылки на него; но, скорее всего, многие детали, представленные в документации по декомпозиции, не будут значимыми для свидетельств, представленных в документе «Описание архитектуры безопасности».

Описание архитектурной целостности может быть выполнено посредством проведения разработчиком анализа уязвимостей, в процессе которого должно быть получено логическое обоснование того, что ФБО являются полными и осуществляют выполнение всех ФТБ. В случае, если целостность достигается особыми механизмами безопасности, эти механизмы тестируются в части требований глубины (ATE\_DPT); если целостность достигается только за счет архитектуры безопасности, режим ее безопасности будет тестироваться по требованиям части класса AVA «Требования оценки уязвимостей».

В данном семействе содержатся требования, предъявляемые к описанию архитектуры безопасности, которые относятся к принципам собственной защиты, разделения доменов и невозможности обхода, включая описание того, как эти принципы поддерживаются частями TOE, используемыми при инициализации ФБО.

Дополнительная информация по таким свойствам архитектуры безопасности, как обеспечение собственной защиты, разделения доменов и невозможности обхода, представлена в приложении А.1, ADV\_ARC «Дополнительные сведения по архитектуре безопасности».

**10.2.4 ADV\_ARC.1 Описание архитектуры безопасности**

Зависимости: ADV\_FSP.1 Базовая функциональная спецификация

ADV\_TDS.1 Базовый проект

Элементы действий разработчика

ADV\_ARC.1.1D

Разработчик должен спроектировать TOE и обеспечить реализацию проекта таким образом, чтобы свойства безопасности ФБО невозможно было обойти.

ADV\_ARC.1.2D

Разработчик должен спроектировать ФБО и обеспечить их реализацию таким образом, чтобы ФБО обеспечивали собственную защиту от вмешательства недоверенных сущностей.

ADV\_ARC.1.3D

Разработчик должен предоставить «Описание архитектуры безопасности» ФБО.

Элементы содержания и представления свидетельств

ADV\_ARC.1.1C

Уровень детализации «Описания архитектуры безопасности» должен соответствовать представленному в проектной документации по TOE описанию абстракций (элементов представления TOE), осуществляющих выполнение ФТБ.

ADV\_ARC.1.2C

В «Описание архитектуры безопасности» должно быть включено описание доменов безопасности, обеспеченных согласованностью ФБО с ФТБ.

ADV\_ARC.1.3C

«Описание архитектуры безопасности» должно предоставлять информацию о том, насколько процесс инициализации ФБО является защищенным.

ADV\_ARC.1.4C

В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО обеспечивают собственную защиту от вмешательства.

ADV\_ARC.1.5C

В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО не допускают возможности обхода функциональных возможностей, осуществляющих выполнение ФТБ.

Элементы действий оценщика

ADV\_ARC.1.1E

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

**10.3 Функциональная спецификация (ADV\_FSP)**

**10.3.1 Цели**

В настоящем семействе предъявляются требования к функциональной спецификации, в которой описываются интерфейсы ФБО (ИФБО). ИФБО включают в себя все способы, которыми пользователи могут вызвать тот или иной сервис ФБО (путем предоставления информации, которая обрабатывается ФБО) и соответствующую реакцию на запросы на обслуживание. Однако в функциональной спецификации не описывается, каким образом ФБО обрабатывает эти запросы или как организована связь при запросе ФБО обслуживания из среды функционирования; эта информация представлена в семействах «Проект TOE» (ADV\_TDS) и «Доверие к зависимым компонентам» (ACO\_REL) соответственно.

Данное семейство обеспечивает получение доверия непосредственно путем предоставления оценщику возможности понять, как ФБО выполняют заявленные ФТБ. Кроме того, оно обеспечивает и получение доверия косвенным образом, предоставляя исходную информацию для других классов и семейств доверия:

- для семейства ADV\_ARC «Архитектура безопасности», в котором описание ИФБО может быть использовано для получения лучшего понимания того, каким образом ФБО защищены от искажения (например, от нарушения свойств обеспечения собственной защиты и разделения доменов) и/или обхода;

- для класса АТЕ «Тестирование», в котором описание ИФБО предоставляет важную исходную информацию для проведения тестовых испытаний как разработчиком, так и оценщиком;

- для класса AVA «Анализ уязвимостей», в котором описание ИФБО используется в процессе поиска уязвимостей.

10.3.2 Ранжирование компонентов

Компоненты настоящего семейства ранжированы в зависимости от степени формализации и детализации, требуемых для описания интерфейсов ФБО.

**10.3.3 Замечания по применению**

10.3.3.1 Общие положения

После определения ИФБО (см. приложение А.2.1, «Руководства и примеры по определению ИФБО») они описываются. Для компонентов более низкого уровня разработчики составляют документацию (а оценщики проводят оценку этой документации), направленную на описание тех аспектов ОО, которые имеют большее значение для безопасности. Определяются три категории ИФБО в зависимости от степени значимости тех сервисов, к которым эти интерфейсы предоставляют доступ для заявленных ФТБ:

- если сервис, доступ к которому предоставляется интерфейсом, может быть сопоставлен с одним из ФТБ, предъявляемым к ФБО, тогда данный интерфейс относится к категории осуществляющих выполнение ФТБ. Следует отметить, что один интерфейс может обеспечивать доступ к нескольким различным сервисам и предоставлять различные результаты, некоторые из которых могут осуществлять выполнение ФТБ, а другие нет;

- интерфейсы сервисов (или сервисы, доступные при обращении к связанным с ними интерфейсам), от которых зависят функциональные возможности, осуществляющие выполнение ФТБ, но при этом от них для осуществления политики безопасности ОО требуется только правильное функционирование, относятся к категории поддерживающих выполнение ФТБ.

- интерфейсы сервисов, от которых никак не зависят функциональные возможности, осуществляющие выполнение ФТБ, относятся к не влияющим на выполнение ФТБ.

Следует отметить, что для того, чтобы интерфейс был отнесен к поддерживающим или не влияющим на выполнение ФТБ, он не должен включать в себя сервисы и результаты, осуществляющие выполнение ФТБ. Напротив, осуществляющий выполнение ФТБ интерфейс может включать поддерживающие выполнение ФТБ сервисы (например, возможность выставить время в системе может выполняться сервисом интерфейса, осуществляющего выполнение ФТБ, но если этот же интерфейс используется для отображения даты в системе, то этот сервис может быть исключительно поддерживающим выполнение ФТБ). В качестве яркого примера «исключительно поддерживающего выполнение ФТБ интерфейса» можно привести интерфейс системных вызовов, который используется как пользователями, так и частью ФБО, запускаемых от имени пользователей.

Чем больший объем информации предоставляется о ИФБО, тем больше приобретаемое доверие к тому, что данные интерфейсы правильно категорированы и проанализированы. Требования структурированы таким образом, что на самом низком уровне для описания интерфейсов, не влияющих на выполнение ФТБ, требуется только минимально необходимый объем информации для того, чтобы оценщик мог сделать заключение эффективным образом. Чем выше требуемый уровень доверия, тем больший объем информации предоставляется оценщику для того, чтобы у него было больше уверенности в проектировании.

Цель в определении этих категорий («осуществляющие ФТБ», «поддерживающие ФТБ» и «не влияющие на выполнение ФТБ») и предъявлении к каждой из них различных требований (для компонентов более низкого уровня) состоит в том, чтобы предоставить в первом приближении представление о том, на что должен быть направлен анализ, и о свидетельствах, на основании которых проводится данный анализ. Если в документации, представленной разработчиком по интерфейсам ФБО, все интерфейсы описаны на уровне детализации, определенной в требованиях, предъявляемым к интерфейсам, осуществляющим выполнение ФТБ (т. е. в случае, когда документация усиливает требования), разработчику не требуется создавать отдельное свидетельство для соответствия этим требованиям. Аналогично, так как разделение интерфейсов по категориям нужно только для того, чтобы распределить виды интерфейсов по строгости предъявляемым к их описаниям требованиям, от разработчика не требуется вносить изменения в свидетельства только для того, чтобы классифицировать имеющиеся интерфейсы по описанным выше категориям. Основная цель такого разделения заключается в том, чтобы позволить разработчикам с менее развитой методологией разработки (что приводит к появлению таких недостатков как излишне детализированная документация по проекту и интерфейсам) предоставлять только необходимые свидетельства без лишних затрат.

В последнем элементе группы «С» («Элементы содержания и представления свидетельств») каждого компонента семейства представлено прямое соответствие между ФТБ и функциональной спецификацией;

в нем отражается, какие интерфейсы используются для выполнения каждого требуемого ФТБ. В случаях, когда в ЗБ содержатся такие функциональные требования, как представленные в ISO/IEC 15408-2 в компоненте «Защита остаточной информации» (FDP\_RIP), функциональные возможности которых не могут проявлять себя в ИФБО, эти ФТБ должны быть определены в функциональной спецификации и/или прослеживании; включение их в функциональную спецификацию поможет обеспечить уверенность в том, что они не будут упущены из виду на более низких уровнях декомпозиции, где они будут иметь важное значение для безопасности

10.3.3.2 Детализация интерфейсов

Предъявляются определенные требования к тому, с какой детализацией следует представлять информацию об ИФБО. Согласно этим требованиям, интерфейсы специфицируются (на разных уровнях детализации) в терминах назначения интерфейса, метода использования, параметров, описаний параметров и сообщений об ошибках.

Назначение интерфейса включает в себя высокоуровневое описание основной цели интерфейса (например, обработка команд графического интерфейса пользователя, получение сетевых пакетов, обеспечение вывода на печать и т.п.).

Метод использования интерфейса описывает предполагаемый метод использования конкретного интерфейса. Такое описание рекомендуется основывать на различных взаимодействиях, которые доступны для данного интерфейса. Например, если в качестве интерфейса используется командный процессор оболочки ОС Unix, то взаимодействиями данного интерфейса будут являться команды «Is» (просмотр списка файлов), «mv» (перемещение файлов) и «ср» (копирование файлов). Метод использования для каждого взаимодействия описывает функциональные возможности данного взаимодействия (что именно оно делает), реакцию интерфейса на определенные действия (например, вызов программистом интерфейса прикладных программ, изменение пользователем операционной системы Windows настроек реестра и т.п.), а также влияние этой реакции на другие интерфейсы (например, создание записи в журнале аудита).

Параметры — это подробные исходные данные и данные на выходе интерфейса, которые управляют режимом работы интерфейса. Например, параметрами являются аргументы (независимые переменные), поставляемые интерфейсу прикладных программ; различные поля в пакетах данного сетевого протокола; индивидуальные значения ключей в реестре ОС Windows; сигналы на контактах микросхемы; параметры, которые можно присвоить команде Is и т.д. Параметры «идентифицируются» путем предоставления простого списка того, что они из себя представляют.

Описание параметра предоставляет содержательную информацию о параметре. Например, приемлемое описание параметра интерфейса foo(i) — «параметр i является целым числом, которое отражает число пользователей, вошедших в систему в настоящий момент». Описание вида «параметр i является целым числом» является неприемлемым.

Описание действий интерфейса включает в себя представление функциональных возможностей данного интерфейса (что он делает). Это описание должно быть более детализованным, чем описание назначения интерфейса, т. к. в назначении прописывается только то, для чего может потребоваться использовать данный интерфейс, а в «действиях» отражаются все выполняемые интерфейсом функции.

Такие действия могут быть как относящимися к ФТБ, так и не относящимися к ним. В тех случаях, когда действия интерфейса не относятся к ФТБ, приводится их краткое описание, которое только подтверждает факт того, что действия не относятся к ФТБ.

Описание сообщений об ошибках включает в себя описание состояния, вызвавшего сообщение об ошибке, содержание сообщения и значение любых кодовых обозначений ошибок. Сообщение об ошибке генерируется ФБО для извещения о возникновении некой проблемы или нестабильности работы. Требования данного семейства предъявляются к различным видам сообщений об ошибках:

- сообщение о «непосредственных» ошибках — это имеющая отношение к безопасности реакция, возникающая при вызове особого ИФБО;

- «косвенную» ошибку нельзя связать с вызовом конкретного ИФБО, поскольку возникает такая ошибка из-за некоторого состояния всей системы в целом (например, из-за нехватки ресурсов, нарушения взаимодействий и т.п.). Также к косвенным ошибкам относятся все ошибки, не имеющие отношения к безопасности;

- к «прочим» ошибкам относятся любые другие ошибки, которые могут встретиться в коде программы. Например, использование фрагмента кода проверки условий, который проверяет наличие логически невозможных условий (например, заключительный «else» после списка операторов «case»), обеспечивается для генерации обобщенного сообщения обо всех ошибках такого рода, присутствующих в коде; не следует, чтобы в функционирующем TOE такие сообщения об ошибках были видны пользователю.

Пример функциональной спецификации приведен в приложении А.2.3.

10.3.3.3 Компоненты данного семейства

Увеличение доверия путем увеличения полноты и точности спецификации интерфейсов отражается в документации, требуемой от разработчика, как детально описывается в иерархических компонентах данного семейства.

В компоненте ADV\_FSP.1 «Базовая функциональная спецификация» единственной требуемой документацией является определение параметров всех ИФБО и высокоуровневое описание интерфейсов, осуществляющих и поддерживающих выполнение ФТБ. Для обеспечения некоторого доверия тому, что «важные» аспекты ФБО верно характеризуют все ИФБО, от разработчика требуется представить информацию о назначении и методе использования, а также о параметрах, поддерживающих и осуществляющих выполнение ФТБ интерфейсов.

В компоненте ADV\_FSP.2 «Детализация вопросов безопасности в функциональной спецификации» от разработчика требуется представить информацию о назначении и методах использования, а также параметры и описание параметров для всех ИФБО. Кроме того, для ИФБО, обеспечивающих безопасность, разработчик обязан описать обеспечивающие безопасность действия и сообщения о не посредственных ошибках.

В компоненте ADV\_FSP.3 «Функциональная спецификация с полной аннотацией» разработчик должен, в дополнение к информации, требуемой компонентом ADV\_FSP.2, предоставить в достаточном объеме информацию о действиях, поддерживающих выполнение ФТБ или не влияющих на их выполнение для того, чтобы продемонстрировать, что эти действия не являются осуществляющими выполнение ФТБ. Кроме того, разработчик должен задокументировать все сообщения о непосредственных ошибках, возникающих в результате вызова ИФБО, осуществляющих выполнение ФТБ.

В компоненте ADV\_FSP.4 «Полная функциональная спецификация» описания всех ИФБО — осуществляющих, поддерживающих, не влияющих на выполнение ФТБ — должны быть представлены в равной степени детализации, включая сообщения обо всех непосредственных ошибках.

В компоненте ADV\_FSP.5 «Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках» в описания ИФБО также включается информация об ошибках, возникающих не в результате вызова ИФБО.

В компоненте ADV\_FSP6 «Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией» в описания, помимо информации, требуемой компонентом ADV\_FSP.5, включаются все остальные сообщения об ошибках. Кроме того, разработчик должен дополнительно предоставить формальное описание ИФБО. Таким образом обеспечивается альтернативное представление ИФБО, которое может помочь выявить несоответствия или неполноту спецификации.

**10.3.4 ADV\_FSR1 Базовая функциональная спецификация**

Зависимости: отсутствуют.

Элементы действий разработчика

ADV\_FSP.1.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSP.1.2D

Разработчик должен представить прослеживание функциональной спецификации к ФТБ.

Элементы содержания и представления свидетельств

ADV\_FSP.1.1C

В функциональной спецификации должны описываться назначение и метод использования для каждого из ИФБО, осуществляющих или поддерживающих выполнение ФТБ.

ADV\_FSP.1.2C

В функциональной спецификации должны быть идентифицированы все параметры, связанные с каждым ИФБО, осуществляющим или поддерживающим ФТБ.

ADV\_FSP.1.3C

В функциональной спецификации должно приводиться обоснование неявного категорирования интерфейсов как не влияющих на выполнение ФТБ.

ADV\_FSP.1.4C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.1.1E

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

ADV\_FSP.1.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности TOE.

**10.3.5 ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации**

Зависимости: ADV\_TDS.1 Базовый проект

Элементы действий разработчика

ADV\_FSP.2.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSP.2.2D

Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV\_FSP.2.1C

В функциональной спецификации должны быть полностью представлены ФБО.

ADV\_FSP.2.2C

В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV\_FSP.2.3C

В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV\_FSP.2.4C

Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание связанных с данным ИФБО действий, осуществляющих выполнение ФТБ.

ADV\_FSP.2.5C

Для ИФБО, осуществляющих выполнение ФТБ, функциональная спецификация должна содержать описание сообщений о непосредственных ошибках, возникающих в результате функционирования, связанного с действиями, осуществляющими выполнение ФТБ.

ADV\_FSP.2.6C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.2.1E

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

ADV\_FSP.2.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

**10.3.6 ADV\_FSP.3 Функциональная спецификация с полной аннотацией**

Зависимости: ADV\_TDS.1 Базовый проект

Элементы действий разработчика

ADV\_FSP.3.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSP.3.2D

Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV\_FSP.3.1C

В функциональной спецификации должны быть полностью представлены ФБО.

ADV\_FSP.3.2C

В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV\_FSP.3.3C

В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV\_FSP.3.4C

Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание связанных с данным ИФБО действий, осуществляющих выполнение ФТБ.

ADV\_FSP.3.5C

Для каждого ИФБО, осуществляющего выполнение ФТБ, функциональная спецификация должна содержать описание сообщений о непосредственных ошибках, возникающих в результате влияющих на безопасность эффектов и нештатных ситуаций, связанных с вызовом данного ИФБО.

ADV\_FSP.3.6C

В функциональной спецификации должны быть приведены все связанные с каждым ИФБО действия, поддерживающие или не влияющие на выполнение ФТБ.

ADV\_FSP.3.7C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.3.1E

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

ADV\_FSP.3.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

**10.3.7 ADV\_FSP.4 Полная функциональная спецификация**

Зависимости: ADV\_TDS.1 Базовый проект

Элементы действий разработчика

ADV\_FSP.4.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSP.4.2D

Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV\_FSP.4.1C

В функциональной спецификации должны быть полностью представлены ФБО.

ADV\_FSP.4.2C

В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV\_FSP.4.3C

В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV\_FSP.4.4C

В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV\_FSP.4.5C

Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV\_FSP.4.6C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.4.1E

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

ADV\_FSP.4.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

**10.3.8 ADV\_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках**

Зависимости: ADV\_TDS.1 Базовый проект

ADVJMP.1 Представление реализации ФБО

Элементы действий разработчика

ADV\_FSP.5.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSP.5.2D

Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV\_FSP.5.1C

В функциональной спецификации должны быть полностью представлены ФБО.

ADV\_FSP.5.2C

Функциональная спецификация должна содержать полуформальное описание ИФБО.

ADV\_FSP.5.3C

В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV\_FSP.5.4C

В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV\_FSP.5.5C

В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV\_FSP.5.6C

Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV\_FSP.5.7C

Функциональная спецификация должна содержать описание всех сообщений об ошибках, возникающих не в результате вызова ИФБО.

ADV\_FSP.5.8C

Функциональная спецификация должна содержать обоснование каждого сообщения об ошибке, содержащегося в реализации ФБО, но не являющегося результатом вызова ИФБО.

ADV\_FSP.5.9C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.5.1E

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

ADV\_FSP.5.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

**10.3.9 ADV\_FSP.6 Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией**

Зависимости: ADV\_TDS.1 Базовый проект

ADV\_IMR1 Представление реализации ФБО

Элементы действий разработчика

ADV\_FSR6.1D

Разработчик должен представить функциональную спецификацию.

ADV\_FSR6.2D

Разработчик должен представить формальное представление функциональной спецификации ФБО.

ADV\_FSP.6.3D

Разработчик должен представить прослеживание функциональной спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV\_FSP.6.1C

В функциональной спецификации должны быть полностью представлены ФБО.

ADV\_FSP.6.2C

Функциональная спецификация должна содержать формальное описание ИФБО.

ADV\_FSP.6.3C

В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV\_FSP.6.4C

В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV\_FSP.6.5C

В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV\_FSP.6.6C

Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV\_FSP.6.7C

Функциональная спецификация должна содержать описание всех сообщений об ошибках, содержащихся в представлении реализации ФБО.

ADV\_FSP.6.8C

Функциональная спецификация должна содержать обоснование каждого сообщения об ошибках, содержащегося в реализации ФБО, но при этом не описанного в функциональной спецификации, и того, почему эти сообщения об ошибках не связаны с ИФБО.

ADV\_FSP.6.9C

В формальном представлении функциональной спецификации ФБО должно быть изложено формальное описание ИФБО, дополненное, где это необходимо, неформальным пояснительным текстом.

ADV\_FSP.6.10C

В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV\_FSP.6.1E

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

ADV\_FSP.6.2E

Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

**10.4 Представление реализации (ADV\_IMP)**

**10.4.1 Цели**

Семейство «Представление реализации» (ADV\_IMP) предназначено для того, чтобы разработчик сделал доступным представление реализации (а на более высоких уровнях — саму реализацию) ОО в форме, которая может быть проанализирована оценщиком. Представление реализации используется при проведении действий по анализу и в рамках других семейств (например, при анализе проекта ОО) для того, чтобы продемонстрировать, что ОО соответствует своему проекту, а также для создания основы для проведения исследований по другим областям оценки (например, для поиска уязвимостей). Ожидается, что представление реализации будет выполнено в такой форме, чтобы в нем были зафиксированы процессы внутреннего содержания ФБО в виде исходного текста программ, микропрограмм, схем аппаратных средств и/или программного кода модели интегральных схем или размещения данных.

**10.4.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы в зависимости от полноты реализации, которая прослеживается к описанию проекта ОО.

**10.4.3 Замечания по применению**

Примерами частей представления реализации являются: исходный текст программы или схема аппаратного средства и/или программный код модели интегральных схем или размещения данных, которые используются для построения действующего оборудования. Важно отметить, что хотя представление реализации должно быть доступно оценщику, это не подразумевает, что нужно иметь его у себя. Например, разработчик может потребовать от оценщика составить аннотацию на представление реализации на месте, указанном разработчиком.

Доступ ко всему представлению реализации предоставляется для того, чтобы обеспечить уверенность в том, что действия по анализу не будут сокращены вследствие недостаточности информации. Однако это не подразумевает, что при проведении действий по анализу исследуется все представление. Такой подход в большинстве случаев нецелесообразен; кроме того, он не предоставляет более высокого уровня доверия для ОО по сравнению с целенаправленной выборкой представления реализации. Представление реализации позволяет провести анализ других элементов декомпозиции проекта ОО (например, функциональной спецификации, проекта 00) и получить уверенность в том, что функциональные возможности безопасности, описанные на более высоком уровне проекта, фактически реализованы в ОО. Некоторые условности в представлении реализации могут значительно усложнить или сделать невозможным определение по одному только представлению реализации того, каким будет фактический результат компиляции или процесса реализации. Например, согласно указателям для компиляторов на языке программирования Си, компиляторы включают в код или исключают из него целые участки. Поэтому для точного определения представления реализации важно, чтобы была предоставлена эта «дополнительная» информация или описание связанных с нею средств (скриптов, компиляторов и т.д.).

Прослеживание между представлением реализации и описанием проекта ОО служит для того, чтобы помочь оценщику провести анализ. В случае, если проект ОО подвергается анализу вместе с соответствующими частями представления реализации, может быть достигнуто лучшее понимание внутреннего содержания ОО. Отображение представления реализации в описании проекта ОО служит в качестве указателя на представление реализации. Для компонентов низкого уровня в описании проекта ОО отображается только некое подмножество представления реализации. Из-за того, что точно неизвестно, какие части представления реализации необходимо будет отобразить в проекте ОО, разработчик может либо принять решение об отображении всего представления реализации заранее, либо подождать, пока оценщик определит, какие части представления реализации требуется отобразить.

Представление реализации выполняется разработчиком таким образом, чтобы была возможность преобразовать это представление в фактическую реализацию. Например, разработчик может работать с файлами, содержащими исходный текст программ, который потом будет скомпилирован и станет частью ФБО. Разработчик делает доступным представление реализации в том виде, в котором он его использует, благодаря чему оценщик может применять автоматизированные методы анализа.

Это также повышает уверенность в том, что оцениваемое представление реализации является именно тем, которое используется при производстве ФБО (в отличие оттого случая, когда оно сопровождается альтернативным форматом представления, например документом текстового процессора). Следует отметить, что разработчик может использовать различные другие формы представления реализации; они также должны прилагаться. Основная цель состоит в том, чтобы снабдить оценщика такой информацией, которая позволила бы максимизировать эффективность его усилий по анализу.

Для некоторых форм представления реализации требуется дополнительная информация, поскольку их довольно сложно понять и проанализировать. В качестве примера можно привести «скрытый» или каким-либо образом запутанный фрагмент исходного кода программы, который сложно понять и/или проанализировать. Подобные формы представления реализации чаще всего возникают, когда разработчик ОО применяет к некоторой версии представления реализации некие программы по сокрытию или запутыванию кода. В то время как представление со скрытыми участками кода является именно тем, которое будет в дальнейшем подвергнуто компиляции, а потому может быть даже ближе к реализации (по структуре), чем оригинальная версия, предоставление оценщику запутанного программного кода может привести к тому, что анализ рисков, связанных с данным представлением реализации, потребует значительно больше времени. При создании подобных форм представления в компонентах данного семейства должны быть детализированы примененные средства/алгоритмы сокрытия, что позволит снабдить оценщика представлением до применения сокрытия участков кода, а дополнительная информация может быть использована для получения уверенности в том, что процесс сокрытия участков кода не нарушил выполнения каких-либо функциональных возможностей безопасности.

**10.4.4 ADV\_IMP 1 Представление реализации ФБО**

Зависимости: ADV\_TDS.3 Базовый модульный проект

А1\_С\_ТАТ.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ADV\_IMP 1.1D

Разработчик должен обеспечить представление реализации для всех ФБО.

ADV\_IMP.1.2D

Разработчик должен обеспечить прослеживание выборки представления реализации к описанию проекта ОО.

Элементы содержания и представления свидетельств

ADV\_IMP.1.1C

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

ADV\_IMP.1.2C

Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.

ADV\_IMP.1.3C

В прослеживании между выборкой представления реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.

Элементы действий оценщика

ADV\_IMP.1.1E

Оценщик должен подтвердить, что для выборки представления реализации представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

**10.4.5 ADV\_IMP.2 Полное отображение представления реализации ФБО**

Зависимости: ADV\_TDS.3 Базовый модульный проект

А1\_С\_ТАТ.1 Полностью определенные инструментальные средства разработки

ALC\_CMC.5 Расширенная поддержка

Элементы действий разработчика

ADV\_IMP.2.1D

Разработчик должен обеспечить оценщику доступ к представлению реализации для всех ФБО.

ADV\_IMP.2.2D

Разработчик должен обеспечить прослеживание всего представления реализации к описанию проекта ОО.

Элементы содержания и представления свидетельств

ADV\_IMP.2.1C

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

ADV\_IMP.2.2C

Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.

ADV\_IMP.2.3C

В прослеживании между всем представлением реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.

Элементы действий оценщика

ADV\_IMP.2.1E

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

**10.5 Внутренняя структура ФБО (ADV\_INT)**

**10.5.1 Цели**

Это семейство связано с оценкой внутренней структуры ФБО. ФБО с полностью определенной внутренней структурой легче реализовать, при этом меньше вероятность того, что они будут содержать недостатки, которые в дальнейшем могут привести к уязвимостям. Кроме того, их легче сопровождать без внедрения при этом недостатков.

**10.5.2 Ранжирование компонентов**

Компоненты этого семейства ранжированы на основе требуемой степени структурированности и минимизации сложности. Компонент ADV\_INT. 1 «Подмножество ФБО с полностью определенной внутренней структурой» предъявляет требования полностью определенной внутренней структуры только для некоторой выборки ФБО. Данный компонент не включается в ОУД потому, что предназначен для использования в определенных обстоятельствах (например, если заявитель особо заинтересован в реализации криптографического модуля, который изолирован от остальной части ФБО), а следовательно, невозможно его широкое применение.

На следующем уровне требования полностью определенной внутренней структуры предъявляются ко всем ФБО. И наконец, требование по минимизации сложности вводится в компонент высшего уровня.

**10.5.3 Замечания по применению**

Приведенные требования при применении к внутренней структуре ФБО обычно приводят к улучшениям, которые помогают и разработчику, и оценщику в понимании ФБО, а также предоставляют основу для проектирования и проведения оценки подмножества тестов. Кроме того, следует, чтобы улучшение понимания ФБО помогло разработчику упростить их сопровождение.

Требования данного семейства представляются в довольно абстрактном виде. Из-за большого разнообразия различных ОО не представляется возможным определить более точные термины, чем выражения «с полностью определенной структурой» или «минимизация сложности». Заключения о структуре и сложности выносятся на основании особых технологий, используемых в ОО. Например, программное обеспечение скорее всего будет характеризовано как имеющее полностью определенную структуру в случае, если в нем будут представлены качества и характеристики, установленные для программного обеспечения техническими дисциплинами и их стандартами. Компоненты данного семейства требуют идентификации стандартов, согласно которым будут оцениваться качества, характеризующие полноту определения и отсутствие избыточной сложности.

**10.5.4 ADV\_INT.1 Подмножество ФБО с полностью определенной внутренней структурой**

Зависимости: ADV\_IMP.1 Представление реализации ФБО

ADV\_TDS.3 Базовый модульный проект

А1\_С\_ТАТ1 Полностью определенные инструментальные средства разработки

Цели

Цель данного компонента состоит в предоставлении возможности предъявления требований к тому, чтобы некоторые части ФБО имели полностью определенную внутреннюю структуру. Компонент предназначен для того, чтобы все ФБО были спроектированы и реализованы с использованием правильных технических принципов, а анализ выполнялся только в отношении некоторого конкретного подмножества ФБО.

Замечания по применению

В данном компоненте предъявляются требования к разработчику ПЗ или ЗБ по предоставлению информации о назначении подмножества ФБО. Это подмножество может быть определено на любом уровне представления:

a) на уровне структурных элементов ФБО, как определено в проекте ОО (например: «Разработчик должен спроектировать и реализовать подсистему аудита с полностью определенной внутренней структурой»);

b) на уровне реализации (например: «Разработчик должен спроектировать и реализовать файлы encrypt.c и decrypt.с таким образом, чтобы они имели полностью определенную внутреннюю структуру» или «Разработчик должен спроектировать и реализовать интегральную микросхему 6227 так, чтобы у нее имелась полностью определенная внутренняя структура»).

Выполнить это путем ссылки на заявленные ФТБ не представляется возможным (например, в виде: «Разработчик должен спроектировать и реализовать ту часть ФБО, которая обеспечивает выполнение требования к анонимности согласно компоненту FPR\_AN0.2 таким образом, чтобы эта часть обладала полностью определенной внутренней структурой»), поскольку такое представление не отражает, на что именно должен быть направлен анализ.

Ценность данного компонента ограничена, компонент применим в тех случаях, когда потенциально опасные пользователи/субъекты имеют ограниченный или строго контролируемый доступ к ИФБО или тогда, когда есть другие средства защиты (например, разделение доменов), которые обеспечивают, что на выбранное подмножество ФБО не могут неблагоприятно повлиять остальные ФБО (например, когда криптографические функции, которые изолированы от остальных ФБО, имеют полностью определенную внутреннюю структуру).

Элементы действий разработчика

ADV\_INT.1.1D

Разработчик должен выполнить проектирование и реализацию [назначение: подмножество ФБО] таким образом, чтобы внутренняя структура была полностью определенной.

ADV\_INT.1.2D

Разработчик должен представить описание и логическое обоснование внутренней структуры.

Элементы содержания и представления свидетельств

ADV\_INT.1.1C

В логическом обосновании должно приводиться объяснение того, на основании каких характеристик оценивается «полнота определения» внутренней структуры.

ADV\_INT.1.2C

В описании внутренней структуры ФБО должно быть продемонстрировано, что внутренняя структура заданного подмножества ФБО является полностью определенной.

Элементы действий оценщика

ADV\_INT.1.1E

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

ADV\_INT.1.2E

Оценщик должен выполнить внутренний анализ назначенного подмножества ФБО.

**10.5.5 ADV\_INT.2 Полностью определенная внутренняя структура**

Зависимости: ADV\_IMP.1 Представление реализации ФБО

ADV\_TDS.3 Базовый модульный проект

А1\_С\_ТАТ.1 Полностью определенные инструментальные средства разработки

Цели

Цель данного компонента состоит в предоставлении возможности предъявления к ФБО требований по полностью определенной внутренней структуре. Компонент предназначен для того, чтобы ФБО были спроектированы и реализованы с использованием правильных технических принципов.

Замечания по применению

Заключение о соответствии структуры требованиям принимается на основании изучения конкретных технологий, используемых в ОО. Этот компонент требует идентификации стандартов, согласно которым будут оцениваться качества, характеризующие полноту определения структуры.

Элементы действий разработчика

ADV\_INT.2.1D

Разработчик должен выполнить проектирование и реализацию всех ФБО таким образом, чтобы их внутренняя структура была полностью определена.

ADV\_INT.2.2D

Разработчик должен представить описание и логическое обоснование внутренней структуры.

Элементы содержания и представления свидетельств

ADV\_INT.2.1C

В логическом обосновании должно приводиться описание характеристик, на основании которых оценивается «полнота определения» внутренней структуры.

ADV\_INT.2.2C

В описании внутренней структуры ФБО должно быть продемонстрировано, что внутренняя структура всех ФБО является полностью определенной.

Элементы действий оценщика

ADV\_INT.2.1E

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

ADV\_INT.2.2E

Оценщик должен провести анализ внутренней структуры ФБО.

**10.5.6 ADV\_INT.3 Минимальная сложность внутренней структуры системы**

Зависимости: ADV\_IMP.1 Представление реализации ФБО

ADV\_TDS.3 Базовый модульный проект

А1\_С\_ТАТ.1 Полностью определенные инструментальные средства разработки

Цели

Цель данного компонента состоит в предоставлении возможности предъявления к ФБО требований по полностью определенной внутренней структуре и минимальной сложности. Компонент предназначен для того, чтобы все ФБО были спроектированы и реализованы с использованием правильных технических принципов.

Замечания по применению

Заключение о соответствии структуры требованиям и об отсутствии избыточной сложности принимается на основании изучения конкретных технологий, используемых в ОО. Этот компонент требует идентификации стандартов, согласно которым будут оцениваться качества, характеризующие полноту определения структуры и ее сложность.

Элементы действий разработчика

ADV\_INT.3.1D

Разработчик должен выполнить проектирование и реализацию всех ФБО таким образом, чтобы их внутренняя структура была полностью определена.

ADV\_INT.3.2D

Разработчик должен представить описание и логическое обоснование внутренней структуры.

Элементы содержания и представления свидетельств

ADV\_INT.3.1C

В логическом обосновании должно приводиться описание характеристик, на основании которых оценивается «полнота определения» и «сложность» внутренней структуры.

ADV\_INT.3.2C

В описании внутренней структуры ФБО должно быть продемонстрировано, что внутренняя структура всех ФБО полностью определена и не является избыточно сложной.

Элементы действий оценщика

ADV\_INT.3.1E

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

ADV\_INT.3.2E

Оценщик должен провести анализ внутренней структуры всех ФБО.

**10.6 Моделирование политики безопасности (ADV\_SPM)**

**10.6.1 Цели**

Целью этого семейства является обеспечение дополнительных гарантий посредством разработки формального представления ФБО и их свойств, определенных ФТБ и целями безопасности ЗБ, далее называемых формальной моделью и формальными свойствами, соответственно. Ожидается, что посредством формального доказательства будет установлено, что эти формальные свойства сохраняются в формальной модели, а также будет установлено посредством обоснования соответствия, что функциональная спецификация ОО сохраняет формальные свойства, доказанные для формальной модели. Ожидается формальное доказательство или полуформальная демонстрация сохранения формальных свойств в формальной или полуформальной спецификации, если последняя существует (ADV\_FSP.5 или ADV\_FSP.6 соответственно).

**10.6.2 Ранжирование компонентов**

Семейство содержит только один компонент.

**10.6.3 Замечания по применению**

Несоответствия ОО могут быть результатом либо непонимания требований безопасности, либо неправильной реализации этих требований безопасности. Адекватное определение требований безопасности для обеспечения их понимания может оказаться проблематичным, поскольку определение должно быть достаточно точным, чтобы предотвратить нежелательные результаты или тонкие недостатки во время реализации ОО. На протяжении процессов проектирования, реализации и анализа формальное представление ФБО и их свойств может использоваться в качестве точного руководства по проектированию и реализации, тем самым обеспечивая повышенную уверенность в том, что ОО удовлетворяет ФТБ и целям безопасности ЗБ. Полученное в результате руководство и точность представления ФБО и их свойств, определенных ФТБ и целями безопасности ЗБ, значительно улучшаются за счет определения формальной модели и определения формальных свойств с использованием формального языка и предоставления формального доказательства того, что эти формальные свойства сохраняются в формальной модели.

Создание формальной модели политики безопасности (SPM) ФБО должно быть завершено в отношении ЗБ; Такая модель помогает выявлять и устранять двусмысленные, непоследовательные, противоречивые или неисполнимые элементы, а также избегать любых недоразумений в отношении объема. С этой целью оценка должна определить, полностью ли формальная модель и формальные свойства охватывают ЗБ и принимаются ли только ЗБ и УП, которые совпадают по объему. После построения ОО формальная модель служит для оценки, способствуя вынесению оценщиком заключения о том, насколько хорошо разработчик понял реализуемые ФБО и существуют ли несоответствия между формальными свойствами, определенными целями безопасности ЗБ, и конструкция ОО. Доверие, полученное путем формального доказательства свойств модели, сопровождается доверием, полученным путем определения обоснования соответствия между формальной моделью и функциональной спецификацией ОО (как определено для ADV\_FSP). Обоснование соответствия состоит из формального доказательства при отображении на формальные аспекты функциональной спецификации ОО и полуформальной демонстрации в противном случае. Комбинация различных формальных систем (языков моделирования, инструментов, систем доказательства) может использоваться для различных частей ЗБ (ФТБ и целей безопасности) и обоснований соответствия.

**10.6.4 ADV\_SPM.1 Формальная модель политики безопасности ОО**

Зависимости: ADV\_FSP.4 Полная функциональная спецификация

Элементы действий разработчика

ADV\_SPM.1.1D

Разработчик должен представить формальную модель ПБО для [назначение: список формально моделируемых политик].

ADV\_SPM.1.2D

Для каждой политики, охваченной формальной моделью ПБО, в модели должны быть отражены значимые фрагменты изложения ФТБ, которые составляют данную политику.

ADV\_SPM.1.3D

Разработчик должен представить формальное доказательство соответствия между какой-либо формальной функциональной спецификацией и моделью ПБО.

ADV\_SPM.1.4D

Разработчик должен продемонстрировать соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV\_SPM.1.1C

Модель ПБО должна быть изложена в формальном стиле с предоставлением вспомогательного пояснительного текста согласно требованиям и в ней должны быть идентифицированы моделируемые политики ФБО.

ADV\_SPM.1.2C

Для всех моделируемых политик в модели ПБО должно быть определено понятие «безопасность» для данного ОО и должно быть представлено формальное доказательство того, что ОО не может перейти в небезопасное состояние.

ADV\_SPM.1.3C

Соответствие между моделью и функциональной спецификацией должно быть представлено на соответствующем уровне формализации.

ADV\_SPM.1.4C

В соответствии между моделью ПБО и функциональной спецификацией должно быть продемонстрировано, что функциональная спецификация является непротиворечивой и полной относительно модели ПБО.

ADV\_SPM.1.5C

Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показывать, что интерфейсы в функциональной спецификации являются непротиворечивыми и полными относительно политик, указанных в назначении компонента ADV\_SMP.1.1D.

Элементы действий оценщика

ADV\_SPM.1.1E

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

**10.7 Проект ОО (ADV\_TDS)**

**10.7.1 Цели**

В описании проекта ОО предоставляется краткое содержание описания ФБО, а также полное описание ФБО. С увеличением требуемого уровня доверия увеличивается и требуемый уровень детализации описания. При увеличении размера и сложности системы ФБО целесообразно применение различных уровней декомпозиции. Требования к проекту предназначены для предоставления такой информации (соответствующей заданному уровню доверия), чтобы можно было сделать заключение, что ФТБ реализованы.

**10.7.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы в зависимости от объема информации, которую требуется предоставить в отношении ФБО, и в зависимости от степени формализации, которая требуется для описания проекта.

**10.7.3 Замечания по применению**

10.7.3.1 Общие положения

Цель проектной документации состоит в предоставлении информации, достаточной для определения границ ОО и для описания того, каким образом ФБО реализуют ФТБ. Количество и структура документов по проекту будет зависеть от сложности ОО и от количества ФТБ; в общем случае для очень сложного ОО с большим числом ФТБ потребуется разработать больше проектной документации, чем для очень простого ОО, реализующего только несколько ФТБ. Для сложных ОО в плане обеспечения доверия весьма полезно применять различные уровни декомпозиции при описании проекта, тогда как для простых ОО не требуется представлять описания их реализации и на верхнем, и на нижнем уровне.

В данном семействе используются два уровня декомпозиции: на уровне подсистем и на уровне модулей. Модуль — это наиболее конкретное описание функциональных возможностей; он представляет собой описание реализации. Разработчику следует иметь возможность реализовать описанную на уровне модулей часть ОО без дополнительных проектных решений. Подсистема — это описание проекта ОО; описание на уровне подсистем помогает предоставить описание верхнего уровня того, что и каким образом выполняет данная часть ОО. Подсистема может подразделяться на подсистемы более низкого уровня или на модули. Для адекватного описания функционирования очень сложных объектов может потребоваться несколько уровней подсистем. Напротив, для описания простых ОО может не требоваться уровень подсистем; предоставить четкое описание функционирования таких ОО можно с применением модульного описания.

Применяемый в общем случае подход к разработке проектной документации заключается в том, что при увеличении уровня доверия акцент при предоставлении описания смещается от обобщенного, менее детализированного уровня описания (уровень подсистем) к более детализированному (уровень модулей). В случае, когда приемлем модульный уровень описания, поскольку ОО достаточно прост, чтобы описать его на этом уровне, но при этом для этого уровня доверия требуется описание на уровне подсистем, будет достаточно предоставить описание на уровне модуля. Однако для сложных ОО данный принцип неприменим: излишняя детализация описания на модульном уровне будет совершенно недоступной для понимания без сопроводительного описания на уровне подсистем.

Данный подход следует основной парадигме, гласящей, что предоставление дополнительной детальной информации по реализации ФБО позволит обеспечить большее доверие тому, что ФТБ верно реализованы. Кроме того, такая информация может быть использована для подтверждения этого при проведении тестирования (АТЕ «Тестирования»).

В требованиях данного семейства термин «интерфейс» употребляется как средство взаимодействия (между двумя подсистемами или модулями) и описывает, каким образом осуществляются такие взаимодействия, аналогично детализации ИФБО в функциональной спецификации (см. ADV\_FSP «Функциональная спецификация»). Термин «взаимодействие» используется для идентификации цели взаимодействия; он определяет причину взаимодействия двух подсистем или двух модулей друг с другом.

10.7.3.2 Детализация модулей и подсистем

Согласно требованиям, для подсистем и модулей должна быть предоставлена следующая подробная информация:

а) подсистемы и модули идентифицируются путем предоставления простого списка с обозначением того, чем они являются;

b) подсистемы и модули могут быть категорированы (как явным, так и неявным образом) как «осуществляющие выполнение ФТБ», «поддерживающие выполнение ФТБ», «не влияющие на выполнение ФТБ»; данные термины употребляются в том же значении, что и в семействе «Функциональная спецификация» (ADV\_FSP);

c) режим функционирования подсистемы — это описание того, что именно выполняет подсистема. Режимы функционирования тоже могут подразделяться на категории: «осуществляющие выполнение ФТБ», «поддерживающие выполнение ФТБ», «не влияющие на выполнение ФТБ». При этом режим функционирования подсистемы не может быть отнесен к категории большей значимости, чем сама подсистема. Например, осуществляющая выполнение ФТБ подсистема может функционировать в режиме, осуществляющем выполнение ФТБ, а также в поддерживающем или не влияющем на ФТБ;

d) краткая информация о режиме функционирования — это обзор всех выполняемых подсистемой действий (например: «Подсистема протокола TCP собирает пакеты данных IP и связанную с ними адресную информацию в надежные информационные потоки»);

e) описание режима функционирования подсистемы является объяснением всего, что выполняет данная система. Это описание следует составлять на таком уровне детализации, чтобы было легко определить, влияет ли данный режим функционирования каким-либо образом на обеспечение выполнения ФТБ;

f) в описании взаимодействий подсистем или модулей идентифицируется причина взаимодействия модулей и подсистем, а также характеризуется информация, которой они обмениваются. Не требуется представлять информацию в данном описании на таком же уровне детализации, как в спецификации интерфейсов. Например, будет достаточно указать, что: «подсистема X запрашивает блок памяти из модуля управления памятью, который отвечает на запрос путем предоставления участка распределенной памяти»;

g) в описании интерфейсов предоставляется детализация того, каким образом осуществляются процессы взаимодействия между модулями. В описании интерфейсов не приводится описание причин и целей взаимодействия модулей (это описание относится к описанию взаимодействий), но детально описываются методы осуществления данного взаимодействия в терминах структуры и содержания сообщений, сигналов, процессов внутренних взаимодействий и т.д.;

h) назначение описывает, каким образом модуль выполняет свои функциональные возможности. Причем представленной детальной информации должно быть достаточно, чтобы не потребовалось дополнительных проектных решений. Следует, чтобы назначение модуля явно соответствовало представлению реализации, которым данный модуль реализуется;

i) иначе модуль описывается в терминах того, что определяется в элементе доверия.

Подсистемы и модули, как осуществляющие выполнение ФТБ, так и все остальные, более подробно объясняются в приложении А.4, «ADV\_TDS: Подсистемы и модули».

**10.7.4 ADV\_TDS.1 Базовый проект**

Зависимости: ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации

Элементы действий разработчика

ADV\_TDS.1.1D

Разработчик должен представить проект ОО.

ADV\_TDS.1.2D

Разработчик должен обеспечить прослеживание от ИФБО в функциональной спецификации к самому низкому уровню декомпозиции, имеющемуся в проекте ОО.

Элементы содержания и представления свидетельств

ADV\_TDS.1.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.1.2C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.1.3C

В проекте должно приводиться описание режима функционирования для каждой подсистемы, поддерживающей выполнение ФТБ или не влияющей на их выполнение, с предоставлением детальной информации, достаточной для того, чтобы установить, что подсистема не является осуществляющей выполнение ФТБ.

ADV\_TDS.1.4C

В проекте должна приводиться аннотация осуществляющих выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.

ADV\_TDS.1.5C

В проекте должно приводиться описание взаимодействий между осуществляющими выполнение ФТБ подсистемами ФБО, а также между ними и другими подсистемами ФБО.

ADV\_TDS.1.6C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.1.1E

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

ADV\_TDS.1.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

**10.7.5 ADV\_TDS.2 Архитектурный проект**

Зависимости: ADV\_FSP.3 Функциональная спецификация с полной аннотацией

Элементы действий разработчика

ADV\_TDS.2.1D

Разработчик должен представить проект ОО.

ADV\_TDS.2.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления свидетельств

ADV\_TDS.2.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.2.2C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.2.3C

В проекте должно приводиться описание режима функционирования для каждой подсистемы ФБО, не влияющей на выполнение ФТБ, с предоставлением детальной информации, достаточной для того, чтобы установить, что подсистема является не влияющей на выполнение ФТБ.

ADV\_TDS.2.4C

В проекте должно приводиться описание осуществляющих выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.

ADV\_TDS.2.5C

В проекте должна приводиться аннотация поддерживающих и не влияющих на выполнение ФТБ режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.

ADV\_TDS.2.6C

В проекте должна приводиться аннотация режимов безопасности тех подсистем, которые являются осуществляющими выполнение ФТБ.

ADV\_TDS.2.7C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.2.8C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.2.1E

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

ADV\_TDS.2.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

Элементы содержания и представления свидетельств

ADV\_TDS.3.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.3.2C

В проекте должно приводиться описание структуры ОО на уровне модулей.

ADV\_TDS.3.3C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.3.4C

В проекте должно приводиться описание каждой из подсистем ФБО.

ADV\_TDS.3.5C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.3.6C

В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.

ADV\_TDS.3.7C

В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV\_TDS.3.8C

В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

ADV\_TDS.3.9C

В проекте должен быть описан каждый поддерживающий и не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV\_TDS.3.10C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.3.1E

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

ADV\_TDS.3.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

**10.7.6 ADV\_TDS.3 Базовый модульный проект**

Зависимости: ADV\_FSP.4 Полная функциональная спецификация

Элементы действий разработчика

ADV\_TDS.3.1D

Разработчик должен представить проект ОО.

ADV\_TDS.3.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

**10.7.7 ADV\_TDS.4 Полуформальный модульный проект**

Зависимости: ADV\_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках

Элементы действий разработчика

ADV\_TDS.4.1D

Разработчик должен представить проект ОО.

ADV\_TDS.4.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления свидетельств

ADV\_TDS.4.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.4.2C

В проекте должно приводиться описание структуры ОО на уровне модулей с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.

ADV\_TDS.4.3C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.4.4C

В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется целесообразным.

ADV\_TDS.4.5C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.4.6C

В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.

ADV\_TDS.4.7C

В проекте должен быть описан каждый осуществляющий и поддерживающий выполнение ФТБ модуль сточки зрения его назначения и взаимодействия с другими модулями.

ADV\_TDS.4.8C

В проекте должен быть описан каждый осуществляющий и поддерживающий выполнение ФТБ модуль с точки зрения относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

ADV\_TDS.4.9C

В проекте должен быть описан каждый не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV\_TDS.4.10C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.4.1E

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

ADV\_TDS.3.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

10.7.8 ADV\_TDS.5 Полный полуформальный модульный проект

Зависимости: ADV\_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках

Элементы действий разработчика

ADV\_TDS.5.1D

Разработчик должен представить проект ОО.

ADV\_TDS.5.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления свидетельств

ADV\_TDS.5.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.5.2C

В проекте должно приводиться описание структуры ОО на уровне модулей с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.

ADV\_TDS.5.3C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.5.4C

В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV\_TDS.5.5C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.5.6C

В проекте должно быть осуществлено прослеживание подсистем ФБО к модулям ФБО.

ADV\_TDS.5.7C

В проекте должно приводиться полуформальное описание каждого модуля с точки зрения его назначения, взаимодействия с другими модулями, интерфейсов и значений, предоставляемых этими интерфейсами в ответ на запросы, а также вызываемых интерфейсов других модулей.

Полуформальное описание сопровождается вспомогательным пояснительным неформальным текстом, если это представляется целесообразным.

ADV\_TDS.5.8C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.5.1E

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

ADV\_TDS.5.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

**10.7.8 ADV\_TDS.5 Полный полуформальный модульный проект**

Зависимости: ADV\_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибках

Элементы действий разработчика

ADV\_TDS.5.1D

Разработчик должен представить проект ОО.

ADV\_TDS.5.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Элементы содержания и представления свидетельств

ADV\_TDS.5.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.5.2C

В проекте должно приводиться описание структуры ОО на уровне модулей с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.

ADV\_TDS.5.3C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.5.4C

В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV\_TDS.5.5C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.5.6C

В проекте должно быть осуществлено прослеживание подсистем ФБО к модулям ФБО.

ADV\_TDS.5.7C

В проекте должно приводиться полуформальное описание каждого модуля с точки зрения его назначения, взаимодействия с другими модулями, интерфейсов и значений, предоставляемых этими интерфейсами в ответ на запросы, а также вызываемых интерфейсов других модулей.

Полуформальное описание сопровождается вспомогательным пояснительным неформальным текстом, если это представляется целесообразным.

ADV\_TDS.5.8C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV\_TDS.5.1E

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

ADV\_TDS.5.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

**10.7.9 ADV\_TDS.6 Полный полуформальный модульный проект с формальным представлением проекта на верхнем уровне**

Зависимости: ADV\_FSP.6 Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией

Элементы действий разработчика

ADV\_TDS.6.1D

Разработчик должен представить проект ОО.

ADV\_TDS.6.2D

Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

ADV\_TDS.6.3D

Разработчик должен представить формальную спецификацию подсистем ФБО.

ADV\_TDS.6.4D

Разработчик должен представить доказательство соответствия формальных спецификаций подсистем ФБО функциональной спецификации.

Элементы содержания и представления свидетельств

ADV\_TDS.6.1C

В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV\_TDS.6.2C

В проекте должно приводиться описание структуры ОО на уровне модулей с присвоением каждому модулю категории либо осуществляющего выполнение ФТБ, либо поддерживающего, либо не влияющего на выполнение ФТБ.

ADV\_TDS.6.3C

В проекте должны быть идентифицированы все подсистемы ФБО.

ADV\_TDS.6.4C

В проекте должно приводиться полуформальное описание каждой из подсистем ФБО, сопровождающееся вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV\_TDS.6.5C

В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV\_TDS.6.6C

В проекте должно быть осуществлено прослеживание подсистем ФБО к модулям ФБО.

ADV\_TDS.6.7C

В проекте должно приводиться описание в полуформальном стиле каждого модуля сточки зрения его назначения, взаимодействия с другими модулями, интерфейсов и значений, предоставляемых этими интерфейсами в ответ на запросы, а также вызываемых интерфейсов других модулей. Полуформальное описание сопровождается вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV\_TDS.6.8C

Формальная спецификация подсистем ФБО должна содержать формальное описание ФБО и сопровождаться вспомогательным пояснительным неформальным текстом, если это представляется уместным.

ADV\_TDS.6.9C

В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

ADV TDS.6.10C

В свидетельстве о соответствии формальных спецификаций подсистем ФБО функциональной спецификации должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования являются правильным и полным отображением вызывающих их ИФБО.

Элементы действий оценщика

ADV\_TDS.6.1E

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

ADV\_TDS.6.2E

Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

10.8 Соответствие составной конструкции (ADV\_COMP)

10.8.1 Цели

Целью этого семейства является определение того, выполняются ли в составном изделии требования к зависимому компоненту, предъявляемые соответствующим базовым компонентом.

**10.8.2 Ранжирование компонентов**

Это семейство содержит только один компонент.

**10.8.3 Замечания по применению**

Требования к зависимому компоненту, предъявляемые соответствующим базовым компонентом, могут быть сформулированы в соответствующем руководстве пользователя, связанном с базовым компонентом, ETR для комплексной оценки (в форме наблюдений и рекомендаций) и отчете органа по оценке базового компонента (например, в форме ограничений и рекомендаций). Разработчик зависимого компонента должен учитывать каждый из этих источников, если таковой имеется, и реализовать зависимый компонент таким образом, чтобы были выполнены применимые требования. Оценщик составного продукта должен проверить, что все условия для зависимого компонента, налагаемые базовым компонентом и представленные в его документации, связанной с оценкой, выполняются составным продуктом, т.е. были учтены разработчиком зависимого компонента.

Спонсор оценки составного продукта должен обеспечить, чтобы оценщику составного продукта было предоставлено следующее:

- руководство пользователя, связанное с базовыми компонентами,

- ETR, связанный с базовым компонентом, для комплексной оценки, подготовленный оценщиком базового компонента,

- отчет органа по оценке базовых компонентов,

- обоснование безопасного внедрения составного продукта, включая доказательства, подготовленные разработчиком зависимого компонента.

ФБО составного продукта представлены на различных уровнях абстракции в семействах класса разработки ADV. Исходя из опыта, соответствующими уровнями представления проекта для проверки того, выполняются ли составным продуктом требования базового компонента, являются проект ОО (ADV\_TDS), архитектура безопасности (ADV\_ARC) и реализация (ADV\_IMP). В случае, если эти уровни представления проекта недоступны (например, из-за выбранного пакета обеспечения качества EAL1), текущее семейство неприменимо (причину см. в следующем параграфе).

Из-за определения составного продукта интерфейс между его базовым компонентом и зависимым компонентом является внутренним, следовательно, функциональная спецификация (ADV\_FSP) как уровень представления не подходит для анализа соответствия проекта.

Архитектура безопасности ADV\_ARC как семейство гарантий предназначена для обеспечения правильной работы интегративных служб безопасности, таких как разделение доменов, самозащита и невозможность обхода. Невозможно и не имеет смысла комплексная оценка иметь представление об архитектурных внутренностях соответствующего базового компонента (это вопрос оценки базового компонента). В контексте ADV\_ARC оценщик составной продукции должен:

i. определить, использует ли зависимый компонент услуги связанного базового документа в пределах своего собственного составного продукта ST для обеспечения разделения доменов, самозащиты, необходимости и защищенного запуска; если нет, то для ADV\_ARC дальнейших составных действий нет; если да, то

ii. оценщик должен определить, использует ли зависимый компонент эти услуги базового компонента соответствующим/безопасным способом (см. руководство пользователя базового компонента).

Поскольку согласованность политики безопасности составного продукта уже рассматривалась в контексте ЗБ в семействе гарантий ASE\_COMP, нет необходимости рассматривать непротиворечивость модели политики безопасности (ADV\_SPM) составного продукта и модели политики безопасности соответствующего базового компонента.

**10.8.4 ADV\_COMP.1 Соответствие проекта руководству пользователя, касающемуся базового компонента, ETR для комплексной оценки и отчету органа по оценке базового компонента**

Зависимости: Зависимости отсутствуют.

Элементы действий разработчика

ADV\_COMP.1.1D

Разработчик должен предоставить обоснование соответствия проекта.

Элементы контента и презентации

ADV\_COMP.1.1C

Обоснование соответствия проекта должно обеспечивать обоснование соответствия проекта – на соответствующем уровне представления – того, как требования к зависимому компоненту, предъявляемые соответствующим базовым компонентом, выполняются в составном изделии.

Элементы действий оценщика

ADV\_COMP.1.1E

Оценщик должен подтвердить, что обоснование соответствия проекта является полным, последовательным и внутренне непротиворечивым.

## **11 Класс AGD: Руководства**

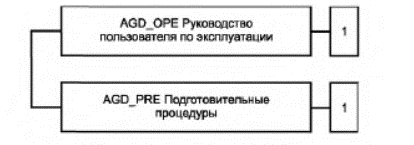
**11.1 Общие положения**

Класс «Руководства» предоставляет требования к документации руководств для всех пользовательских ролей. Для безопасной подготовки и безопасного функционирования ОО необходимо описать все существенные аспекты, относящиеся к безопасному применению ОО. В данном классе также рассматриваются случаи непреднамеренных неточностей конфигурации или ошибок эксплуатации ОО.

Во многих случаях уместно предоставление отдельных руководств по подготовительным процедурам и эксплуатации ОО или даже отдельных руководств для различных пользовательских ролей: конечных пользователей, администраторов, программистов-разработчиков приложений, использующих программные и аппаратные интерфейсы и т.д.

Класс «Руководства» подразделяется на два семейства: касающееся руководства пользователя по подготовительным процедурам (что должно делаться для перевода поставленного ОО в оцененную конфигурацию в среде его функционирования, как описано в ЗБ) и руководства пользователя по эксплуатации (что должно делаться в процессе функционирования ОО в его оцененной конфигурации).

На рисунке 9 показаны семейства этого класса и иерархия компонентов в семействах.



**Рисунок 9 – Декомпозиция класса AGD «Руководства»**

**11.2 Руководство пользователя по эксплуатации (AGD\_OPE)**

**11.2.1 Цели**

Руководство пользователя по эксплуатации относится к печатным документам, которые предназначены для использования всеми пользователями оцененной конфигурации ОО: конечными пользователями, лицами, ответственными за правильное обслуживание и администрирование ОО с целью максимизации безопасности, а также другими лицами (например, программистами), использующими внешние интерфейсы ОО. Руководство пользователя по эксплуатации описывает функции, предоставляемые ФБО, содержит инструкции и рекомендации по безопасности (включая предупреждения), способствующие пониманию ФБО и содержащие информацию, критически важную для безопасности, а также критически важные для обеспечения безопасного состояния действия. Не рекомендуется, чтобы в руководствах были неточные и необоснованные инструкции; для всех режимов функционирования следует назначить процедуры безопасности. Следует, чтобы небезопасные состояния выявлялись без затруднений.

Руководство пользователя по эксплуатации обеспечивает некоторую степень доверия к тому, что санкционированные пользователи (не являющиеся злоумышленниками), администраторы, поставщики приложений и другие лица, использующие внешние интерфейсы ОО, имеют представление о безопасном функционировании ОО и будут использовать ОО по назначению. Оценка руководства пользователя включает проверку того, может ли ОО функционировать в небезопасном режиме таким образом, что пользователь при этом будет обоснованно полагать, что функционирование происходит в безопасном режиме. Целью является минимизация рисков человеческого фактора или других ошибок при эксплуатации, которые могут повлечь деактивацию, недоступность или сбой активации функций безопасности, что, в свою очередь, приведет к невыявленному небезопасному состоянию.

**11.2.2 Ранжирование компонентов**

Это семейство содержит только один компонент.

**11.2.3 Замечания по применению**

В ОО могут быть различные роли или группы пользователей, которые могут взаимодействовать с ФБО. Эти роли или группы пользователей следует учитывать в руководстве пользователя по эксплуатации. Пользователи могут быть разделены на администраторов и лиц, не являющихся администраторами, а могут быть разделены и сточки зрения функциональных обязанностей на лиц, ответственных за получение, приемку, установку и обслуживание ОО, разработчиков приложений, проверяющих, аудиторов, администраторов, конечных пользователей. Каждая роль может объединять в себе обширный набор прав, а может включать одиночное право.

Требования элемента AGD\_OPE.1.1C охватывают тот аспект, что в руководстве пользователя должны быть отражены соответствующим образом все описанные в ПЗ/ЗБ предупреждения пользователям ОО, относящиеся к определению проблемы безопасности и к целям безопасности для среды функционирования.

Концепция безопасных значений, используемая в элементе AGD\_OPE.1.3C, значима, если пользователь управляет параметрами безопасности. В руководстве необходимо представить безопасные и потенциально опасные значения для таких параметров.

В элементе AGD\_OPE.1.40 содержится требование, чтобы в руководстве пользователя было описание соответствующей реакции на все события, имеющие значение для безопасности. Хотя многие имеющие значение для безопасности события являются результатом выполнения функций, это не всегда так (например, переполнение журнала аудита, обнаружение вторжения). Кроме того, событие, имеющее значение для безопасности, может происходить в результате выполнения определенной последовательности функций или наоборот: несколько имеющих значение для безопасности событий могут быть вызваны выполнением одной функции.

В элементе AGD\_OPE.1.7C содержится требование, чтобы руководство пользователя было четким и обоснованным. Нечеткие и необоснованные инструкции могут ввести пользователя ОО в заблуждение в отношении состояния безопасности ОО: пользователь будет считать, что ОО находится в безопасном состоянии, тогда как это не так.

Примером нечеткой инструкции может служить описание отдельной инструкции руководства, которая может быть двояко истолкована, что может привести к небезопасному состоянию.

Примером необоснованной инструкции может служить рекомендация следовать настолько усложненной процедуре, что нецелесообразно ожидать от пользователей выполнения данной рекомендации.

**11.2.4 AGD\_OPE.1 Руководство пользователя по эксплуатации**

Зависимости: ADV\_FSP.1 Базовая функциональная спецификация

Элементы действий разработчика

AGD\_OPE.1.1D

Разработчик должен представить руководство пользователя по эксплуатации.

Элементы содержания и представления свидетельств

AGD\_OPE.1.1C

В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.

AGD\_OPE.1.2C

В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в ОО интерфейсами.

AGD\_OPE.1.3C

В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.

AGD\_OPE.1.4C

В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.

AGD\_OPE.1.5C

В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы 00 (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.

AGD\_OPE.1.6C

В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ.

AGD\_OPE.1.7C

Руководство пользователя по эксплуатации должно быть четким и обоснованным.

Элементы действий оценщика

AGD\_OPE1.1E

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

**11.3 Подготовительные процедуры (AGD\_PRE)**

**11.3.1 Цели**

Подготовительные процедуры необходимы для обеспечения того, что 00 был получен и установлен безопасным образом, в соответствии с намерениями разработчика. Требования к подготовительным процедурам направлены на безопасный переход от поставленного ОО к его первоначальной среде функционирования. Это включает также и исследование на предмет возможности конфигурации или установки ОО небезопасным образом, при котором пользователь будет обоснованно считать, что ОО находится в безопасном состоянии.

**11.3.2 Ранжирование компонентов**

Это семейство содержит только один компонент.

**11.3.3 Замечания по применению**

Необходимо учитывать, что применение данных требований будет варьироваться в зависимости от таких аспектов, как предоставлен ли 00 в рабочем состоянии или он установлен в месте размещения владельца ОО на месте владельца и т. п.

Первый процесс, который охватывают подготовительные процедуры, состоит в безопасной приемке потребителем полученного 00 в соответствии с процедурами поставки разработчика. Даже если разработчик не определил процедуры поставки, безопасность приемки все равно должна быть обеспечена.

Установка ОО включает преобразование среды его функционирования в состояние, удовлетворяющее целям безопасности для среды функционирования, изложенным в ЗБ.

Возможна также ситуация, когда установка не требуется, например, для смарт-карт. В этом случае необязательно требовать и анализировать процедуры установки.

Требования этого семейства доверия представлены отдельно от требований семейства «Руководство пользователя по эксплуатации» (AGD\_OPE) в силу малой употребимости, а возможно, и вовсе однократного применения подготовительных процедур.

**11.3.4 AGD\_PRE.1 Подготовительные процедуры**

Зависимости: отсутствуют.

Элементы действий разработчика

AGD\_PRE.1.1D

Разработчик должен предоставить ОО вместе с подготовительными процедурами.

Элементы содержания и представления свидетельств

AGD\_PRE1.1C

В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного ОО в соответствии с процедурами поставки разработчика.

AGD\_PRE1.2C

В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

Элементы действий оценщика

AGD\_PRE.1.1E

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

AGD\_PRE.1.2E

Оценщик должен использовать подготовительные процедуры для подтверждения того, что ОО может быть безопасно подготовлен к работе.

## **12 Класс ALC: Поддержка жизненного цикла**

**12.1 Общие положения**

Поддержка жизненного цикла является аспектом установления организационного порядка и управления в процессе совершенствования ОО во время его разработки и сопровождения. Уверенность в соответствии ОО требованиям безопасности к ОО будет больше, если анализ безопасности и формирование свидетельств выполняются на регулярной основе как неотъемлемая часть деятельности по разработке и сопровождению.

В жизненном цикле продукта определяется, под чьей ответственностью находится ОО — разработчика или пользователя, а не то, расположен ли он в пользовательской среде или среде разработки. Переходным моментом является момент передачи ОО пользователю. Это также момент перехода от требований класса ALC «Поддержка жизненного цикла» к требованиям класса AGD «Руководства».

В состав класса ALC «Поддержка жизненного цикла» входят девять семейств:

- Семейство «Определение жизненного цикла» (ALC\_LCD) содержит требования к описанию верхнего уровня жизненного цикла ОО;

- Семейство «Возможности УК» (ALC\_CMC) содержит требования к более подробному описанию управления элементами конфигурации.

- В семействе «Область УК» (ALC\_CMS) представлены требования к минимальному набору средств конфигурации для должного управления элементами конфигурации.

- Семейство «Безопасность разработки» (ALC\_DVS) включает требования к физическим, процедурным, организационным мерам безопасности и другим критериям безопасности;

- Семейство «Инструментальные средства и методы» (ALC\_TAT) включает требования к инструментальным средствам разработки и выполнению стандартов реализации, используемых разработчиком;

- Семейство «Устранение недостатков» (ALC\_FLR) включает требования по обработке недостатков безопасности.

- Семейство «Поставка» (ALC\_DEL) определяет требования к процедурам, используемым при поставке ОО потребителю. Процессы поставки, происходящие во время разработки ОО, рассматриваются скорее как транспортировка, и обрабатываются в контексте процедур интеграции и приемки других семейств данного класса;

- ALC\_TDA касается создания определенных артефактов в процессе разработки;

- ALC\_COMP занимается интеграцией частей композиции и проверкой согласованности процедур доставки.

В данном классе термин «разработка» и родственные ему понятия («разработчик», «разрабатывать») используются в более общем смысле для определения разработки и производства, в то время как «производство» само по себе означает процесс превращения представления реализации в готовый ОО.

На рисунке 10 показаны семейства этого класса и иерархия компонентов в семействах.



**Рисунок 10 – Декомпозиция класса ALC «Поддержка жизненного цикла»**

**12.2 Возможности УК (ALC\_CMC)**

**12.2.1 Цели**

Управление конфигурацией (УК) — один из способов увеличения доверия к тому, что ОО соответствует ФТБ. УК устанавливает это посредством предъявления требований к организационному порядку и управлению процессами усовершенствования и модификации ОО и связанной с ним информации.

Системы УК реализуются для того, чтобы удостовериться в целостности частей ОО, подвергающихся контролю со стороны этих систем путем отслеживания любых изменений, а также обеспечения санкционированности всех изменений.

Цель данного семейства состоит в предъявлении требований к наличию определенных возможностей в системе УК разработчика. Эти требования предъявляются с целью снижения вероятности появления несанкционированных изменений элементов конфигурации. Системе УК следует обеспечить целостность ОО на ранних этапах проектирования и во время всех последующих операций по сопровождению.

Целью введения автоматизированных инструментальных средств УК является повышение эффективности системы УК. Хотя и автоматизированную, и ручную систему УК можно обойти, проигнорировать или доказать их недостаточность для предотвращения внесения несанкционированных изменений, автоматизированные системы менее подвержены человеческим ошибкам или халатности.

Цели данного семейства состоят в следующем:

a) в обеспечении корректности и полноты ОО перед отправкой его потребителю;

b) в обеспечении того, чтобы ни один элемент конфигурации не был упущен в процессе оценки;

c) в предотвращении несанкционированной модификации, добавлении или удалении элементов конфигурации ОО.

**12.2.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе возможностей системы УК, объема документации УК и свидетельств, предоставленных разработчиком.

**12.2.3 Замечания по применению**

Желательным считается применение УК уже на ранних этапах проектирования и впоследствии в будущем, тем не менее данное семейство содержит требование, чтобы УК были введены в эксплуатацию и использовались до окончания оценки.

В случае, когда ОО является подмножеством продукта, требования этого семейства применяются только к элементам конфигурации ОО, а не к продукту в целом.

От разработчиков, использующих отдельные системы УК для различных фаз жизненного цикла (например, при разработке, производстве и/или для готового продукта), требуется задокументировать все системы УК. С целью проведения оценки отдельные системы УК следует рассматривать как часть общей системы УК, которая является предметом рассмотрения в настоящих критериях.

Аналогично: если части ОО произведены разными разработчиками или в различных местах, системы УК, используемые в разных местах, следует рассматривать как часть общей системы УК, которая является предметом рассмотрения в настоящих критериях. В таком случае также следует принимать во внимание аспекты интеграции.

Некоторые элементы этого семейства относятся к элементам конфигурации. Эти элементы определяют требования УК, которые будут предъявляться ко всем элементам, указанным в списке конфигурации, при этом содержание самого списка остается на усмотрение разработчика. С целью ограничения этого списка могут быть использованы требования класса «Область УК» (ALC\_CMS), в котором определены конкретные элементы, которые должны быть включены в список конфигурации и, следовательно, должны быть охвачены УК.

Элемент ALC\_CMC.2.3C содержит требование, чтобы в системе УК были уникально идентифицированы все элементы конфигурации. Также требуется, чтобы модификация элемента конфигурации приводила к присвоению ему нового уникального идентификатора.

Элемент ALC\_CMC.3.8C содержит требование, что в свидетельстве должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК. Примерами такого свидетельства может быть такая документация, как снимок экрана или запись журнала аудита из системы УК, а также подробная демонстрация системы УК разработчиком. Оценщик является ответственным за вынесение заключения, что это свидетельство является достаточным для демонстрации того, что система УК функционирует в соответствии с планом УК.

Элемент ALC\_CMC.4.5C содержит требование, чтобы в системе УК поддерживались автоматизированные средства для поддержки производства ОО. Для этого требуется, чтобы в системе УК имелись автоматизированные средства, способствующие вынесению заключения, что при генерации ОО были использованы правильные элементы конфигурации.

Элемент ALC\_СМС.5.10С содержит требование, чтобы системой УК предоставлялись автоматизированные средства, позволяющие выявить изменения в данном ОО и его предыдущей версии. Даже если предыдущей версии ОО не существует, разработчику нужно предоставить автоматизированные средства для выявления изменений в данном ОО и его следующей версии.

**12.2.4 ALC\_СМС.1 Маркировка ОО**

Зависимости: ALC\_CMS.1 Охват УК ОО

Цели

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

Элементы действий разработчика

ALC\_CMC.1.1D

Разработчик должен предоставить ОО и маркировку для ОО.

Элементы содержания и представления свидетельств

ALC\_СМС.1.1С

ОО должен быть помечен уникальной маркировкой.

Элементы действий оценщика

ALC\_САР.1.1Е

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

**12.2.5 ALC\_CMC.2 Использование системы УК**

Зависимости: ALC\_CMS.1 Охват УК ОО

Цели

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

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

Использование системы УК увеличивает доверие к тому, что элементы конфигурации обслуживаются управляемым образом.

Элементы действий разработчика

ALC\_CMC.2.1D

Разработчик должен предоставить ОО и маркировку для ОО.

ALC\_CMC.2.2D

Разработчик должен предоставить документацию УК.

ALC\_CMC.2.3D

Разработчик должен использовать систему УК.

Элементы содержания и представления свидетельств

А1\_С\_СМС.2.1С

ОО должен быть помечен уникальной маркировкой.

ALC\_CMC.2.2C

В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC\_CMC.2.3C

В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

Элементы действий оценщика

ALC\_СМС.2.1Е

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

**12.2.6 ALC\_CMC.3 Средства контроля авторизации**

Зависимости: ALC\_CMS.1 Охват УК ОО

ALC\_DVS.1 Идентификация мер безопасности

ALC\_LCD.1 Определенная разработчиком модель жизненного цикла

Модель жизненного цикла включает процедуры, инструменты и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают методы проектирования, процедуры проверки, средства контроля управления проектом, процедуры контроля изменений, методы тестирования и процедуры приемки. Эффективная модель жизненного цикла будет учитывать эти аспекты процесса разработки и сопровождения в рамках общей структуры управления, которая распределяет обязанности и контролирует прогресс.

Существуют различные типы ситуаций приемки, которые рассматриваются в разных местах критериев:

— приемка деталей, поставленных субподрядчиками («интеграция»), должна рассматриваться в этом семействе,

— Определение жизненного цикла разработки (ALC\_LCD),

— приемка после внутренних перевозок в Безопасность среды разработки (ALC\_DVS),

— приемка деталей в систему CM в возможностях CM (ALC\_CMC), и

— принятие поставленного ОО потребителем в стадии поставки (ALC\_DEL).

Первые три типа могут пересекаться.

Хотя определение жизненного цикла связано с сопровождением ОО и, следовательно, с аспектами, которые становятся актуальными после завершения оценки, его оценка добавляет уверенности за счет анализа информации о жизненном цикле ОО, предоставленной во время оценки.

Модель жизненного цикла обеспечивает необходимый контроль над разработкой и сопровождением ОО, если модель позволяет в достаточной степени минимизировать опасность того, что ОО не будет соответствовать требованиям безопасности.

Измеримая модель жизненного цикла — это модель, использующая некоторую количественную оценку (арифметические параметры и/или метрики) управляемого продукта для измерения свойств продукта при разработке. Типичными показателями являются показатели сложности исходного кода, плотность дефектов (ошибок на размер кода) или среднее время до отказа. Для оценки безопасности имеют значение все эти метрики, которые используются для повышения качества за счет уменьшения вероятности ошибок и тем самым, в свою очередь, повышения уверенности в безопасности ОО.

Следует учитывать, что существуют стандартизированные модели жизненного цикла с одной стороны (например, водопадная модель) и стандартизированные метрики с другой стороны (например, плотность ошибок), которые можно комбинировать. Серия стандартов ISO/IEC 15408 не требует, чтобы жизненный цикл соответствовал одному стандарту, определяющему оба аспекта.

ALC\_LCD.1 Разработчик определяет процессы жизненного цикла

Цели

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

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

Использование системы УК увеличивает доверие к тому, что элементы конфигурации обслуживаются управляемым образом.

Поддержанию целостности ОО способствует применение средств контроля, исключающих выполнение несанкционированных модификаций ОО («Управление доступом к УК»), а также обеспечение надлежащих функциональных возможностей и использование системы УК.

Элементы действий разработчика

ALC\_CMC.3.1D

Разработчик должен предоставить ОО и маркировку для ОО.

ALC\_CMC.3.2D

Разработчик должен предоставить документацию УК.

ALC\_CMC.3.3D

Разработчик должен использовать систему УК.

Элементы содержания и представления свидетельств

ALC\_СМС.3.1С

ОО должен быть помечен уникальной маркировкой.

ALC\_CMC.3.2C

В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC\_CMC.3.3C

В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

ALC\_CMC.3.4C

В системе УК должны быть предусмотрены такие меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.

ALC\_CMC.3.5C

Документация УК должна включать в себя план УК.

ALC\_CMC.3.6C

В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.

ALC\_CMC.3.7C

В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC\_CMC.3.8C

В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий оценщика

ALC\_СМС.3.1Е

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

**12.2.7 ALC\_CMC.4 Поддержка генерации, процедуры приемки и автоматизация**

Зависимости: ALC\_CMS.1 Охват УК ОО

ALC\_DVS.1 Идентификация мер безопасности

ALC\_LCD.1 Определенная разработчиком модель жизненного цикла

Цели

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

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

Использование системы УК увеличивает доверие к тому, что элементы конфигурации обслуживаются управляемым образом.

Поддержанию целостности ОО способствует применение средств контроля, исключающих выполнение несанкционированных модификаций ОО («Управление доступом к УК»), а также обеспечение надлежащих функциональных возможностей и использование системы УК.

Процедуры приемки предназначены для того, чтобы подтвердить, что любое создание или модификация элементов конфигурации санкционировано. Процедуры приемки — исключительно важный элемент процессов интеграции и управления жизненным циклом ОО.

В средах разработки, где элементы конфигурации являются сложными, трудно контролировать изменения без поддержки автоматизированными средствами. В частности, эти автоматизированные инструменты должны быть в состоянии поддерживать многочисленные изменения, которые происходят во время разработки, и обеспечивать санкционированность этих изменений. Цель данного компонента состоит в том, чтобы обеспечить управление элементами конфигурации при помощи автоматизированных средств. Если ОО разрабатывается несколькими разработчиками, т.е. имеет место интеграция, то использование автоматизированных средств также целесообразно.

Процедуры поддержки производства позволяют удостовериться в том, что генерация ОО из поставленного набора элементов конфигурации выполнена должным образом, особенно в том случае, когда вовлечены разные разработчики и необходимо осуществить процессы интеграции.

Элементы действий разработчика

ALC\_CMC.4.1D

Разработчик должен предоставить ОО и маркировку для ОО.

ALC\_CMC.4.2D

Разработчик должен предоставить документацию УК.

ALC\_CMC.4.3D

Разработчик должен использовать систему УК.

Элементы содержания и представления свидетельств

ALC\_CMC.4.1C

ОО должен быть помечен уникальной маркировкой.

ALC\_CMC.4.2C

В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC\_CMC.4.3C

В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

ALC\_CMC.4.4C

В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.

ALC\_CMC.4.5C

Система УК должна поддерживать производство ОО автоматизированными средствами.

ALC\_CMC.4.6C

Документация УК должна включать в себя план УК.

ALC\_CMC.4.7C

В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.

ALC\_CMC.4.8C

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

ALC\_CMC.4.9C

В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC\_СМС.4.10С

В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий оценщика

ALC\_СМС.4.1Е

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

**12.2.8 ALC\_CMC.5 Расширенная поддержка**

Зависимости: ALC\_CMS.1 Охват УК ОО

ALC\_DVS.2 Достаточность мер безопасности

ALC\_LCD.1 Определенная разработчиком модель жизненного цикла

Модель жизненного цикла включает процедуры, инструменты и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают методы проектирования, процедуры проверки, средства контроля управления проектом, процедуры контроля изменений, методы тестирования и процедуры приемки. Эффективная модель жизненного цикла будет учитывать эти аспекты процесса разработки и сопровождения в рамках общей структуры управления, которая распределяет обязанности и контролирует прогресс.

Существуют различные типы ситуаций приемки, которые рассматриваются в разных местах критериев:

— приемка деталей, поставленных субподрядчиками («интеграция»), должна рассматриваться в этом семействе,

— Определение жизненного цикла разработки (ALC\_LCD),

— приемка после внутренних перевозок в Безопасность среды разработки (ALC\_DVS),

— приемка деталей в систему CM в возможностях CM (ALC\_CMC), и

— принятие поставленного ОО потребителем в стадии поставки (ALC\_DEL).

Первые три типа могут пересекаться.

Хотя определение жизненного цикла связано с сопровождением ОО и, следовательно, с аспектами, которые становятся актуальными после завершения оценки, его оценка добавляет уверенности за счет анализа информации о жизненном цикле ОО, предоставленной во время оценки.

Модель жизненного цикла обеспечивает необходимый контроль над разработкой и сопровождением ОО, если модель позволяет в достаточной степени минимизировать опасность того, что ОО не будет соответствовать требованиям безопасности.

Измеримая модель жизненного цикла — это модель, использующая некоторую количественную оценку (арифметические параметры и/или метрики) управляемого продукта для измерения свойств продукта при разработке. Типичными показателями являются показатели сложности исходного кода, плотность дефектов (ошибок на размер кода) или среднее время до отказа. Для оценки безопасности имеют значение все эти метрики, которые используются для повышения качества за счет уменьшения вероятности ошибок и тем самым, в свою очередь, повышения уверенности в безопасности ОО.

Следует учитывать, что существуют стандартизированные модели жизненного цикла с одной стороны (например, водопадная модель) и стандартизированные метрики с другой стороны (например, плотность ошибок), которые можно комбинировать. Серия стандартов ISO/IEC 15408 не требует, чтобы жизненный цикл соответствовал одному стандарту, определяющему оба аспекта.

ALC\_LCD.1 Разработчик определяет процессы жизненного цикла

Цели

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

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

Использование системы УК увеличивает доверие к тому, что элементы конфигурации обслуживаются управляемым образом.

Поддержанию целостности ОО способствует применение средств контроля, исключающих выполнение несанкционированных модификаций ОО («Управление доступом к УК»), а также обеспечение надлежащих функциональных возможностей и использование системы УК.

Процедуры приемки предназначены для того, чтобы подтвердить, что любое создание или модификация элементов конфигурации санкционировано. Процедуры приемки — исключительно важный элемент процессов интеграции и управления жизненным циклом ОО.

В средах разработки, где элементы конфигурации являются сложными, трудно контролировать изменения без поддержки автоматизированными средствами. В частности, эти автоматизированные инструменты должны быть в состоянии поддерживать многочисленные изменения, которые происходят во время разработки, и обеспечивать санкционированность этих изменений. Цель данного компонента состоит в том, чтобы обеспечить управление элементами конфигурации при помощи автоматизированных средств. Если ОО разрабатывается несколькими разработчиками, т. е. имеет место интеграция, то использование автоматизированных средств также целесообразно.

Процедуры поддержки производства позволяют удостовериться в том, что генерация 00 из поставленного набора элементов конфигурации выполнена должным образом, особенно в том случае, когда вовлечены разные разработчики и необходимо осуществить процессы интеграции.

Требование, чтобы система УК была способна идентифицировать версию представления реализации, используемую для генерации 00, помогает обеспечить сохранение целостности этого материала путем применения соответствующих технических, физических и процедурных мер защиты.

Предоставление автоматизированных средств установления различий между версиями ОО и определения того, на какие элементы конфигурации влияют изменения других элементов конфигурации, помогает в определении влияния изменений между последовательными версиями ОО. Это, в свою очередь, может предоставить ценную информацию для вынесения заключения о том, не нарушают ли вносимые изменения согласованность всех элементов друг с другом.

Элементы действий разработчика

ALC\_CMC.5.1D

Разработчик должен предоставить 00 и маркировку для 00.

ALC\_CMC.5.2D

Разработчик должен предоставить документацию УК.

ALC\_CMC.5.3D

Разработчик должен использовать систему УК.

Элементы содержания и представления свидетельств

ALC\_СМС.5.1С

00 должен быть помечен уникальной маркировкой.

ALC\_CMC.5.2C

В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC\_CMC.5.3C

В документации по УК должно быть обоснование того, что процедуры приемки предоставляют рациональный и приемлемый обзор изменений всех элементов конфигурации.

ALC\_CMC.5.4C

В системе УК должны быть уникально идентифицированы все элементы конфигурации.

ALC\_CMC.5.5C

В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

ALC\_CMC.5.6C

Система УК должна поддерживать производство ОО автоматизированными средствами.

ALC\_CMC.5.7C

Система УК должна обеспечивать, что лицо, ответственное за приемку элемента конфигурации в УК, не является разработчиком этого элемента.

ALC\_CMC.5.8C

В системе УК должны быть идентифицированы элементы конфигурации, которые составляют ФБО.

ALC\_CMC.5.9C

Система УК должна поддерживать аудит всех изменений ОО автоматизированными средствами с указанием пользователя, инициирующего изменение, а также даты и времени изменения в журнале аудита.

ALC\_СМС.5.1 ОС

Система УК должна предоставить автоматизированное средство идентификации всех других элементов конфигурации, на которых оказывает влияние изменение конкретного элемента конфигурации.

ALC\_СМС.5.11С

Система УК должна быть в состоянии идентифицировать версию представления реализации, на основании которой сгенерирован ОО.

ALC\_CMC.5.12C

Документация УК должна включать в себя план УК.

ALC\_СМС.5.13С

В плане УК должно содержаться описание того, каким образом система УК используется для разработки 00.

ALC\_СМС.5.14С

План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части 00.

ALC\_СМС.5.15С

В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC\_СМС.5.16С

В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий оценщика

ALC\_СМС.5.1Е

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

ALC\_СМС.5.2Е

Оценщик должен определить, что итогом применения процедур поддержки производства становится 00, аналогичный предоставленному разработчиком для действий по оценке.

**12.3 Область УК (ALC\_CMS)**

**12.3.1 Цели**

Цель этого семейства состоит в определении тех элементов, которые должны быть включены в элементы конфигурации и к которым, следовательно, должны применяться требования семейства ALC\_CMC «Возможности УК». Применение управления конфигурацией по отношению к этим дополнительным элементам обеспечивает получение дополнительного доверия к поддержанию целостности ОО.

**12.3.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе того, что именно из перечисленного ниже требуется включить в элементы конфигурации: ОО и свидетельства оценки, необходимые согласно ТДБ; части ОО; представление реализации, недостатки безопасности, инструментальные средства разработки и связанная с ними информация.

**12.3.3 Замечания по применению**

Требования семейства ALC\_CMS «Область УК» определяют необходимость списка элементов конфигурации и то, что каждый элемент этого списка должен находиться под УК; при этом содержание списка элементов конфигурации в соответствии с требованиями семейства ALC\_CMC «Возможности УК» остается на усмотрение разработчика. Требования семейства ALC\_CMS «Область УК» ограничивают эту возможность разработчика, идентифицируя элементы, которые должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями семейства ALC\_CMC «Возможности УК».

**12.3.4 ALC\_CMS.1 Охват УК объекта оценки**

Зависимости: отсутствуют.

Цели

Система УК может управлять изменениями только тех элементов, которые были включены под контроль системы УК (т.е. элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под контроль системы УК самого ОО и свидетельств оценки, необходимых по ТДБ в ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Замечания по применению

Элемент ALC\_CMS.1.1C содержит требование, что сам ОО и свидетельства оценки, необходимые по ТДБ в ЗБ, должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями к УК семейства ALC\_CMC «Возможности УК».

Элементы действий разработчика

ALC\_CMS.1.1D

Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC\_CMS.1.1C

Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по ТДБ в ЗБ.

ALC\_CMS.1.2C

Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

Элементы действий оценщика

ALC\_CMS.1.1E

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

**12.3.5 ALC\_CMS.2 Охват УК частей ОО**

Зависимости: отсутствуют

Цели

Система УК может управлять изменениями только тех элементов, которые были включены под контроль системы УК (т. е. элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под контроль системы УК самого ОО, составляющих частей ОО и свидетельств оценки, необходимых по ТДБ в ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Замечания по применению

Элемент ALC\_CMS.2.1C содержит требование, что составляющие части ОО (все поставленные заказчику, например, аппаратные части и исполняемые файлы программ) должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями к УК семейства ALC\_CMC «Возможности УК».

Элемент ALC\_CMS.2.3С содержит требование, что в списке элементов конфигурации указывается разработчик каждого значимого для ФБО элемента конфигурации. В данном случае под «разработчиком» понимается не какое-либо лицо, а организация, ответственная за разработку элемента.

Элементы действий разработчика

ALC\_CMS.2.1D

Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC\_CMS.2.1C

Список элементов конфигурации должен включать следующее: сам ОО и свидетельства оценки, необходимые по требованиям доверия к безопасности, а также части, которые входят в состав ОО.

ALC\_CMS.2.2C

Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC\_CMS.2.3C

Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC\_CMS.2.1E

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

**12.3.6 ALC\_CMS.3 Охват УК представления реализации**

Зависимости: отсутствуют

Цели

Система УК может управлять изменениями только тех элементов, которые были включены под контроль системы УК (т.е. элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под контроль системы УК самого ОО, составляющих частей ОО, представления реализации ОО и свидетельств оценки, необходимых по требованиям доверия к безопасности в ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Замечания по применению

Элемент ALC\_CMS.3.1 С содержит требование, что представление реализации ОО должно быть включено в список элементов конфигурации и, следовательно, должно находиться под УК в соответствии с требованиями к УК семейства ALC\_CMC «Возможности УК».

Элементы действий разработчика

ALC\_CMS.3.1D

Разработчик должен представить список элементов конфигурации для 00.

Элементы содержания и представления свидетельств

ALC\_CMS.3.1C

Список элементов конфигурации должен включать следующее: сам 00 и свидетельства оценки, необходимые по требованиям доверия к безопасности, части, которые входят в состав ОО, а также представление реализации.

ALC\_CMS.3.2C

Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC\_CMS.3.3C

Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC\_CMS.3.1E

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

**12.3.7 ALC\_CMS.4 Охват УК отслеживания проблем**

Зависимости: отсутствуют

Цели

Система УК может контролировать изменения только тех элементов, которые были включены под контроль системы УК (т.е. элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под контроль системы УК самого ОО, составляющих частей ОО, представления реализации ОО и свидетельств оценки, необходимых по требованиям доверия к безопасности в ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Включение недостатков безопасности под контроль системы УК не позволяет пропустить или проигнорировать сообщения о недостатках защиты, давая возможность разработчику отслеживать недостатки безопасности вплоть до их устранения.

Замечания по применению

Элемент ALC\_CMS.4.1C содержит требование, что недостатки безопасности должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями УК семейства ALC\_CMC «Возможности УК». Согласно этому требованию, должно обеспечиваться сопровождение не только детальной информации о возникавших ранее недостатках и методах их устранения, но и об имеющихся в настоящий момент недостатках безопасности.

Элементы действий разработчика

ALC\_CMS.4.1D

Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC\_CMS.4.1C

Список элементов конфигурации должен включать следующее: сам ОО; свидетельства оценки, необходимые по требованиям доверия к безопасности; представление реализации; сведения о недостатках безопасности и стадии их устранения.

ALC\_CMS.4.2C

Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC\_CMS.4.3C

Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC\_CMS.4.1E

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

**12.3.8 ALC\_CMS.5 Охват УК инструментальных средств разработки**

Зависимости: отсутствуют

Цели

Система УК может контролировать изменения только тех элементов, которые были включены под контроль системы УК (т. е. элементов конфигурации, идентифицированных в списке элементов конфигурации). Включение под контроль системы УК самого ОО, составляющих частей ОО, представления реализации ОО и свидетельств оценки, необходимых по требованиям доверия к безопасности в ЗБ, обеспечивает доверие к тому, что они могут быть модифицированы только контролируемым способом при наличии соответствующих полномочий.

Включение недостатков безопасности под контроль системы УК не позволяет пропустить или проигнорировать сообщения о недостатках безопасности, давая возможность разработчику отслеживать недостатки безопасности вплоть до их устранения.

Инструментальные средства разработки играют важную роль в обеспечении производства качественной версии ОО. Следовательно, важно управлять модификацией этих средств.

Замечания по применению

Элемент ALC\_CMS.5.1 С содержит требование, что средства разработки и связанная с ними информация должны быть включены в список элементов конфигурации и, следовательно, должны находиться под УК в соответствии с требованиями УК семейства ALC\_CMC «Возможности УК». Примерами средств разработки являются языки программирования и компиляторы. Информация, имеющая отношение к элементам генерации ОО (такая, как опции компилятора, опции инсталляции/генерации и опции компоновки) — пример информации, относящейся к инструментальным средствам разработки.

Элементы действий разработчика

ALC\_CMS.5.1D

Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC\_CMS.5.1C

Список элементов конфигурации должен включать следующее: сам ОО; составляющие части ОО; представление реализации; сведения о недостатках безопасности и стадии их устранения; инструментальные средства разработки и связанную с ними информацию, а также свидетельства оценки, необходимые по требованиям доверия к безопасности.

ALC\_CMS.5.2C

Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC\_CMS.5.3C

Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC\_CMS.5.1E

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

**12.4 Поставка (ALC\_DEL)**

**12.4.1 Цели**

Назначение данного семейства состоит в том, чтобы обеспечить безопасную передачу готового ОО из среды разработки под ответственность пользователя.

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

**12.4.2 Ранжирование компонентов**

Семейство содержит только один компонент. Усиление уровня защиты достигается путем предъявления требований к соизмеримости процедур поставки с потенциалом нападения предполагаемого нарушителя, определяемым в семействе «Анализ уязвимостей» (AVA\_VAN).

**12.4.3 Замечания по применению**

Вопросы транспортировки от субподрядчиков к разработчику или между различными местами разработки рассматриваются не в этом семействе, а в семействе «Безопасность разработки» (ALC\_DVS).

Окончанием фазы поставки считается факт передачи ОО под ответственность пользователя.

Следует, чтобы в процедурах поставки затрагивались следующие вопросы:

a) обеспечение точного соответствия между ОО, полученного потребителем, и прошедшим оценку ОО;

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

c) предотвращение поставки фальсифицированной версии ОО;

d) избежание нежелательной утечки информации о распространении ОО потребителю; возможны

случаи, при которых потенциальным нарушителям не следует знать о том, когда и каким образом поставляется ОО;

e) избежание/обнаружение перехвата ОО во время поставки; и

f) избежание задержки поставки или невыполнения поставки ОО.

К процедурам поставки следует относить также и действия получателя, подразумеваемые по рассмотренным выше вопросам. Согласованное описание таких действий рассматривается в соответствии с требованиями семейства «Подготовительные процедуры» (AGD\_PRE) при наличии такого описания.

**12.4.4 ALC\_DEL.1 Процедуры поставки**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_DEL.1.1D

Разработчик должен задокументировать процедуры поставки ОО или его частей потребителю.

ALC\_DEL.1.2D

Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ALC\_DEL.1.1C

Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при распространении версий ОО потребителю.

Элементы действий оценщика

ALC\_DEL.1.1E

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

**12.5 Безопасность разработки (ALC\_DVS)**

**12.5.1 Цели**

Семейство «Безопасность разработки» связано с физическими, процедурными, организационны-

ми и другими мерами безопасности, которые могут применяться в среде разработки для защиты ОО

и его частей. К этому относится и физическая защита места разработки и любые процедуры, связанные

с отбором персонала, занимающегося разработкой.

**12.5.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе того, требуется ли логическое обоснование достаточности мер безопасности.

**12.5.3 Замечания по применению**

Данное семейство связано с мерами по устранению или ослаблению угроз, существующих в месте разработки.

Оценщику следует посетить место разработки для оценки свидетельств безопасности разработки.

Кроме того, следует посетить и субподрядчиков, вовлеченных в разработку и производство ОО. Решение о непосещении мест разработки должно быть согласовано с руководящим органом по оценке.

Хотя безопасность разработки касается и сопровождения ОО и, соответственно, тех аспектов, которые становятся значимыми после завершения оценки, требования семейства «Безопасность разработки» (ALC\_DVS) специфицируют только то, что меры безопасности разработки должны быть готовы к использованию во время оценки. Кроме того, «Безопасность разработки» (ALC\_DVS) не содержит требований по отношению к намерениям организатора применять меры безопасности разработки в будущем, после завершения оценки.

Известно, что сохранение конфиденциальности не всегда может включаться в задачи защиты ОО в среде его разработки. Использование слова «необходимый» в компонентах данного семейства предусматривает возможность выбора соответствующих мер защиты.

**12.5.4 ALC\_DVS.1 Идентификация мер безопасности**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_DVS.1.1D

Разработчик должен представить документацию по безопасности разработки.

Элементы содержания и представления свидетельств

ALC\_DVS.1.1C

Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта 00 и его реализации в среде разработки.

Элементы действий оценщика

ALC\_DVS.1.1E

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

ALC\_DVS.1.2E

Оценщик должен подтвердить, что меры безопасности применяются.

**12.5.5 ALC\_DVS.2 Достаточность мер безопасности**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_DVS.2.1D

Разработчик должен представить документацию по безопасности разработки.

Элементы содержания и представления свидетельств

ALC\_DVS.2.1C

Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

ALC\_DVS.2.2C

Свидетельство должно содержать логическое обоснование того, что меры безопасности обеспечивают необходимый уровень защиты для поддержания конфиденциальности и целостности ОО.

Элементы действий оценщика

ALC\_DVS.2.1E

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

ALC\_DVS.2.2E

Оценщик должен подтвердить, что меры безопасности применяются.

**12.6 Устранение недостатков (ALC\_FLR)**

**12.6.1 Цели**

Семейство «Устранение недостатков» содержит требование, чтобы обнаруженные недостатки безопасности отслеживались и исправлялись разработчиком. Хотя в процессе оценки 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 для распространения информации о недостатках и их исправлении.

**12.6.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе расширения области применения процедур устранения недостатков и повышения строгости политик устранения недостатков.

**12.6.3 Замечания по применению**

В данном семействе обеспечивается доверие к сопровождению и поддержке ОО в будущем путем предъявления требований к разработчику ОО по отслеживанию и исправлению недостатков ОО. Кроме того, приводятся требования к распространению сведений об исправлении недостатков. Однако это семейство не налагает требований, выходящих за рамки текущей оценки.

Пользователь ОО считается основным ответственным лицом в организации за получение и применение исправлений недостатков безопасности. Таким лицом необязательно является 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 либо отдельным пользователем, либо централизованно административным органом.

В процедурах устранения недостатков следует описать методы реагирования на все типы выявленных недостатков. Об этих недостатках могут сообщить разработчик ОО, пользователи ОО, другие стороны, знакомые с ОО. Некоторые недостатки не могут быть исправлены немедленно. Не исключено, что недостаток вообще не может быть исправлен, и необходимо применить другие (например, процедурные) меры. В представленной документации следует охватывать процедуры по обеспечению исправлений в местах эксплуатации, а также предоставлять информацию о недостатках, для которых исправление отложено или невозможно (с описанием того, что следует делать в этой ситуации).

Изменения, вносимые в оцененный ОО, приводят к тому, что он не может более считаться оцененным, а первоначальные результаты оценки являются применимыми к измененной версии лишь в некоторой степени. Поэтому термин «релиз ОО», используемый в данном семействе, относится к версии продукта, который является релизом сертифицированного ОО, в который были внесены изменения.

**12.6.4 ALC\_FLR.1 Базовое устранение недостатков**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_FLR.1.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

Элементы содержания и представления свидетельств

ALC\_FLR.1.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

ALC\_FLR.1.2C

Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC\_FLR.1.3C

Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

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.

Элементы действий оценщика

ALC\_FLR.1.1E

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

**12.6.5 ALC\_FLR.2 Процедуры сообщений о недостатках**

Зависимости: отсутствуют.

Цели

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.

Элементы действий разработчика

ALC\_FLR.2.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

ALC\_FLR.2.2D

Разработчик должен установить процедуру получения и отработки всех сообщений о недостатках безопасности и запросов на их исправление.

ALC\_FLR.2.3D

Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

Элементы содержания и представления свидетельств

ALC\_FLR.2.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

ALC\_FLR.2.2C

Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC\_FLR.2.3C

Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

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.

ALC\_FLR.2.5C

Процедуры устранения недостатков должны описывать средства, посредством которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.

ALC\_FLR.2.6C

Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.

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 недостатков.

ALC\_FLR.2.8C

Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.

Элементы действий оценщика

ALC\_FLR.2.1E

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

**12.6.6 ALC\_FLR.3 Систематическое устранение недостатков**

Зависимости: отсутствуют.

Цели

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.

Элементы действий разработчика

ALC\_FLR.3.1D

Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

ALC\_FLR.3.2D

Разработчик должен установить процедуру получения и отработки всех сообщений пользователей о недостатках безопасности и запросов на исправление этих недостатков.

ALC\_FLR.3.3D

Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

Элементы содержания и представления свидетельств

ALC\_FLR.3.1C

Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

ALC\_FLR.3.2C

Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC\_FLR.3.3C

Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

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.

ALC\_FLR.3.5C

Процедуры устранения недостатков должны описывать средства, посредством которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.

ALC\_FLR.3.6C

Процедуры устранения недостатков должны включать процедуру своевременного реагирования для автоматического распространения сообщений о недостатках безопасности и материалов по их исправлению зарегистрированным пользователям, для которых эти недостатки могут иметь последствия.

ALC\_FLR.3.7C

Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.

ALC\_FLR.3.8C

Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых недостатков.

ALC\_FLR.3.9C

Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.

ALC\_FLR.3.10C

Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут регистрироваться у разработчика, чтобы иметь право получать сообщения о недостатках безопасности и исправления.

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.

Элементы действий оценщика

ALC\_FLR.3.1E

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

**12.7 Определение жизненного цикла (ALC\_LCD)**

**12.7.1 Цели**

Плохое управление процессами разработки и сопровождения ОО может приводить к тому, что ОО отвечает не всем ФТБ. Поэтому важно, чтобы модель разработки и сопровождения ОО была установлена как можно раньше в жизненном цикле ОО.

Использование модели разработки и сопровождения ОО не дает уверенности, что ОО будет отвечать всем ФТБ. Может оказаться, что выбранная модель будет недостаточной или неадекватной, и поэтому прирост качества ОО не будет заметен. Использование модели жизненного цикла, которая одобрена некоторой группой экспертов (например, специалистами-теоретиками, органами по стандартизации), повышает вероятность того, что применение модели разработки и сопровождения будет содействовать тому, что ОО отвечает предъявляемым ФТБ. Использование модели жизненного цикла, включая некоторую количественную оценку, позволяет получить дополнительное доверие общему качеству процесса разработки 00.

**12.7.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе повышения требований к измеримости модели жизненного цикла, а также к согласованности с этой моделью.

**12.7.3 Замечания по применению**

Модель жизненного цикла объединяет в себе процедуры, инструментальные средства и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают методы проектирования, процедуры просмотра, средства управления проектом, процедуры управления изменениями, методы тестирования и процедуры приемки. Эффективная модель жизненного цикла позволит включить аспекты процесса разработки и сопровождения в общую структуру управления, которая устанавливает обязанности и контролирует ход процессов.

Возможны различные ситуации при приемке, при возникновении которых приходится иметь дело с различными разделами настоящего стандарта: приемку частей, полученных от субподрядчиков («интеграцию») следует рассматривать в рамках требований данного семейства «Определение жизненного цикла» (ACL\_LCD), последующую приемку при внутренних транспортировках— в рамках требований семейства «Безопасность разработки» (ALC\_DVS), приемку частей в систему УК — в рамках требований семейства «Возможности УК» (ALC\_CMC), а приемку поставленного пользователю ОО — в рамках требований семейства «Поставка» (ALC\_DEL). Первые три типа приемки могут частично совпадать.

Хотя в семействе «Определение жизненного цикла» рассматривается сопровождение ОО и, соответственно, аспекты, которые становятся значимыми после завершения оценки, оценка по требованиям данного семейства позволяет получить дополнительное доверие за счет анализа информации о жизненном цикле ОО, представленной во время оценки.

Модель жизненного цикла предоставляет необходимый контроль за разработкой и сопровождением ОО, если она успешно минимизирует опасность того, что ОО не будет соответствовать предъявляемым к нему требованиям безопасности.

Измеримая модель жизненного цикла — это модель, использующая количественные параметры (арифметические и/или метрические) управляемого продукта для измерения характеристик разработки продукта. Типовые метрические показатели — сложность исходного кода, концентрация дефектов (количество ошибок на участок кода), среднее время до сбоя. Для оценки безопасности все эти показатели являются значимыми, что используется для увеличения качества системы путем снижения вероятности сбоев и, таким образом, для обеспечения повышения доверия к безопасности ОО.

Следует принять во внимание, что, с одной стороны, существуют стандартные модели жизненного цикла (например, «модель водопада», последовательной разработки), с другой стороны — стандартные метрические показатели (например, количество ошибок на участок кода), которые могут комбинироваться. В настоящем стандарте не требуется, чтобы жизненный цикл следовал одному стандарту для обоих этих аспектов.

**12.7.4 ALC\_LCD.1 Определенная разработчиком модель жизненного цикла**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_LCD.1.1D

Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

ALC\_LCD.1.2D

Разработчик должен представить документацию по определению жизненного цикла.

Элементы содержания и представления свидетельств

ALC\_LCD.1.1C

Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

ALC\_LCD.1.2C

Модель жизненного цикла должна обеспечить необходимый контроль над разработкой и сопровождением ОО.

Элементы действий оценщика

ALC\_LCD.1.1E

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

**12.7.5 ALC\_LCD.2 Стандартизованная модель жизненного цикла**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_LCD.2.1D

Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении 00.

ALC\_LCD.2.2D

Разработчик должен представить документацию по определению жизненного цикла.

ALC\_LCD.2.3D

Разработчик должен использовать стандартизованную модель жизненного цикла для разработки и сопровождения ОО.

ALC\_LCD.2.4D

Разработчик должен предоставить документацию по выходным данным жизненного цикла.

Элементы содержания и представления свидетельств

ALC\_LCD.2.1C

Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО, в том числе детализацию арифметических параметров и/или метрик, используемых для измерения качества ОО и/или его разработки.

ALC\_LCD.2.2C

В модели жизненного цикла должен быть обеспечен необходимый контроль над разработкой и сопровождением ОО.

ALC\_LCD.2.3C

В документации по выходным данным жизненного цикла должны быть представлены результаты измерения качества разработки ОО с использованием стандартизированной модели.

Элементы действий оценщика

ALC\_LCD.2.1E

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

ALC\_LCD.2.2E

Оценщик должен подтвердить, что измерения процессов разработки ОО и связанных с безопасностью свойств ОО способствуют улучшениям процессов разработки и/или самого ОО.

**12.8 Артефакты разработки ОО (ALC\_TDA)**

**12.8.1 Цели**

Данное семейство стремится добавить доверия к процессу разработки или развитию. Он фокусируется на создании определенных артефактов в процессе разработки. Эти артефакты используются позднее для оценки степени надежности процесса разработки. Это доверие реализуется посредством проверки сгенерированных артефактов на предмет подтверждения того, что они являются достаточным доказательством для надежной разработки.

Это семейство вводит методы разработки в процесс разработки для создания необходимых артефактов для реализации надежной разработки. Если требование в этом семействе явно не определяет использование автоматизации для создания требуемых артефактов, разработчик может выполнить соответствующую практику вручную или использовать некоторую интегрированную автоматизацию в процессе разработки, или использовать гибридный метод того и другого. Ожидается, что степень доверия к процессу разработки пропорциональна степени внедрения автоматизации для реализации соответствующей практики в процессе разработки.

Это семейство также связано с семейством ALC\_TAT. Поскольку ALC\_TAT фокусируется на аспекте инструментов и методов разработки, анализа и реализации ОО, он обеспечивает необходимый контекст при описании практик этого семейства, внедряемых в процесс разработки.

**12.8.2 Ранжирование компонентов**

Компоненты этого семейства ранжируются на основе увеличения перекрестной проверки на соответствие соответствующим свидетельствам компонентов других семейств других классов обеспечения безопасности.

**12.8.3 Замечания по применению**

Требования ALC\_TDA.1 обеспечивают определенную степень доверия к способности разработчика идентифицировать набор представлений реализации, который фактически использовался во время создания ОО. Такая степень доверия помогает положительно ответить на вопрос «действительно ли это исходный код для этого программного обеспечения» или «действительно ли это конструкция или описание уровня передачи регистров (RTL) для этого аппаратного обеспечения интегральной схемы» или «это действительно набор представлений реализации для данного ОО», что потенциально важно при оценке. Такая степень доверия строится на

а) время, когда набор идентификаторов представления реализации записывается или регистрируется,

b) целостность и подлинность записи идентификаторов представления реализации, и

c) прослеживаемость идентификаторов представления реализации из ОО.

В случае, когда некоторые элементы представления реализации также включены в список конфигурации из-за ALC\_CMS.3, требования в ALC\_TDA.2 гарантируют, что эти элементы представления реализации действительно идентифицируются посредством использования идентификаторов представления реализации ALC\_TDA.1.

Благодаря точной регистрации фактического представления реализации, используемого инструментами разработки в рамках ALC\_TAT, это обеспечивает дополнительное свидетельство, позволяющее убедить третью сторону в том, что повторное создание ОО функционально эквивалентно исходному ОО.

Требования ALC\_TDA.3 предоставляют разработчику возможность подтвердить отсутствие функциональных различий между двумя, возможно, явно разными ОО, которые были независимо сгенерированы из идентичного набора представлений реализации.

**12.8.4 ALC\_TDA.1 Уникально идентифицирующее представление реализации**

Зависимости: отсутствуют.

Элементы действий разработчика

ALC\_TDA.1.1D

Разработчик должен идентифицировать отдельные элементы представления реализации ОО для записи списка уникальных идентификаторов представления реализации ОО по мере того, как средство разработки генерирует ОО.

ALC\_TDA.1.2D

Разработчик должен использовать текущую дату и время для отметки времени в списке уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.1.3D

Разработчик должен поддерживать целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.1.4D

Разработчик должен обеспечить подлинность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, с сохранением информации о происхождении (автора).

ALC\_TDA.1.5D

Разработчик должен иметь возможность проследить путь от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.1.6D

Разработчик должен подготовить и предоставить документацию, описывающую

а) создание разработчиком списка уникальных идентификаторов представления реализации ОО, как записано;

b) временная метка разработчика применяется к списку уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

c) ведение информации о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

d) поддержание целостности списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации (автора) о происхождении;

e) механизм разработчика для отслеживания от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

Элементы контента и презентации

ALC\_TDA.1.1C

Список уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должен демонстрировать соответствие между идентификаторами элементов представления реализации ОО и именами элементов представления реализации ОО.

ALC\_TDA.1.2C

Имена элементов представления реализации ОО должны быть в той же форме, в которой они используются или на которые ссылается средство разработки для создания ОО.

ALC\_TDA.1.3C

Временная метка списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должна соответствовать времени создания ОО.

ALC\_TDA.1.4C

Информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, должна быть согласована с информацией о происхождении (автора) ОО. Информацией о происхождении автора может быть имя филиала организации.

Элементы действий оценщика

ALC\_TDA.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ALC\_TDA.1.2E

Оценщик должен подтвердить, что инструмент разработки для создания ОО способен использовать или ссылаться на имена элементов представления реализации.

ALC\_TDA.1.3E

Оценщик должен подтвердить, что список уникальных идентификаторов представления реализации ОО, записанный во время генерации ОО, соответствует времени создания ОО.

ALC\_TDA.1.4E

Оценщик должен подтвердить, что информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, согласуется с информацией о происхождении (автора) ОО.

ALC\_TDA.1.5E

Оценщик должен проверить целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации о происхождении (автора).

ALC\_TDA.1.6E

Оценщик должен подтвердить способность разработчика проследить от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

**12.8.5 ALC\_TDA.2 Соответствующее представление области реализации CMS**

Зависимости: ALC\_CMS.3 Представление реализации, охват CM

Элементы действий разработчика

ALC\_TDA.2.1D

Разработчик должен идентифицировать отдельные элементы представления реализации ОО для записи списка уникальных идентификаторов представления реализации ОО по мере того, как средство разработки генерирует ОО.

ALC\_TDA.2.2D

Разработчик должен использовать текущую дату и время для отметки времени в списке уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.2.3D

Разработчик должен поддерживать целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.2.4D

Разработчик должен обеспечить подлинность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, с сохранением информации о происхождении (автора).

ALC\_TDA.2.5D

Разработчик должен иметь возможность проследить путь от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.2.6D

Разработчик должен подготовить и предоставить документацию, описывающую

а) создание разработчиком списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

b) временная метка разработчика применяется к списку уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

c) ведение информации о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

d) поддержание целостности списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации (автора) о происхождении;

e) механизм разработчика для отслеживания от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.2.7D

Разработчик должен предоставить доказательства того, что элементы представления реализации в области конфигурации ALC\_CMS.3 идентифицируются списком уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

Элементы контента и презентации

ALC\_TDA.2.1C

Список уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должен демонстрировать соответствие между идентификаторами элементов представления реализации ОО и именами элементов представления реализации ОО.

ALC\_TDA.2.2C

Имена элементов представления реализации ОО должны быть в той же форме, в которой они используются или на которые ссылается средство разработки для создания ОО.

ALC\_TDA.2.3C

Временная метка списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должна соответствовать времени создания ОО.

ALC\_TDA.2.4C

Информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, должна быть согласована с информацией о происхождении (автора) ОО. Информацией о происхождении автора может быть имя филиала организации.

ALC\_TDA.2.5C

Список идентификаторов элементов представления реализации в области конфигурации ALC\_CMS.3 должен совпадать со списком уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

Элементы действий оценщика

ALC\_TDA.2.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ALC\_TDA.2.2E

Оценщик должен подтвердить, что инструмент разработки для создания ОО способен использовать или ссылаться на имена элементов представления реализации.

ALC\_TDA.2.3E

Оценщик должен подтвердить, что список уникальных идентификаторов представления реализации ОО, записанный во время генерации ОО, соответствует времени создания ОО.

ALC\_TDA.2.4E

Оценщик должен подтвердить, что информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, согласуется с информацией о происхождении (автора) ОО.

ALC\_TDA.2.5E

Оценщик должен проверить целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации о происхождении (автора).

ALC\_TDA.2.6E

Оценщик должен подтвердить способность разработчика проследить от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.2.7E

Оценщик должен подтвердить, что список идентификаторов элементов представления реализации в области конфигурации ALC\_CMS.3 соответствует списку уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

**12.8.6 ALC\_TDA.3 Регенерация ОО с помощью четко определенных инструментов разработки**

Зависимости:

ALC\_CMS.3 Охват CM представления реализации

ALC\_TAT.1 Четко определенные инструменты разработки и

ADV\_IMP.1 Представление реализации ФБО

Элементы действий разработчика

ALC\_TDA.3.1D

Разработчик должен идентифицировать отдельные элементы представления реализации ОО для записи списка уникальных идентификаторов представления реализации ОО по мере того, как средство разработки генерирует ОО.

ALC\_TDA.3.2D

Разработчик должен использовать текущую дату и время для отметки времени в списке уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.3D

Разработчик должен поддерживать целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.4D

Разработчик должен обеспечить подлинность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, с сохранением информации о происхождении (автора).

ALC\_TDA.3.5D

Разработчик должен иметь возможность проследить путь от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.6D

Разработчик должен подготовить и предоставить документацию, описывающую

а) создание разработчиком списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

b) временная метка разработчика применяется к списку уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

c) ведение информации о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО;

d) поддержание целостности списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации (автора) о происхождении;

e) механизм разработчика для отслеживания от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.7D

Разработчик должен предоставить доказательства того, что элементы представления реализации в области конфигурации ALC\_CMS.3 идентифицируются списком уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.8D

После применения инструментов разработки к другой копии представления реализации ОО в соответствии со списком уникальных идентификаторов представления реализации ОО для повторного создания копии ОО разработчик должен объяснить функциональные различия, если таковые имеются, между копией ОО и исходным ОО.

ALC\_TDA.3.9D

Разработчик должен подготовить и предоставить документацию, объясняющую функциональные различия, если таковые имеются, между восстановленной копией ОО и исходным ОО.

Элементы контента и презентации

ALC\_TDA.3.1C

Список уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должен демонстрировать соответствие между идентификаторами элементов представления реализации ОО и именами элементов представления реализации ОО.

ALC\_TDA.3.2C

Имена элементов представления реализации ОО должны быть в той же форме, в которой они используются или на которые ссылается средство разработки для создания ОО.

ALC\_TDA.3.3C

Временная метка списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, должна соответствовать времени создания ОО.

ALC\_TDA.3.4C

Информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, должна быть согласована с информацией о происхождении (автора) ОО. Информацией о происхождении автора может быть имя филиала организации.

ALC\_TDA.3.5C

Список идентификаторов элементов представления реализации в области конфигурации ALC\_CMS.3 должен совпадать со списком уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.6C

Объяснение разработчиком функциональных различий, если таковые имеются, между регенерированной копией ОО и исходным ОО, должно учитывать все видимые различия, если таковые имеются, между регенерированной копией ОО и исходным ОО.

Элементы действий оценщика

ALC\_TDA.3.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ALC\_TDA.3.2E

Оценщик должен подтвердить, что инструмент разработки для создания ОО способен использовать или ссылаться на имена элементов представления реализации.

ALC\_TDA.3.3E

Оценщик должен подтвердить, что список уникальных идентификаторов представления реализации ОО, записанный во время генерации ОО, соответствует времени создания ОО.

ALC\_TDA.3.4E

Оценщик должен подтвердить, что информация о происхождении (автора) списка уникальных идентификаторов представления реализации ОО, записанная во время генерации ОО, согласуется с информацией о происхождении (автора) ОО.

ALC\_TDA.3.5E

Оценщик должен проверить целостность списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО, а также связанной с ним временной метки и информации о происхождении (автора).

ALC\_TDA.3.6E

Оценщик должен подтвердить способность разработчика проследить от ОО до списка уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.7E

Оценщик должен подтвердить, что список идентификаторов элементов представления реализации в области конфигурации ALC\_CMS.3 соответствует списку уникальных идентификаторов представления реализации ОО, записанных во время генерации ОО.

ALC\_TDA.3.8E

Оценщик должен проверить, что объяснение разработчиком функциональных различий, если таковые имеются, между регенерированной копией ОО и исходным ОО, учитывает все видимые различия, если таковые имеются, между регенерированной копией ОО и исходным ОО.

**12.9 Инструментальные средства и методы (ALC\_TAT)**

**12.9.1 Цели**

Требования данного семейства связаны с выбором инструментальных средств, используемых для разработки, анализа и реализации ОО. Семейство содержит требования по предотвращению использования плохо определенных, несогласованных или неверных инструментальных средств для разработки ОО. Это относится, в частности, к языкам программирования, документации, стандартам реализации и некоторым другим частям ОО, например вспомогательным динамическим библиотекам.

**12.9.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе повышения требований к описанию и области применения стандартов реализации и документации по опциям, зависимым от реализации.

**12.9.3 Замечания по применению**

Существуют определенные требования к полностью определенным средствам. Полностью определенными называют инструментальные средства, которые полно и четко описаны. Например, принято считать полностью определенными языки программирования и системы автоматизации проектирования (САПР), которые основаны на стандартах, изданных органами по стандартизации. Для средств, разработанных самими разработчиками ОО, потребуется проведение дополнительных исследований для определения того, являются ли они полностью определенными.

Требование элемента А1\_С\_ТАТ.1.2С применяют, главным образом, к языкам программирования для обеспечения однозначности всех языковых конструкций исходного текста.

Руководства по реализации компонентов ALC\_TAT2 и ALC\_TAT3 могут быть приняты в качестве стандартов реализации, если они были одобрены группой экспертов (например, специалистами-теоретиками, органами по стандартизации). Стандарты реализации обычно общедоступны и являются принятыми на практике в определенных сферах, но руководства по реализации, уточненные разработчиком, также могут быть приняты в качестве стандарта; акцент при этом делается на компетентность разработчика.

В данном семействе различают стандарты реализации, которые применялись разработчиком (ALC\_TAT.2.3D), и стандарты реализации для «всех частей ОО» (ALC\_TAT.3.3D), куда дополнительно включены программные, аппаратные или программно-аппаратные средства сторонних разработчиков.

Список элементов конфигурации, представленный в семействе «Охват УК» (ALC\_CMS) предъявляет требования к тому, чтобы для каждого элемента конфигурации, значимого для ФБО, было указано, был ли он создан разработчиком ОО или сторонними разработчиками.

**12.9.4 ALC\_TAT.1 Полностью определенные инструментальные средства разработки**

Зависимости: ADV\_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ALC\_TAT.1.1D

Разработчик должен идентифицировать каждое инструментальное средство, используемое для разработки ОО.

ALC\_TAT.1.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

Элементы содержания и представления свидетельств

ALC\_TAT.1.1C

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC\_TAT.1.2C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех языковых конструкций, используемых в реализации.

ALC\_TAT.1.3C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.

Элементы действий оценщика

ALC\_TAT.1.1E

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

**12.9.5 ALC\_TAT.2 Соответствие стандартам реализации**

Зависимости: ADV\_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ALC\_TAT.2.1D

Разработчик должен идентифицировать каждое инструментальное средство, используемое для разработки ОО.

ALC\_TAT.2.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

ALC\_TAT.2.3D

Разработчик должен привести описание применявшихся стандартов реализации.

Элементы содержания и представления свидетельств

А1\_С\_ТАТ.2.1С

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC\_TAT.2.2C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех конструкций языка, используемых в реализации.

ALC\_TAT.2.3C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.

Элементы действий оценщика

ALC\_TAT.2.1E

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

ALC\_TAT.2.2E

Оценщик должен подтвердить факт применения стандартов реализации.

**12.9.6 ALC\_TAT.3 Соответствие всех частей ОО стандартам реализации**

Зависимости: ADV\_IMP.1 Представление реализации ФБО

Элементы действий разработчика

ALC\_TAT.3.1D

Разработчик должен идентифицировать каждое инструментальное средство, используемое для разработки ОО.

ALC\_TAT.3.2D

Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

ALC\_TAT.3.3D

Разработчик должен привести описание стандартов реализации для всех частей ОО.

Элементы содержания и представления свидетельств

А1\_С\_ТАТ.3.1С

Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC\_TAT.3.2C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех конструкций языка, используемых в реализации.

ALC\_TAT.3.3C

В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.

Элементы действий оценщика

А1\_С\_ТАТ.3.1Е

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

ALC\_TAT.3.2E

Оценщик должен подтвердить факт применения стандартов реализации.

**12.10 Интеграция частей состава и проверка согласованности процедур доставки (ALC\_COMP)**

**12.10.1 Цели**

Цель этого семейства – определить:

- правильная версия зависимого компонента установлена/встроена в правильную версию соответствующего базового компонента, и

- подготовительные процедуры разработчика базового компонента и разработчика зависимого компонента совместимы с процедурами приемки интегратора составного продукта.

12.10.2 Ранжирование компонентов

Это семейство содержит только один компонент.

12.10.3 Замечания по применению

Оценщик составного продукта должен проверить, что правильная версия оцениваемого зависимого компонента была установлена в оцениваемую версию соответствующего базового компонента составного продукта или встроена в него.

Спонсор оценки составного продукта должен обеспечить, чтобы соответствующие доказательства, полученные интегратором составного продукта, были доступны оценщику составного продукта. Это свидетельство может включать, среди прочего, список конфигурации разработчика базового компонента (например, представленный в его заявлении о подтверждении).

Оценщик составного продукта должен проверить, что процедуры поставки разработчика базового компонента и разработчика зависимого компонента совместимы с процедурами приемки, используемыми интегратором составного продукта.

Оценщик составного продукта должен проверить, что все параметры конфигурации, предписанные разработчиком базового компонента и разработчиком зависимого компонента (например, данные предварительной персонализации, сценарии предварительной персонализации), используются интегратором составного продукта.

Спонсор оценки составного продукта должен обеспечить, чтобы соответствующие доказательства, полученные интегратором составного продукта, были доступны оценщику составного продукта. Это свидетельство может включать, среди прочего, элемент свидетельства приема, принятия и параметризации зависимого компонента разработчиком базового компонента (например, в форме его заявления о подтверждении).

**12.10.4 ALC\_COMP.1 Интеграция зависимого компонента в связанный базовый компонент и проверка согласованности для процедур поставки и приемки**

Зависимости: отсутствуют

Элементы действий разработчика

ALC\_COMP.1.1D

Разработчик должен предоставить доказательства конфигурации компонентов.

Элементы контента и презентации

ALC\_COMP.1.1C

Свидетельства конфигурации компонентов должны показывать, что оцененная версия зависимого компонента была установлена в оцененную версию соответствующего базового компонента или встроена в нее.

ALC\_COMP.1.2C

Свидетельства конфигурации компонентов должны показывать, что:

a) Доказательства совместимости поставки и приемки должны показывать, что процедуры поставки разработчика базового компонента и разработчика зависимого компонента совместимы с процедурами приемки интегратора составного продукта.

b) Доказательства должны показывать, что подготовительные инструкции, предписанные разработчиком базового компонента и разработчиком зависимого компонента, либо фактически используются интегратором составного продукта, либо совместимы с руководством интегратора составного продукта и не противоречат друг другу.

Элементы действий оценщика

ALC\_COMP.1.1E

Оценщик должен подтвердить, что предоставленная информация соответствует всем требованиям к содержанию и представлению доказательств.

ALC\_COMP.1.2E

Оценщик должен подтвердить, что доказательства совместимости доставки являются полными, последовательными и внутренне непротиворечивыми.

## **13 Класс АТЕ: Тестирование**

**13.1 Общие положения**

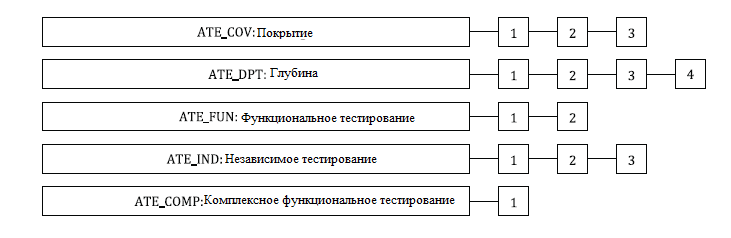
Класс «Тестирование» включает в себя четыре семейства: ATE\_COV «Покрытие», ATE\_DPT «Глубина», ATE\_FUN «Функциональное тестирование» nATE\_IND «Независимое тестирование» (например, функциональное тестирование, выполняемое оценщиками). Тестирование позволяет получить доверие к тому, что ФБО функционирует в описанном (в функциональной спецификации, проекте ОО, представлении реализации) режиме.

Основное внимание в требованиях этого класса уделено подтверждению того, что ФБО выполняются согласно описаниям в проекте. Этот класс не распространяется на тестирование проникновения, которое основывается на анализе ФБО, направленном специально на идентификацию уязвимостей в проекте и реализации ФБО. Тестирование проникновения рассматривается отдельно как аспект оценки уязвимостей в классе AVA «Оценка уязвимостей».

В классе АТЕ «Тестирование» тесты разделяются на проводимые разработчиком и проводимые оценщиком. Требования семейств ATE\_COV «Покрытие» и ATE\_DPT «Глубина» направлены на достижение полноты тестов, проводимых разработчиком. Требования семейства ATE\_COV «Покрытие» определяют строгость, с которой тестируется функциональная спецификация; в семействе ATE\_DPT «Глубина» определяется, требуется ли тестирование по другим проектным описаниям (архитектура безопасности, проект ОО, представление реализации).

Семейство ATE\_FUN «Функциональное тестирование» направлено на выполнение тестов, проводимых разработчиком, и на то, каким образом следует документировать эти тесты. Наконец, требования семейства ATEJND «Независимое тестирование» обращены к тестам, проводимым оценщиком: следует ли оценщику повторно проводить часть тестирований, проведенных разработчиком, и какой объем независимых тестирований ему предстоит провести.

На рисунке 11 показаны семейства этого класса и иерархия компонентов в семействах.



**Рисунок 11 – Декомпозиция класса АТЕ «Тестирование»**

**13.2 Покрытие (ATE\_COV)**

**13.2.1 Цели**

В данном семействе устанавливается, были ли протестированы ФБО на соответствие его их функциональной спецификации. Это достигается путем проверки свидетельств о соответствии, полученных от разработчика.

**13.2.2 Ранжирование компонентов**

Компоненты данного семейства ранжированы на основе их спецификации.

**13.2.3 Замечания по применению**

**13.2.4 ATE\_COV.1 Свидетельство покрытия**

Зависимости: ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации

ATE\_FUN.1 Функциональное тестирование

Цель данного компонента состоит в том, чтобы установить, что некоторые ИФБО были подвергнуты тестированию.

Замечания по применению

В этом компоненте от разработчика требуется продемонстрировать, насколько идентифицированные тесты соответствуют ИФБО из функциональной спецификации. Это может быть достигнуто представлением утверждения о соответствии (возможно, с использованием таблицы).

Элементы действий разработчика

ATE\_COV.1.1D

Разработчик должен представить свидетельство покрытия тестами.

Элементы содержания и представления свидетельств

ATE\_COV.1.1C

Свидетельство покрытия тестами должно демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

Элементы действий оценщика

ATECOV.1.1E

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

**13.2.5 ATE\_COV.2 Анализ покрытия**

Зависимости: ADV\_FSR2 Детализация вопросов безопасности в функциональной спецификации

ATE\_FUN.1 Функциональное тестирование

Цели

Цель этого компонента состоит в том, чтобы установить, что все ИФБО были подвергнуты тестированию.

Замечания по применению

В этом компоненте от разработчика требуется подтвердить, что тестовая документация соотносится с ИФБО из функциональной спецификации. Это может быть достигнуто представлением утверждения о соответствии (возможно, с использованием таблицы), при этом разработчик также должен предоставить анализ покрытия тестами.

Элементы действий разработчика

ATE\_COV.2.1D

Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE\_COV.2.1 С

Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

ATE\_COV.2.2C

Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были подвергнуты тестированию.

Элементы действий оценщика

ATE\_COV.2.1E

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

**13.2.6 ATE\_COV.3 Строгий анализ покрытия**

Зависимости: ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации

ATE\_FUN.1 Функциональное тестирование

Цели

Цель этого компонента состоит в том, чтобы подтвердить, что разработчиком были проведены исчерпывающим образом тесты всех интерфейсов в функциональной спецификации.

Цель компонента состоит в подтверждении того, что все параметры всех ИФБО были подвергнуты тестированию.

Замечания по применению

От разработчика требуется продемонстрировать соответствие тестов из тестовой документации всем ИФБО из функциональной спецификации. Это может быть достигнуто представлением утверждения о соответствии (допускается табличная форма), при этом от разработчика требуется также продемонстрировать, что в тестах были подвергнуты тестированию все параметры всех ИФБО. Это дополнительное требование включает и так называемое ограниченное тестирование (т.е. выполняющее проверку тех ошибок, которые возникают при превышении/нарушении некоторых установленных ограничений) и негативное тестирование (например, когда дается доступ пользователю А и проверяется не только получение им доступа, но и то, не получил ли при этом доступ пользователь В). Такие виды тестирования не являются исчерпывающими, поскольку не ожидается, что будет протестировано каждое возможное значение параметра.

Элементы действий разработчика

ATE\_COV.3.1D

Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

ATE\_COV.3.1C

Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

ATE\_COV.3.2C

Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были полностью протестированы.

Элементы действий оценщика

ATE\_COV.3.1E

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

**13.3 Глубина (ATE\_DPT)**

**13.3.1 Цели**

Компоненты семейства ATE\_DPT имеют отношение к уровню детализации тестирования разработчиком ФБО. Тестирование функциональных возможностей безопасности основано на увеличении глубины представления информации, которая является производной от дополнительных описаний и представлений по проекту (проект ОО, представление реализации, описание архитектуры безопасности).

Целью является противостояние риску пропуска ошибки при разработке 00. Тестирование того, что конкретные внутренние интерфейсы могут предоставлять доверие не только к тому, что ФБО представляют желательный режим безопасности, но также к тому, что этот режим является следствием корректного функционирования внутренней структуры.

**13.3.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе увеличения степени детализации в представлениях ФБО от проекта ОО до представления реализации. Это ранжирование отражает представления ФБО, представленные в классе ADV.

**13.3.3 Замечания по применению**

Проект ОО описывает внутренние компоненты (например, подсистемы) и, по возможности, модули ФБО в совокупности с описанием взаимодействий между этими компонентами и модулями. Свидетельство тестирования данного проекта 00 должно продемонстрировать, что внутренние интерфейсы были реализованы и функционируют согласно описаниям. Это может быть достигнуто либо тестированием через внешние интерфейсы ФБО, либо тестированием подсистем ОО или интерфейсов модулей изолированно, возможно, с использованием средств тестирования. В случаях, когда некоторые аспекты внутреннего интерфейса не могут быть протестированы через внешние интерфейсы, следует либо иметь логическое обоснование того, что эти аспекты необязательно подвергать тестированию, либо провести тестирование этого внутреннего интерфейса напрямую. В последнем случае необходимо, чтобы проект 00 был достаточно детализирован для облегчения тестирования напрямую.

В случаях, когда в описании целостности архитектуры ФБО (в семействе ADV\_ARC «Архитектура безопасности») перечислены конкретные механизмы, выполняемые разработчиком тесты должны демонстрировать, что механизмы реализованы и функционируют в соответствии с описаниями.

Для самого высокого по иерархии компонента этого семейства тестирование проводится не только по проекту 00, но и по представлению реализации.

**13.3.4 ATE\_DPT.1 Тестирование: базовый проект**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_TDS.2 Архитектурный проект

ATE\_FUN.1 Функциональное тестирование

Цели

Описание подсистем ФБО предоставляет описание верхнего уровня для внутреннего содержания ФБО. Тестирование на уровне подсистем ОО обеспечивает доверие к тому, что подсистемы ФБО функционируют и взаимодействуют согласно описаниям в проекте ОО и «Описании архитектуры безопасности».

Элементы действий разработчика

ATE\_DPT.1.1D

Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE\_DPT.1.1C

Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами ФБО из проекта ОО.

ATE\_DPT.1.2C

Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО в проекте ОО были подвергнуты тестированию.

Элементы действий оценщика

ATE\_DPT.1.1E

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

**13.3.5 ATE\_DPT.2 Тестирование: модули, осуществляющие безопасность**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_TDS.3 Базовый модульный проект

ATE\_FUN.1 Функциональное тестирование

Цели

Описания подсистем и модулей ФБО предоставляют описание верхнего уровня внутреннего содержания ФБО и описание интерфейсов, осуществляющих выполнение ФТБ модулей ФБО. Тестирование на этом уровне описания ОО обеспечивает доверие к тому, что подсистемы ФБО и осуществляющие выполнение ФТБ модули функционируют и взаимодействуют так, как описано в проекте ОО и в «Описании архитектуры безопасности».

Элементы действий разработчика

ATE\_DPT.2.1D

Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE\_DPT.2.1C

Анализ глубины тестирования должен демонстрировать соответствие между тестами в тестовой документации и подсистемами ФБО, а также осуществляющими выполнение ФТБ модулями из проекта ОО.

ATE\_DPT.2.2C

Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.

ATE\_DPT.2.3C

Анализ глубины тестирования должен демонстрировать, что осуществляющие выполнение ФТБ модули из проекта ОО были подвергнуты тестированию.

Элементы действий оценщика

ATE\_DPT.2.1E

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

**13.3.6 ATE\_DPT.3 Тестирование: модульный проект**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_TDS.4 Полуформальный модульный проект

ATE\_FUN.1 Функциональное тестирование

Цели

Описания подсистем и модулей ФБО предоставляет описание верхнего уровня внутреннего содержания ФБО и описание интерфейсов модулей ФБО. Тестирование на данном уровне описания ОО обеспечивает доверие к тому, что подсистемы и модули ФБО функционируют и взаимодействуют так, как описано в проекте ОО и в «Описании архитектуры безопасности».

Элементы действий разработчика

ATE\_DPT.3.1D

Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE\_DPT.3.1C

Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами, и модулями ФБО из проекта ОО.

ATE\_DPT.3.2C

Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.

ATE\_DPT.3.3C

Анализ глубины тестирования должен демонстрировать, что все модули ФБО из проекта ОО были подвергнуты тестированию.

Элементы действий оценщика

ATE\_DPT.3.1E

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

**13.3.7 ATE\_DPT.4 Тестирование представления реализации**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_TDS.4 Полуформальный модульный проект

ADVJMP.1 Представление реализации ФБО

ATE\_FUN.1 Функциональное тестирование

Цели

Описания подсистем и модулей ФБО предоставляет описание верхнего уровня внутреннего содержания ФБО и описание интерфейсов модулей ФБО. Тестирование на данном уровне описания ОО обеспечивает доверие к тому, что подсистемы и модули ФБО функционируют и взаимодействуют так, как описано в проекте 00 и в «Описании архитектуры безопасности», а также в соответствии с представлением реализации.

Элементы действий разработчика

ATE\_DPT.4.1D

Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE\_DPT.4.1C

Анализ глубины тестирования должен демонстрировать соответствие между тестами из тестовой документации и подсистемами и модулями ФБО из проекта ОО.

ATE\_DPT.4.2C

Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.

ATE\_DPT.4.3C

Анализ глубины тестирования должен демонстрировать, что все модули ФБО из проекта ОО были подвергнуты тестированию.

ATE\_DPT.4.4C

Анализ глубины тестирования должен демонстрировать, что ФБО функционирует в соответствии с представлением реализации.

Элементы действий оценщика

ATE\_DPT.4.1E

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

**13.4 Функциональное тестирование (ATE\_FUN)**

**13.4.1 Цели**

Функциональное тестирование, выполняемое разработчиком, предоставляет доверие к тому, что тесты из тестовой документации выполнены и задокументированы правильно. Соответствие тестов описаниям проекта ФБО достигается через выполнение требований семейств ATE\_COV «Покрытие» и ATE\_DPT «Глубина».

Это семейство способствует обеспечению доверия к тому, что вероятность наличия невыявленных недостатков относительно мала.

Семейства ATE\_COV «Покрытие», ATE\_DPT «Глубина» и ATE\_FUN «Функциональное тестирование» используют совместно для определения свидетельств тестирования, которые должны быть поставлены разработчиком. Независимое функциональное тестирование, выполняемое оценщиком, рассматривается в ATEJND «Независимое тестирование».

**13.4.2 Ранжирование компонентов**

Это семейство содержит два компонента. Иерархичный компонент содержит требование, чтобы

была проанализирована зависимость от порядка выполнения процедур тестирования.

**13.4.3 Замечания по применению**

Ожидается, что процедуры выполнения тестов будут содержать инструкции по использованию тестовых программ и комплектов тестов, включая среду и условия тестирования, параметры и значения тестовых данных. Рекомендуется, чтобы процедуры тестирования показывали, каким образом из исходных данных тестирования выводятся результаты тестирования.

Зависимость от порядка выполнения процедур имеет значение, когда успешное выполнение конкретного теста зависит от существования конкретного состояния. Например, может требоваться, чтобы тест А выполнялся непосредственно перед тестом Б, так как состояние, являющееся результатом успешного выполнения теста А, является предпосылкой для успешного выполнения теста Б. Таким образом, неудачное проведение теста Б может быть связано с проблемой зависимости от порядка выполнения. В приведенном примере тест Б может завершиться неудачно, потому что тест В (а не А) был выполнен непосредственно перед ним, или же неудачное проведение теста Б может быть связано с неудачным проведением теста А.

**13.4.4 ATE\_FUN.1 Функциональное тестирование**

Зависимости: ATE\_C0V.1 Свидетельство покрытия

Цели

Цель разработчика состоит в том, чтобы продемонстрировать, что тесты из тестовой документации выполнены и задокументированы правильно.

Элементы действий разработчика

ATE\_FUN.1.1D

Разработчик должен протестировать ФБО и задокументировать результаты.

ATE\_FUN.1.2D

Разработчик должен представить тестовую документацию.

Элементы содержания и представления свидетельств

ATE\_FUN.1.1C

Тестовая документация должна состоять из планов тестирования, а также ожидаемых и фактических результатов тестирования.

ATE\_FUN.1.2C

В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

ATE\_FUN.1.3C

Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.

ATE\_FUN.1.4C

Фактические результаты тестирования должны соответствовать ожидаемым.

Элементы действий оценщика

ATE\_FUN.1.1E

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

**13.4.5 ATE\_FUN.2 Упорядоченное функциональное тестирование**

Зависимости ATE\_COV.1 Свидетельство покрытия

Цели

Цель разработчика состоит в том, чтобы продемонстрировать, что тесты из тестовой документации выполнены и задокументированы правильно и, чтобы обеспечить упорядоченную структуру тестирования, которая позволяет избежать неоднократно повторяющихся разногласий о правильности протестированных интерфейсов.

Замечания по применению

Хотя процедуры тестирования могут устанавливать необходимые начальные условия тестирования в терминах упорядочения тестов, они могут и не содержать какого-либо обоснования этого упорядочения. Анализ упорядочения тестов — важный фактор в определении адекватности тестирования, так как имеется возможность сокрытия ошибок вследствие определенного порядка выполнения тестов.

Элементы действий разработчика

ATE\_FUN.2.1D

Разработчик должен протестировать ФБО и задокументировать результаты.

ATE\_FUN.2.2D

Разработчик должен представить тестовую документацию.

Элементы содержания и представления свидетельств

ATE\_FUN.2.1C

Тестовая документация должна состоять из планов тестирования, а также ожидаемых и фактических результатов тестирования.

ATE\_FUN.2.2C

В планах тестирования должны быть идентифицированы тесты, которые необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

ATE\_FUN.2.3C

Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.

ATE\_FUN.2.4C

Фактические результаты тестирования должны соответствовать ожидаемым.

ATE\_FUN.2.5C

Тестовая документация должна содержать анализ зависимостей от порядка выполнения процедур тестирования.

Элементы действий оценщика

ATE\_FUN.2.1E

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

**13.5 Независимое тестирование (ATE\_IND)**

**13.5.1 Цели**

Цели данного семейства основываются на доверии, приобретенном в рамках семейств ATE\_FUN, ATE\_COV и ATE\_DPT путем проверки выполняемых разработчиком тестов и выполнения оценщиком дополнительных тестов.

**13.5.2 Ранжирование компонентов**

Ранжирование основано на объеме тестовой документации разработчика и поддержки тестирования, а также на объеме тестирования, проведенного оценщиком.

**13.5.3 Замечания по применению**

Это семейство имеет отношение к степени выполнения независимого функционального тестирования ФБО. Независимое функциональное тестирование может принимать форму повторения выполненных разработчиком функциональных тестов (полного или частичного) или увеличения области покрытия или глубины тестов разработчика. Эти действия дополняют друг друга, и для каждого ОО следует планировать приемлемое их сочетание с учетом доступности и области покрытия результатов тестов, а также функциональной сложности ФБО.

Повторение выборки тестов, выполненных разработчиком, предназначено для обеспечения подтверждения, что разработчик выполнил запланированную программу тестирования ФБО и правильно зафиксировал результаты. На объем выборки будут влиять детализация и качество результатов функционального тестирования разработчиком. Оценщику нужно также рассмотреть возможности по разработке дополнительных тестов и относительную пользу, которая может быть получена по этим двум направлениям. 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 этого семейства следует использовать с осторожностью. При формировании выборки рассматривается весь диапазон доступных результатов тестирования, включая те, которые предоставлены для обеспечения выполнения требований семейств ATE\_COV «Покрытие» и АТЕ\_DРТ «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 свое собственное тестирование.

Пригодность ОО для тестирования основана на возможности доступа к ОО и поддерживающей документации и информации, необходимой для выполнения тестов (включая любое программное обеспечение или инструментальные средства для тестирования). Необходимость в такой поддержке отражается 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.

Термин «интерфейсы» относится к интерфейсам, описанным в функциональной спецификации и проекте ОО; параметры, прошедшие испытания, идентифицируются в представлении реализации.

Точный набор интерфейсов, которые должны использоваться, выбирается в компонентах ATE\_COV «Покрытие» и ATE\_DPT «Глубина».

Ссылки на подмножество интерфейсов предназначены для того, чтобы позволить оценщику проектировать приемлемый комплект тестов, который согласуется с целями проводимой оценки.

**13.5.4 ATE\_IND.1 Независимое тестирование на соответствие**

Зависимости: ADV\_FSP.1 Базовая функциональная спецификация

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

Целью данного компонента является демонстрация того, что ОО функционирует в соответствии с представлениями по проекту и документацией руководств.

Замечания по применению

Этот компонент не ориентирован на использование результатов тестирования разработчиком. Он применим, когда такие результаты недоступны, а также в случае, когда тестирование, выполненное разработником, принимается без подтверждения. От оценщика требуется разработать и выполнить тесты с целью подтверждения того, что ОО функционирует в соответствии с представлениями по проекту, включая функциональную спецификацию, но не ограничиваясь только ею. 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 сбалансировано с другими действиями по оценке.

Элементы действий разработчика

ATE\_IND.1.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE\_IND.1.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE\_IND.1.1E

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

ATE\_IND.1.2E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ФБО функционируют в соответствии со спецификациями.

**13.5.5 ATE\_IND.2 Выборочное независимое тестирование**

Зависимости: ADV\_FSP.2 Детализация вопросов безопасности в функциональной

спецификации

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

ATE\_COV.1 Свидетельство покрытия

ATE\_FUN.1 Функциональное тестирование

Цели

Целью данного компонента является демонстрация того, что ОО функционирует в соответствии с представлениями проекта ОО и документацией руководств. Выполняемое оценщиком тестирование подтверждает, что разработчик выполнил некоторые тесты некоторых интерфейсов из функциональной спецификации.

Замечания по применению

Разработчику следует предоставить оценщику материалы, необходимые для эффективного воспроизведения тестов, выполненных разработчиком. Сюда могут быть включены такие материалы, как машиночитаемая тестовая документация, тестовые программы и т.д.

Этот компонент содержит требование, чтобы оценщику были доступны результаты тестирования разработчиком для дополнения программы тестирования. Оценщик повторит выборку тестов, выполненных разработчиком, чтобы получить уверенность в полученных результатах. Получив такую уверенность, оценщик на основе выполненного разработчиком тестирования проведет дополнительные тесты функционирования ОО способом, отличающимся от примененного разработчиком. Основываясь на подтверждении достоверности результатов тестов, выполненных разработчиком, оценщик способен получить уверенность в том, что ОО функционирует правильно, причем в более широком диапазоне условий, чем это было бы возможно усилиями одного разработчика, ограниченного уровнем имеющихся у него ресурсов. Убедившись в том, что разработчик протестировал ОО, оценщик будет также иметь больше свободы для фокусирования тестирования на тех направлениях, где экспертиза документации или имеющиеся у специалиста знания вызвали определенные сомнения.

Элементы действий разработчика

ATE\_IND.2.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE\_IND.2.1C

ОО должен быть пригоден для тестирования.

ATE\_IND.2.2C

Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

Элементы действий оценщика

ATE\_IND.2.1E

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

ATE\_IND.2.2E

Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

ATE\_IND.2.3E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ФБО функционируют в соответствии со спецификациями.

**13.5.6 ATE\_IND.3 Полное независимое тестирование**

Зависимости: ADV\_FSP.4 Полная функциональная спецификация

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

ATE\_COV.1 Свидетельство покрытия

ATE\_FUN.1 Функциональное тестирование

Цели

Целью данного компонента является демонстрация того, что ОО функционирует в соответствии с представлениями проекта ОО и документацией руководств. Выполняемое оценщиком тестирование включает в себя повторное выполнение всех тестов, выполненных разработчиком.

Замечания по применению

Разработчику следует предоставить оценщику материалы, необходимые для эффективного воспроизведения тестов, выполненных разработчиком. Сюда могут быть включены такие материалы, как машиночитаемая тестовая документация, тестовые программы и т.д.

В этом компоненте требуется, чтобы оценщик повторил все выполненные разработчиком тесты как часть программы тестирования. Как и в предыдущем компоненте, оценщик проведет дополнительные тесты, направленные на проверку функционирования ОО способом, отличным от использованного разработчиком. В случае, если выполненное разработчиком тестирование было исчерпывающим, для этого может оставаться лишь небольшая возможность.

Элементы действий разработчика

ATE\_IND.3.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE\_IND.3.1C

ОО должен быть пригоден для тестирования.

ATE\_IND.3.2C

Разработчик должен представить набор ресурсов, эквивалентных использованным им при функциональном тестировании ФБО.

Элементы действий оценщика

ATE\_IND.3.1E

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

ATE\_IND.3.2E

Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что все ФБО функционируют в соответствии со спецификациями.

ATE\_IND.3.3E

Оценщик должен выполнить все тесты из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.

**13.6 Комплексное функциональное тестирование (ATE\_COMP)**

**13.6.1 Цели**

Целью этого семейства является определение того, обладает ли композитный продукт в целом свойствами, необходимыми для удовлетворения функциональных требований его композитного продукта ST.

**13.6.2 Ранжирование компонентов**

Это семейство содержит только один компонент.

**13.6.3 Замечания по применению**

Составной продукт можно протестировать путем тестирования его компонентов по отдельности и тестирования интегрированного продукта. Раздельное тестирование означает, что его базовый компонент и зависимый компонент тестируются независимо друг от друга. В рамках его завершенной оценки могло быть проведено множество испытаний базового компонента. Зависимый компонент может быть протестирован на симуляторе или эмуляторе, представляющем собой виртуальную машину.

Интеграционное тестирование означает, что составной продукт тестируется как есть: зависимый компонент работает вместе со связанным базовым компонентом.

Некоторое тестирование функциональности зависимого компонента может выполняться только на эмуляторах перед его встраиванием/интеграцией в базовый компонент, поскольку эффективность этого тестирования может быть не видна при использовании интерфейсов составного продукта. Тем не менее функциональное тестирование составного изделия должно проводиться и на образцах составного изделия согласно описанию функций безопасности составного изделия и с использованием стандартного подхода, как того требует соответствующий класс обеспечения ATE. Никаких дополнительных действий со стороны разработчика здесь не требуется.

Поскольку объем, охват и глубина функциональных тестов базового компонента уже подтверждены оценкой базового компонента, нет необходимости повторно выполнять эти задачи при комплексной оценке. Обратите внимание, что ETR для комплексной оценки не предоставляет никакой информации о функциональном тестировании базового компонента.

Поведение реализации некоторых SFR может зависеть от свойств базового компонента, а также от зависимого компонента (например, правильность мер составного продукта по противостоянию атакам по побочным каналам или правильность реализации защиты от несанкционированного доступа от физических атак). . В таком случае реализация SFR должна быть протестирована на конечном составном продукте, а не на симуляторе или эмуляторе.

Это семейство ориентировано исключительно на тестирование составного продукта в целом и представляет собой лишь частичные усилия в рамках общего подхода к тестированию, охватываемого классом доверия ATE. Эти интеграционные тесты должны быть определены и выполнены, при этом должен быть применен подход стандартных семейств гарантий класса ATE.

Спонсор оценки составного продукта должен обеспечить, чтобы оценщику составного продукта было доступно следующее:

— образцы композитной продукции, пригодные для испытаний.

**13.6.4 ATE\_COMP.1 Функциональное тестирование составного продукта**

Зависимости: Зависимости отсутствуют

Элементы действий разработчика

ATE\_COMP.1.1D

Разработчик должен предоставить набор тестов в соответствии с выбранным пакетом гарантий.

ATE\_COMP.1.2D

Разработчик предоставляет композитное изделие на испытания.

Элементы контента и презентации

ATE\_COMP.1.1C

Содержание и представление спецификации и документации интеграционных тестов должны соответствовать стандартным10) требованиям семейств гарантий ATE\_FUN и ATE\_COV.

ATE\_COMP.1.2C

Предоставленный композитный продукт должен быть пригоден для испытаний.

Элементы действий оценщика

ATE\_COMP.1.1E

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

## **14 Класс AVA: Оценка уязвимостей**

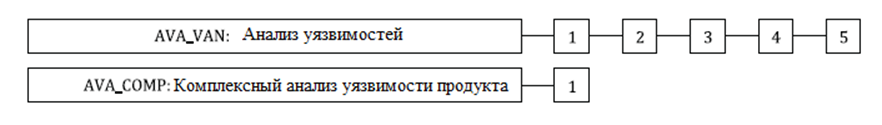
**14.1 Общие положения**

Класс AVA «Оценка уязвимостей» учитывает возможность наличия пригодных для использования уязвимостей, вносимых при разработке или при эксплуатации ОО.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10) в соответствие с ISO/IEC 18045.

На рисунке 12 показаны семейства этого класса и иерархия компонентов в семействах.



**Рисунок 12 – Декомпозиция класса AVA «Оценка уязвимостей»**

**14.2 Замечания по применению**

В общем случае действия по оценке уязвимостей охватывают различные уязвимости, возникающие при разработке и эксплуатации ОО. Уязвимости, возникающие при разработке, связаны с некоторыми свойствами ОО, внесенными в процессе разработки, например, с возможностью преодоления собственной защиты ФБО путем вмешательства, прямой атаки или мониторинга ФБО, преодоления разделения доменов ФБО путем мониторинга или прямой атаки на ФБО или нарушения защиты от обхода ФБО путем обхода ФБО. Уязвимости, возникающие при эксплуатации ОО, связаны с недостатками в нетехнических мерах защиты от нарушения ФТБ ОО, например, с неправильным использованием или с некорректной конфигурацией. Исследование неправильного использования позволяет установить, может ли ОО быть сконфигурирован или использован небезопасным образом так, чтобы администратор или пользователь ОО обоснованно считал бы его защищенным.

Оценка уязвимостей, возникающих при разработке, охвачена семейством доверия AVA\_VAN. В основном все уязвимости, возникающие при разработке, могут быть рассмотрены в контексте AVA\_VAN, исходя из того, что данное семейство допускает применение широкого спектра методик оценки и не является специфичным только для каких-то конкретных типов сценариев атак. Эти обобщенные методики оценки содержат, помимо прочего, также и конкретные методики для тех ФБО, где следует рассмотреть возможность использования скрытых каналов (оценка пропускной способности канала может проводиться с использованием неформальных технических показателей, а также фактических результатов выполнения тестов) или для тех, которые можно преодолеть с использованием ресурсов, достаточных для прямой атаки (основная техническая концепция таких ФБО основывается на вероятностных и перестановочных механизмах; для этих функций квалификация режима безопасности и усилий, требуемых для их преодоления, может быть проведена с использованием количественного или статистического анализа.

Если в ЗБ определены цели безопасности, направленные либо на предотвращение наблюдения одним пользователем ОО за действиями другого, либо на обеспечение того, чтобы невозможно было использовать информационные потоки для распространения неразрешенных информационных сигналов, то в процессе анализа уязвимостей следует проводить анализ скрытых каналов. Это обычно сопровождается включением в ЗБ компонентов из семейства FPR\_UNO «Скрытность» ISO/IEC 15408-2 и отражением в ЗБ политик многоуровневого управления доступом, специфицированных в требованиях семейств «Политика управления доступом» (FDP\_ACC) и/или «Политика управления информационными потоками» (FDP\_IFC).

**14.3 Анализ уязвимостей (AVA\_VAN)**

**14.3.1 Цели**

Анализ уязвимостей представляет собой оценку с целью сделать заключение, могут ли потенциальные уязвимости, идентифицированные в процессе оценки разработки и ожидаемого функционирования ОО или другими методами (например, на основе выдвижения гипотез о недостатках, количественного или статистического анализа режима функционирования соответствующих механизмов безопасности), позволить нарушителям нарушить ФТБ.

При анализе уязвимостей рассматриваются угрозы того, что нарушитель будет способен обнаружить недостатки, которые позволят осуществить несанкционированный доступ к данным и функциональным возможностям, препятствовать выполнению ФБО или вносить изменения в ФБО, а также ограничивать санкционированные возможности других пользователей.

**14.3.2 Ранжирование компонентов**

Компоненты ранжированы на основе повышения оценщиком строгости анализа уязвимостей и повышения уровня потенциала нападения, требующегося нарушителю для идентификации и использования потенциальных уязвимостей.

**14.3.3 AVA\_VAN.1 Обзор уязвимостей**

Зависимости: ADV\_FSP.1 Базовая функциональная спецификация

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

С целью выявления потенциальных уязвимостей, которые могут быть легко обнаружены нарушителем, оценщиком проводится изучение общедоступной информации об уязвимостях.

Оценщик проводит тестирование проникновения с целью подтверждения того, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения — Базовый.

Элементы действий разработчика

AVA\_VAN.1.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA\_VAN.1.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA\_VAN.1.1E

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

AVA\_VAN.1.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.1.3E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Базовым потенциалом нападения.

**14.3.4 AVA\_VAN.2 Анализ уязвимостей**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_FSR1 Базовая функциональная спецификация

ADV\_TDS.1 Базовый проект

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

Оценщиком проводится анализ уязвимостей с целью установить наличие потенциальных уязвимостей.

Оценщик проводит тестирование проникновения с целью подтверждения того, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения — Базовый.

Элементы действий разработчика

AVA\_VAN.2.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA\_VAN.2.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA\_VAN.2.1E

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

AVA\_VAN.2.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.2.3E

Оценщик должен провести независимый анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО и описания архитектуры безопасности, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.2.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Базовым потенциалом нападения.

**14.3.5 AVA\_VAN.3 Фокусированный анализ уязвимостей**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_FSP.2 Детализация вопросов безопасности в функциональной спецификации

ADV\_TDS.3 Базовый модульный проект

ADV\_IMR1 Представление реализации ФБО

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

Оценщиком проводится анализ уязвимостей с целью установить наличие потенциальных уязвимостей.

Оценщик проводит тестирование проникновения с целью удостовериться в том, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения — Усиленный базовый.

Элементы действий разработчика

AVA\_VAN.3.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA\_VAN.3.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA\_VAN.3.1E

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

AVA\_VAN.3.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.3.3E

Оценщик должен провести независимый анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.3.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Усиленным базовым потенциалом нападения.

**14.3.6 AVA\_VAN.4 Методический анализ уязвимостей**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_FSP.2 Детализация вопросов безопасности в функциональной

спецификации

ADV\_TDS.3 Базовый модульный проект

ADVJMP1 Представление реализации ФБО

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

Оценщиком проводится анализ уязвимостей с целью установить наличие потенциальных уязвимостей.

Оценщик проводит тестирование проникновения с целью удостовериться в том, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения — Умеренный.

Элементы действий разработчика

AVA\_VAN.4.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств 15.2.6.3.1 AVA\_VAN.4.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA\_VAN.4.1E

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

AVA\_VAN.4.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.4.3E

Оценщик должен провести независимый методический анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.4.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Умеренным потенциалом нападения.

**14.3.7 AVA\_VAN.5 Усиленный методический анализ**

Зависимости: ADV\_ARC.1 Описание архитектуры безопасности

ADV\_FSR2 Детализация вопросов безопасности в функциональной

спецификации

ADV\_TDS.3 Базовый модульный проект

ADV\_IMR1 Представление реализации ФБО

AGD\_OPE.1 Руководство пользователя по эксплуатации

AGD\_PRE.1 Подготовительные процедуры

Цели

Оценщиком проводится анализ уязвимостей с целью установить наличие потенциальных уязвимостей.

Оценщик проводит тестирование проникновения с целью удостовериться в том, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения — Высокий.

Элементы действий разработчика

AVA\_VAN.5.1D

Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA\_VAN.5.1C

ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA\_VAN.5.1E

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

AVA\_VAN.5.2E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.5.3E

Оценщик должен провести независимый методический анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA\_VAN.5.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим Высоким потенциалом нападения.

**14.4 Комплексная оценка уязвимостей (AVA\_COMP)**

**14.4.1 Цели**

Целью этого семейства является определение возможности использования недостатков или слабых мест составного продукта в целом в предполагаемой среде.

**14.4.2 Ранжирование компонентов**

Это семейство содержит только один компонент.

**14.4.3 Замечания по применению**

Это семейство ориентировано исключительно на оценку уязвимости составного продукта в целом и представляет собой лишь частичные усилия в рамках общего подхода, охватываемого стандартным11) семейством гарантий класса AVA: AVA\_VAN.

Оценщик составного продукта должен выполнить анализ уязвимостей составного продукта, используя, среди прочего, результаты оценки базового компонента. Этот анализ уязвимостей должен быть подтвержден тестированием на проникновение.

Оценщик составного продукта должен проверить, что защита конфиденциальности зависимого компонента, встроенного в базовый компонент или установленного на нем, соответствует уровню конфиденциальности, заявленному разработчиком зависимого компонента для ALC\_DVS.

В особых случаях анализ уязвимостей и определение атак могут быть трудными, требовать значительного времени и обширного предварительного тестирования, если доступна только документация. Базовый компонент также может использоваться способом, который не был предусмотрен разработчиком базового компонента и оценщиком базового компонента, или разработчик зависимого компонента мог не следовать условиям, предусмотренным для базового компонента. В таких случаях существуют различные возможности сократить составной анализ уязвимостей продукта: оценщик составного продукта может проконсультироваться с оценщиком базового компонента и воспользоваться его опытом, полученным в ходе оценки базового компонента. Альтернативно, подход, направленный на разделение уязвимостей зависимого компонента и базового компонента путем использования конкретных тестовых образцов базового компонента, на которые оценщик составного продукта может загружать тестируемые зависимые компоненты по своему усмотрению. Цель настоящего документа состоит в том, чтобы использовать компоненты, зависящие от тестирования, без контрмер и без деактивации каких-либо контрмер, присущих базовому компоненту.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11) в соответствие с ISO/IEC 18045.

Результаты оценки уязвимости базового компонента составного продукта, представленные в ETR для составной оценки, могут быть повторно использованы при следующих условиях: они актуальны и все составные действия на корректность – ASE\_COMP.1, ALC\_COMP.1, ADV\_COMP.1 и ATE\_COMP.1 – завершаются вердиктом PASS.

За счет объединения базового компонента и зависимого компонента возникает новое качество, которое может вызвать дополнительные уязвимости базового компонента, которые могут не быть упомянуты в ETR для составной оценки. В этих обстоятельствах орган по оценке составного продукта может потребовать повторной оценки или повторной оценки базового компонента с упором на новые уязвимости.

Спонсор оценки составного продукта должен обеспечить, чтобы оценщику составного продукта было предоставлено следующее:

- руководство пользователя, связанное с базовыми компонентами,

- ETR, связанный с базовым компонентом, для комплексной оценки, подготовленный оценщиком базового компонента,

- отчет органа по оценке базовых компонентов.

**14.4.4 AVA\_COMP.1 Комплексная оценка уязвимости продукта**

Зависимости: Зависимости отсутствуют

Элементы действий разработчика

AVA\_COMP.1.1D

Разработчик должен предоставить составной продукт для тестирования на проникновение.

Элементы контента и презентации

AVA\_COMP.1.1C

Предоставленный композитный продукт должен быть пригоден для испытаний в целом.

Элементы действий оценщика

AVA\_COMP.1.1Е

Оценщик должен провести тестирование на проникновение составного продукта в целом, основываясь на собственном анализе уязвимостей, проведенном оценщиком, чтобы гарантировать, что уязвимости, имеющие отношение к Цели безопасности составного продукта, не могут быть использованы.

## **15 Класс АСО: Композиция**

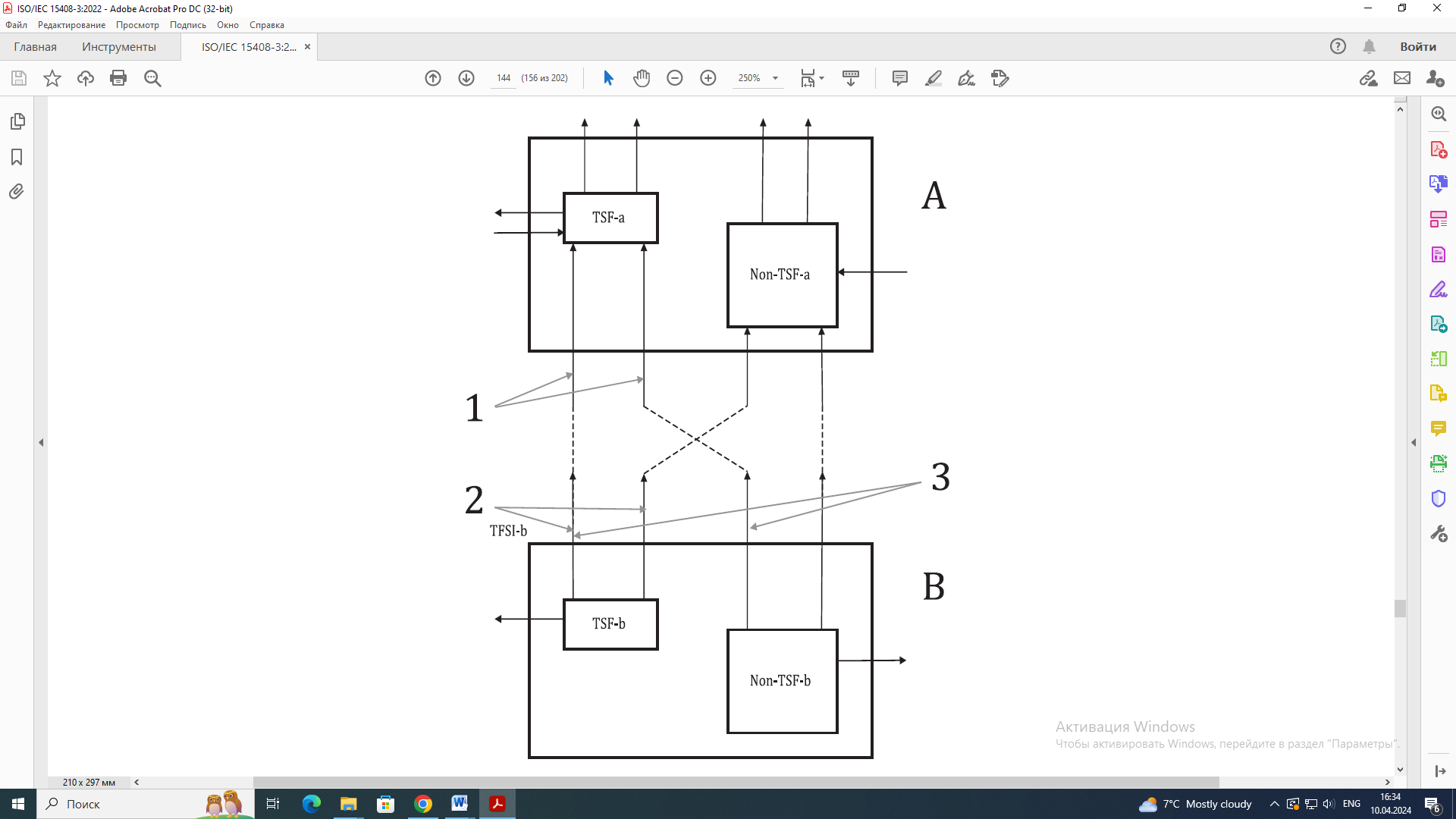
**15.1 Общие положения**

Класс АСО: «Композиция» включает пять семейств. Эти семейства определяют требования доверия, разработанные для обеспечения уверенности, что составной ОО будет функционировать в безопасном режиме, полагаясь на функциональные возможности безопасности, предоставляемые ранее оцененными программными, программно-аппаратными или аппаратными компонентами.

Композиция предполагает, что берутся две или более сущности ИТ, успешно прошедшие оценку на соответствие пакетам требований доверия из ISO/IEC 15408 (являющиеся базовым компонентом и зависимыми компонентами, см. приложение В) и объединяются для применения без дальнейшей разработки какой-либо сущности ИТ. Разработка дополнительных сущностей IT (сущностей, которые до этого не являлись предметом оценки компонентов) не предусматривается. Составной ОО образует новый продукт, который может быть установлен и интегрирован в любой конкретный образец среды, который удовлетворяет целям для среды.

Данный подход не предоставляет альтернативного подхода к оценке компонентов. Композиция в рамках АСО предоставляет интегратору составного ОО метод, который может быть использован как альтернатива другим уровням доверия, определенным в ISO/IEC 15408, с целью получения уверенности в ОО, который является композицией двух или более успешно оцененных компонентов без необходимости повторной оценки составных ФБО (интегратор составного ОО считается «разработчиком» в рамках класса АСО, при наличии же ссылок на разработчика базового или зависимых компонентов упоминается, какой именно разработчик имеется в виду).

Составные пакеты доверия являются шкалой доверия для составных ОО. Данная шкала доверия требуется в дополнение к ОУД, чтобы объединить компоненты, прошедшие оценку по ОУД, и получить итоговый уровень доверия ОУД; все ТДБ в ОУД должны быть применены к составному ОО. Хотя повторное использование результатов оценки ОО-компонентов может быть реализовано, часто есть дополнительные аспекты компонентов, которые должны быть рассмотрены в составном ОО, и которые описаны в приложении В.З. Вследствие того, что в оценку составного ОО вовлечены разные стороны, в общем случае не представляется возможным получить все необходимые свидетельства, касающиеся всех этих дополнительных аспектов компонентов для применения соответствующего ОУД. Поэтому для решения проблем объединения оцененных компонентов и получения значимого результата были определены СоПД. Этот вопрос более детально рассматривается в приложении В.



**Условные обозначения**

А зависимый компонент-a

В базовый компонент-b

1 ACO\_REL (компонент-а)

2 ADV\_FSP (компонент-b)

3 ACO\_DEV (компонент-b)

**Рисунок 13 – Взаимосвязь между семействами АСО и взаимодействиями между компонентами**

В составном ОО, как правило, имеет место ситуация, когда один компонент полагается на сервисы (услуги), предоставляемые другим компонентом. Компонент, которому требуются сервисы, определяется как зависимый компонент, а компонент, предоставляющий сервисы, определяется как базовый компонент. Эти взаимодействия и их особенности рассмотрены далее в приложении В. Предполагается ситуация, когда разработчик зависимого компонента поддерживает оценку составного ОО в той или иной степени (как разработчик, заявитель или лицо, оказывающее содействие и предоставляющее необходимые свидетельства оценки, связанные с оценкой зависимого компонента). Компоненты АСО, включенные в пакеты доверия СоПД, не следует использовать как усиление для оценки ОО-компонента, т. к. это не предоставит значимого доверия к этому компоненту.

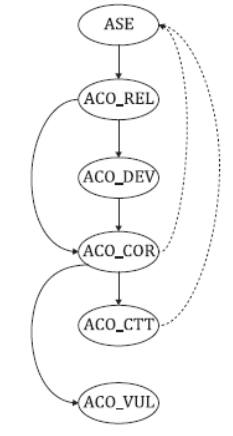
Семейства класса АСО взаимодействуют схожим образом с семействами классов ADV, АТЕ и AVA при оценке составного ОО, и поэтому в некоторых случаях применимы заимствования из спецификации требований этих классов. Однако существует несколько элементов, специфичных для оценки составного ОО. Для установления, как взаимодействуют друг с другом компоненты и для определения любых отклонений от порядка проведения оценки этих компонентов, идентифицируются зависимости, которые имеют компоненты от базового компонента (ACO\_REL). Эта зависимость от базовых компонентов определяется в терминах интерфейсов, через которые зависимые компоненты запрашивают сервисы для поддержки ФТБ зависимых компонентов. Интерфейсы, а на более высоких уровнях режимы поддержки, предоставляемые базовым компонентом в ответ на запросы сервисов, рассматриваются в семействе ACO\_DEV. Семейство ACO\_DEV основывается на семействе ADV\_TDS — так как на простейшем уровне ФБО каждого компонента можно представить в виде подсистемы составного ОО, где дополнительные части каждого компонента рассматриваются как дополнительные подсистемы. Поэтому интерфейсы между компонентами рассматриваются как взаимодействия между подсистемами при оценке составного ОО.

Возможна ситуация, когда описания интерфейсов и режимов поддержки, предоставленные для семейства ACO\_DEV, могут быть неполными. Это выявляется в процессе выполнения оценки по ACO\_COR. Семейство ACO\_COR использует данные на выходе семейств ACO\_REL и ACO\_DEV и определяет, используются ли компоненты в конфигурации, прошедшей оценку, а также идентифицирует, в чем заключается неполнота спецификаций, которые впоследствии рассматриваются как исходные данные для действий семейств «Тестирование составного ОО» (АСО\_СТТ) и «Анализ уязвимостей композиции» (ACO\_VUL).

Тестирование составного ОО проводится, чтобы сделать заключение, что составной ОО демонстрирует ожидаемый режим функционирования, который определен в ФТБ составного ОО, а на более высоких уровнях — демонстрирует совместимость интерфейсов компонентов составного ОО.

Анализ уязвимостей составного ОО обеспечивается использованием данных, полученных в результате анализа уязвимостей при оценке компонентов. При анализе уязвимостей составного ОО рассматриваются любые остаточные уязвимости по результатам оценки компонентов, чтобы сделать заключение, что эти остаточные уязвимости неприменимы для составного ОО. Также выполняется поиск в общедоступных источниках относящейся к компонентам информации для идентификации любых проблем, выявленных в компонентах после завершения соответствующих оценок.

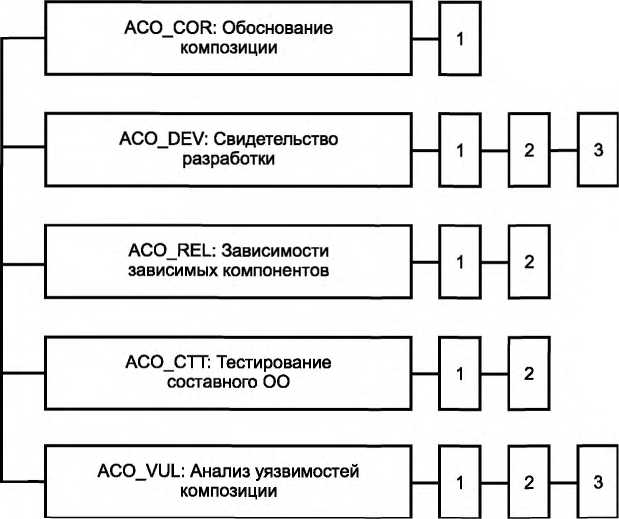
Взаимосвязь семейств АСО отображена на рисунке 14. Сплошными линиями со стрелками показано, когда свидетельства и сведения, полученные для одного семейства, переходят к следующей деятельности. Пунктирными линиями со стрелками показано, когда деятельность имеет обратную связь с ФТБ составного ОО, как описано выше.



**Рисунок 14 – Взаимосвязь между семействами класса АСО**

Дальнейшее рассмотрение определения и взаимосвязей в рамках составного ОО содержится в приложении В.

На рисунке 15 показаны семейства, входящие в состав данного класса, и иерархия компонентов этих семейств.



**Рисунок 15 – Декомпозиция класса АСО «Композиция»**

15.2 Обоснование композиции (ACO\_COR)

15.2.1 Цели

Данное семейство связано с требованиями, необходимыми для демонстрации того, что базовый компонент может предоставить соответствующий уровень доверия для использования в композиции.

15.2.2 Ранжирование компонентов

Данное семейство содержит только один компонент.

15.2.3 ACO\_COR.1 Обоснование композиции

Зависимости: ACO\_DEV.1 Функциональное описание

А1\_С\_СМС.1 Маркировка ОО

ACO\_REL.1 Базовая информация о зависимостях

Элементы действий разработчика

ACO\_COR.1.1D

Разработчик должен предоставить обоснование композиции для базового компонента.

Элементы содержания и представления свидетельств

ACO\_COR.1.1C

Обоснование композиции должно продемонстрировать, что уровень доверия, приобретенный для поддержки функциональных возможностей базового компонента, является таким же высоким или выше, чем уровень доверия к зависимому компоненту, при условии, что конфигурация базового компонента соответствует требованиям для поддержки ФБО зависимого компонента.

Элементы действий оценщика

ACO\_COR.1.1E

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

15.3 Свидетельство разработки (ACO\_DEV)

15.3.1 Цели

Это семейство устанавливает требования к спецификации базового компонента с увеличением уровня детализации. Такая информация требуется для получения уверенности в том, что предоставляются соответствующие функциональные возможности безопасности для поддержки требований зависимого компонента (как идентифицировано в информации о зависимостях).

15.3.2 Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе увеличения степени детализации информации об интерфейсах и способах их реализации.

15.3.3 Замечания по применению

ФБО базового компонента часто определяются без наличия знаний о зависимостях возможных приложений, с которыми он может быть объединен. ФБО этого базового компонента определяются с целью включения всех частей базового компонента, на которые следует полагаться для осуществления ФТБ базового компонента. К этому относятся все части базового компонента, требующиеся для реализации ФТБ базового компонента.

Функциональная спецификация базового компонента описывает ИФБО в терминах интерфейсов, которые базовый компонент предоставляет с целью получения внешней сущностью возможности вызова операций ФБО. Сюда включаются интерфейсы человека-пользователя, допускающие взаимодействие с ФБО в соответствии с ФТБ, а также интерфейсы, позволяющие внешним ИТ-сущностям посылать запросы к ФБО.

Функциональная спецификация содержит только описание того, что предоставляют ФБО через свой интерфейс, а также способы вызова функций ФБО. Следовательно, функциональная спецификация не обязательно содержит полную спецификацию интерфейсов для всех возможных интерфейсов, доступных между внешними сущностями и базовым компонентом. Она также не включает описание того, что ФБО ожидают/требуют от среды функционирования. Описание того, как ФБО зависимых компонентов полагаются на базовый компонент, рассматривается в семействе «Зависимости зависимых компонентов» (ACO\_REL), а в свидетельстве информации по разработке предоставляются ответные реакции для специфицированных интерфейсов.

Свидетельство информации по разработке включает спецификацию базового компонента. Оно может быть свидетельством, использовавшимся в процессе оценки базового компонента для удовлетворения требований класса ADV, или может представлять собой другую форму свидетельства, произведенного либо разработчиком базового компонента, либо разработчиком составного ОО. Такая спецификация базового компонента используется в семействе «Свидетельство разработки» (ACO\_DEV) для получения уверенности в том, что для поддержки требований зависимых компонентов предоставлены соответствующие функциональные возможности безопасности. Уровень детализации, требуемый данным свидетельством, повышается для отражения требуемого уровня доверия к составному ОО. Ожидается, что это позволит в общих чертах отразить повышение уверенности, получаемой через применение составных пакетов доверия к компонентам. Оценщик делает заключение, что это описание базового компонента согласуется с информацией о зависимостях, предоставленной для зависимого компонента.

15.3.4 ACO\_DEV.1 Функциональное описание

Зависимости: ACO\_REL.1 Базовая информация о зависимостях

Цели

Требуется описание интерфейсов базового компонента, на которые полагается зависимый компонент. Оно исследуется, чтобы сделать заключение, согласуется ли данное описание с описанием интерфейсов, на которые полагается зависимый компонент, как представлено в информации о зависимостях.

Элементы действий разработчика

ACO\_DEV.1.1D

Разработчик должен предоставить информацию по разработке базового компонента.

Элементы содержания и представления свидетельств

ACO\_DEV.1.1C

Информация по разработке должна описывать назначение каждого интерфейса базового компонента, используемого в составном ОО.

ACO\_DEV.1.2C

Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.

Элементы действий оценщика

ACO\_DEV.1.1E

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

ACO\_DEV.1.2E

Оценщик должен установить, что предоставленное описание интерфейсов согласуется с информацией о зависимостях, предоставленной для зависимого компонента.

15.3.5 ACO\_DEV.2 Базовое свидетельство по проекту

Зависимости: ACO\_REL.1 Базовая информация о зависимостях

Цели

Требуется описание интерфейсов базового компонента, на которые полагается зависимый компонент. Оно исследуется, чтобы сделать заключение, согласуется ли данное описание с описанием интерфейсов, на которые полагается зависимый компонент, как представлено в информации о зависимостях.

Кроме того, описывается режим безопасного функционирования базового компонента, который поддерживает ФБО зависимого компонента.

Элементы действий разработчика

ACO\_DEV.2.1D

Разработчик должен предоставить информацию по разработке для базового компонента.

Элементы содержания и представления свидетельств

ACO\_DEV.2.1C

Информация по разработке должна описывать назначение и метод использования каждого интерфейса базового компонента, используемого в составном ОО.

ACO\_DEV.2.2C

В информации по разработке должно быть представлено описание верхнего уровня для режима функционирования базового компонента, который поддерживает осуществление ФТБ зависимого компонента.

ACO\_DEV.2.3C

Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.

Элементы действий оценщика

ACO\_DEV.2.1E

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

ACO\_DEV.2.2E

Оценщик должен установить, что предоставленное описание интерфейса согласуется с информацией о зависимостях, предоставленной для зависимого компонента.

15.3.6 ACO\_DEV.3 Детализированное свидетельство по проекту

Зависимости: ACO\_REL.2 Информация о зависимостях

Цели

Требуется описание интерфейсов базового компонента, на которые полагается зависимый компонент. Оно исследуется, чтобы сделать заключение, согласуется ли данное описание с описанием интерфейсов, на которые полагается зависимый компонент, как представлено в информации о зависимостях.

Чтобы у оценщика была возможность сделать заключение, является ли интерфейс сформированной частью ФБО базового компонента, предоставляется описание интерфейсов архитектуры базового компонента.

Элементы действий разработчика

ACO\_DEV.3.1D

Разработчик должен предоставить информацию о разработке базового компонента.

Элементы содержания и представления свидетельств

ACO\_DEV.3.1C

Информация по разработке должна описывать назначение и метод использования каждого интерфейса базового компонента, используемого в составном ОО.

ACO\_DEV.3.2C

В информации по разработке должны быть идентифицированы подсистемы базового компонента, которые предоставляют интерфейсы базового компонента, используемого в составном ОО.

ACO\_DEV.3.3C

В информации по разработке должно быть предоставлено описание верхнего уровня для режима функционирования подсистем базового компонента, которые поддерживают выполнение ФТБ зависимого компонента.

ACO\_DEV.3.4C

В информации о разработке должно быть обеспечено прослеживание интерфейсов к подсистемам базового компонента.

ACO\_DEV.3.5C

Информация по разработке должна показывать соответствие между интерфейсами базового и зависимого компонентов, используемыми в составном ОО для поддержки ФБО зависимого компонента.

Элементы действий оценщика

ACO\_DEV.3.1E

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

ACO\_DEV.3.2E

Оценщик должен установить, что предоставленное описание интерфейса согласуется с информацией о зависимостях, предоставленной для зависимого компонента.

**15.4 Зависимости зависимых компонентов (ACO\_REL)**

**15.4.1 Цели**

Цель данного семейства — предоставить свидетельство, которое описывает зависимость зависимого компонента от базового компонента. Эта информация полезна для лиц, ответственных за интеграцию компонентов с другими прошедшими оценку IT-компонентами для формирования составного ОО и для предоставления понимания свойств безопасности полученной композиции.

В данном семействе предоставлено описание интерфейсов между зависимым и базовым компонентами составного ОО, которые могли не подвергаться анализу в процессе оценки отдельных компонентов, поскольку эти интерфейсы не являлись ИФБО отдельных ОО-компонентов.

**15.4.2 Ранжирование компонентов**

Компоненты в данном семействе ранжированы в соответствии с увеличением степени детализации в описании зависимости зависимого компонента от базового компонента.

**15.4.3 Замечания по применению**

В семействе «Зависимости зависимых компонентов» (ACO\_REL) рассматриваются взаимодействия между компонентами, когда зависимый компонент полагается на некоторый сервис (услугу) базового компонента для поддержки выполнения функциональных возможностей безопасности зависимого компонента. Интерфейсы этих сервисов базового компонента могли не рассматриваться в процессе оценки базового компонента, поскольку этот сервис в процессе оценки компонента не рассматривался как имеющий отношение к безопасности либо по причине своей неотъемлемости (например, изменение типа шрифта), либо в силу того, что связанные с этим сервисом ФТБ из ISO/IEC 15408 не указаны в ЗБ базового компонента (например, интерфейс идентификации (логина) в случае отсутствия в ЗБ указанных ФТБ класса FIA «Идентификация и аутентификация» из ISO/IEC 15408-2). Эти интерфейсы базового компонента часто рассматриваются как функциональные интерфейсы при оценке базового компонента и в дополнение к интерфейсам безопасности (ИФБО) рассматриваются в функциональной спецификации.

Таким образом, ИФБО, описанные в функциональной спецификации, включают только вызовы ФБО внешними сущностями и реакции на эти вызовы. Вызовы, производимые ФБО, которые не рассматривались детально в процессе оценки компонентов, описаны в информации о зависимостях, предоставляемой для удовлетворения требований семейства «Зависимости зависимых компонентов» (ACO\_REL).

**15.4.4 ACO\_REL.1 Базовая информация о зависимостях**

Зависимости: отсутствуют.

Элементы действий разработчика

ACO\_REL.1.1D

Разработчик должен предоставить информацию о зависимостях для зависимого компонента.

Элементы содержания и представления свидетельств

ACO\_REL.1.1C

В информации о зависимостях должны быть описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.

ACO\_REL.1.2C

В информации о зависимостях должны быть описаны все взаимодействия, через которые ФБО зависимого компонента запрашивают сервисы базового компонента.

ACO\_REL.1.3C

В информации о зависимостях должно быть описание того, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.

Элементы действий оценщика

ACO\_REL.1.1E

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

**15.4.5 ACO\_REL.2 Информация о зависимостях**

Зависимости: отсутствуют.

Элементы действий разработчика

ACO\_REL.2.1D

Разработчик должен предоставить информацию о зависимостях для зависимого компонента.

Элементы содержания и представления свидетельств

ACO\_REL.2.1C

В информации о зависимостях должны быть описаны функции аппаратного, программного и программно-аппаратного обеспечения базового компонента, на которые полагаются ФБО зависимого компонента.

ACO\_REL.2.2C

В информации о зависимостях должны быть описаны все взаимодействия, через которые ФБО зависимого компонента запрашивают сервисы базового компонента.

ACO\_REL.2.3C

В информации о зависимостях каждое взаимодействие должно быть описано в терминах, используемых для этих интерфейсов и возвращаемых этими интерфейсами значений.

ACO\_REL.2.4C

В информации о зависимостях должно быть описание того, каким образом ФБО зависимого компонента обеспечивают собственную защиту от вмешательства со стороны базового компонента.

Элементы действий оценщика

ACO\_REL.2.1E

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

**15.5 Тестирование составного ОО (АСО\_СТТ)**

**15.5.1 Цели**

В этом семействе предъявляются требования к тому, чтобы было проведено тестирование составного ОО и тестирование базового компонента, который используется в составном ОО.

**15.5.2 Ранжирование компонентов**

Компоненты в этом семействе ранжированы на основе увеличения строгости тестирования интерфейсов и строгости анализа достаточности тестов для демонстрации того, что ФБО функционируют в соответствии с информацией о зависимостях и с ФТБ составного ОО.

**15.5.3 Замечания по применению**

Существуют два отдельных аспекта тестирования, связанных с данным семейством:

a) тестирование интерфейсов между базовым и зависимым компонентом, на которые полагается зависимый компонент с целью осуществления функциональных возможностей безопасности, для демонстрации их совместимости;

b) тестирование составного ОО для демонстрации того, что данный ОО функционирует в соответствии с ФТБ для составного ОО.

Если тестовые конфигурации, использовавшиеся в процессе оценки зависимого компонента, включали использование базового компонента в качестве «платформы», а тестовые испытания при этом в достаточной степени демонстрируют, что ФБО функционируют в соответствующем ФТБ режиме, то разработчику не требуется проводить дальнейшее тестирование функциональных возможностей составного ОО. Однако, если базовый компонент не использовался при тестировании зависимого компонента или в конфигурацию любого из этих компонентов вносились изменения, то разработчику необходимо выполнить тестирование составного ОО. Такое тестирование может иметь форму повторного тестирования разработчиком зависимого компонента, если это позволит адекватно продемонстрировать, что ФБО функционируют в соответствующем ФТБ режиме.

Разработчик предоставляет свидетельство тестирования интерфейсов базового компонента, используемых в композиции (составном ОО). Функционирование ИФБО базового компонента должно было бы тестироваться как часть действий классу «Тестирование» (АТЕ) при оценке базового компонента. Поэтому при условии, что соответствующие интерфейсы были включены в выборку тестов для оценки базового компонента, а в «Обосновании композиции» (ACO\_COR) делается заключение, что базовый компонент функционирует в соответствии с прошедшей оценку конфигурацией базового компонента, причем все функциональные возможности безопасности, требуемые для зависимого компонента, включены в ФБО, элемент действий оценщика АСО\_СТТ.1.1Е может быть удовлетворен через повторное использование вердиктов по классу «Тестирование» (АТЕ) для базового компонента.

В ином случае относящиеся к композиции используемые интерфейсы базового компонента, на которые влияют какие-либо изменения оцененной конфигурации, и любые дополнительные функциональные возможности безопасности должны подвергаться тестированию для того, чтобы удостовериться, что они демонстрируют ожидаемый режим функционирования. Ожидаемый режим функционирования, подлежащий тестированию — это режим функционирования, описанный в информации о зависимостях (ACO\_REL «Свидетельство зависимости зависимых компонентов»).

**15.5.4 АСО\_СТТ.1 Тестирование интерфейсов**

Зависимости: ACO\_REL.1 Базовая информация о зависимостях

ACO\_DEV.1 Функциональное описание

Цели

Цель данного компонента состоит в том, чтобы удостовериться, что каждый интерфейс базового компонента, на который полагается соответствующий зависимый компонент, протестирован.

Элементы действий разработчика

ACO\_CTT.1.1D

Разработчик должен предоставить тестовую документацию для составного 00.

ACO\_CTT.1.2D

Разработчик должен предоставить тестовую документацию для интерфейсов базового компонента.

ACO\_CTT.1.3D

Разработчик должен предоставить для тестирования составной ОО.

ACO\_CTT.1.4D

Разработчик должен предоставить набор ресурсов, эквивалентный использованному разработчиком при функциональном тестировании базового компонента.

Элементы содержания и представления свидетельств

АСО\_СТТ.1.1С

Тестовая документация для составного ОО и интерфейсов базового компонента должна содержать планы тестирования, ожидаемые результаты тестирования и фактические результаты тестирования.

АСО\_СТТ.1.2С

Тестовая документация разработчика по результатам выполнения тестов по отношению к составному ОО должна демонстрировать, что режим функционирования ФБО соответствует спецификации.

АСО\_СТТ.1.3С

Тестовая документация по результатам выполнения разработчиком тестирования интерфейсов базового компонента должна продемонстрировать, что режим функционирования конкретного интерфейса базового компонента, на который полагается зависимый компонент, соответствует спецификации.

АСО\_СТТ.1.4С

Базовый компонент должен быть пригоден для тестирования.

Элементы действий оценщика

АСО\_СТТ.1.1Е

Оценщик должен подтвердить, что предоставленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСО\_СТТ.1.2Е

Оценщик должен провести выбранное подмножество тестов из тестовой документации, чтобы верифицировать результаты тестов разработчика.

АСО\_СТТ.1.3Е

Оценщик должен протестировать подмножество интерфейсов ФБО составного ОО, чтобы подтвердить, что ФБО составного ОО осуществляются согласно спецификации.

**15.5.5 АСО\_СТТ.2 Строгое тестирование интерфейсов**

Зависимости: ACО\_REL.2 Информация о зависимостях

ACO\_DEV.2 Базовое свидетельство по проекту

Цели

Цель данного компонента состоит в том, чтобы удостовериться, что каждый интерфейс базового компонента, на который полагается соответствующий зависимый компонент, протестирован.

Элементы действий разработчика

ACO\_CTT.2.1D

Разработчик должен предоставить тестовую документацию для составного ОО.

ACO\_CTT.2.2D

Разработчик должен предоставить тестовую документацию для интерфейсов базового компонента.

ACO\_CTT.2.3D

Разработчик должен предоставить для тестирования составной ОО.

ACO\_CTT.2.4D

Разработчик должен предоставить набор ресурсов, эквивалентный использованному разработчиком при функциональном тестировании базового компонента.

Элементы содержания и представления свидетельств

АСО\_СТТ.2.1С

Тестовая документация для составного ОО и интерфейсов базового компонента должна состоять из плана тестирования, прогнозируемых результатов и фактических результатов.

АСО\_СТТ.2.2С

Тестовая документация разработчика по результатам выполнения тестов по отношению к составному ОО должна демонстрировать, что режим функционирования ФБО соответствует спецификации и ФБО являются полными.

АСО\_СТТ.2.3С

Тестовая документация по результатам выполнения разработчиком тестирования интерфейсов базового компонента должна продемонстрировать, что режим функционирования конкретного интерфейса базового компонента, на который полагается зависимый компонент, соответствует спецификации и этот интерфейс является полным.

АСО\_СТТ.2.4С

Базовый компонент должен быть пригоден для тестирования.

Элементы действий оценщика

АСО\_СТТ.2.1Е

Оценщик должен подтвердить, что предоставленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АСО\_СТТ.2.2Е

Оценщик должен провести выбранное подмножество тестов из тестовой документации, чтобы проверить результаты тестов разработчика.

АСО\_СТТ.2.3Е

Оценщик должен протестировать подмножество интерфейсов ФБО составного ОО, чтобы подтвердить, что ФБО составного ОО осуществляются согласно спецификации.

**15.6 Анализ уязвимостей композиции (ACO\_VUL)**

**15.6.1 Цели**

Данным семейством требуется проведение анализа информации об уязвимостях, доступной в общедоступных источниках, а также анализа уязвимостей, возникающих в результате композиции (объединения компонентов).

**15.6.2 Ранжирование компонентов**

Компоненты данного семейства ранжированы на основе повышения тщательности анализа информации об уязвимостях в общедоступных источниках, а также тщательности независимого анализа уязвимостей.

**15.6.3 Замечания по применению**

Разработчик должен предоставить детальную информацию о каких-либо остаточных уязвимостях, приведенных в отчете в процессе оценки компонентов. Эта информация может быть получена от разработчиков компонентов или из отчетов об оценке этих компонентов. Полученная информация используется в качестве исходных данных для проведения оценщиком анализа уязвимостей составного ОО в среде функционирования.

Среда функционирования составного ОО исследуется с целью удостовериться в том, что предположения и цели для среды функционирования компонентов (специфицированные в ЗБ каждого компонента) удовлетворяются в составном ОО. Первоначальный анализ согласованности между предположениями и целями в ЗБ ОО-компонентов и в ЗБ составного ОО выполняется при выполнении действий по оценке класса ASE в отношении составного ОО. Однако этот анализ пересматривается с учетом сведений, полученных при выполнении действий семейств ACO\_REL «Зависимости зависимых компонентов», ACO\_DEV «Свидетельство разработки» и ACO\_COR «Обоснование композиции», чтобы удостовериться, что, например, предположения для зависимого компонента, к которым обращается среда функционирования в ЗБ зависимого компонента, не представляются повторно как результат композиции (т.е. что базовый компонент адекватно обращается к предположениям из ЗБ зависимого компонента в составном ОО).

Поиск оценщиком проблем в каждом компоненте позволит идентифицировать потенциальные уязвимости, о которых приводилось в отчете в общедоступных источниках после завершения оценки компонентов. Все потенциальные уязвимости затем становятся предметом тестирования.

Если базовый компонент, используемый в составном ОО, является предметом преемственности действий, связанных с доверием с момента сертификации, то оценщик в процессе действий по анализу уязвимостей составного ОО должен учитывать все изменения в базовом компоненте.

**15.6.4 ACO\_VUL.1 Краткий анализ уязвимостей композиции**

Зависимости: ACO\_DEV.1 Функциональное описание

Элементы действий разработчика

ACO\_VUL.1.1D

Разработчик должен предоставить для тестирования составной ОО.

Элементы содержания и представления свидетельств

ACO\_VUL.1.1C

Составной ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ACO\_VUL.1.1E

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

ACO\_VUL.1.2E

Оценщик должен выполнить анализ, чтобы сделать заключение, что любые остаточные уязвимости, идентифицированные для базового и зависимых компонентов, не могут быть использованы по отношению к составному ОО в его среде функционирования.

ACO\_VUL.1.3E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать возможные уязвимости, возникающие при использовании базового и зависимых компонентов в среде функционирования составного ОО.

ACO\_VUL.1.4E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы продемонстрировать, что составной ОО противостоит атакам нарушителя с Базовым потенциалом нападения.

**15.6.5 ACO\_VUL.2 Анализ уязвимостей композиции**

Зависимости: ACO\_DEV.2 Базовое свидетельство по проекту

Элементы действий разработчика

ACO\_VUL.2.1D

Разработчик должен представить для тестирования составной ОО.

Элементы содержания и представления свидетельств

ACO\_VUL.2.1C

Составной ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ACO\_VUL.2.1E

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

ACO\_VUL.2.2E

Оценщик должен выполнить анализ, чтобы сделать заключение, что любые остаточные уязвимости, идентифицированные для базового и зависимых компонентов, не могут быть использованы по отношению к составному ОО в его среде функционирования.

ACO\_VUL.2.3E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать возможные уязвимости, возникающие при использовании базового и зависимых компонентов в среде функционирования составного ОО.

ACO\_VUL.2.4E

Оценщик должен выполнить независимый анализ уязвимостей составного ОО, используя документацию руководств, информацию о зависимостях и обоснование композиции для идентификации потенциальных уязвимостей составного ОО.

ACO\_VUL.2.5E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы продемонстрировать, что составной ОО противостоит атакам нарушителя с Базовым потенциалом нападения.

**15.6.6 ACO\_VUL.3 Усиленный базовый анализ уязвимостей композиции**

Зависимости: ACO\_DEV.3 Детализированное свидетельство по проекту

Элементы действий разработчика

ACO\_VUL.3.1D

Разработчик должен представить для тестирования составной ОО.

Элементы содержания и представления свидетельств

ACO\_VUL.3.1C

Составной ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ACO\_VUL.3.1E

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

ACO\_VUL.3.2E

Оценщик должен выполнить анализ, чтобы сделать заключение, что любые остаточные уязвимости, идентифицированные для базового и зависимых компонентов, не могут быть использованы по отношению к составному ОО в его среде функционирования составного ОО.

ACO\_VUL.3.3E

Оценщик должен выполнить поиск информации в общедоступных источниках, чтобы идентифицировать возможные уязвимости, возникающие при использовании базового и зависимых компонентов в среде функционирования составного ОО.

ACO\_VUL.3.4E

Оценщик должен выполнить независимый анализ уязвимостей составного ОО, используя документацию руководств, информацию о зависимостях и обоснование композиции для идентификации потенциальных уязвимостей составного ОО.

ACO\_VUL.3.5E

Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы продемонстрировать, что составной ОО противостоит атакам нарушителя с Усиленным базовым потенциалом нападения.

## **Приложение А**

*(информационное)*

**Разработка (ADV)**

**A.1 ADV\_ARC: Дополнительный материал по архитектурам безопасности**

**А.1.1 Общие положения**

Данное приложение содержит вспомогательный материал для дальнейшего объяснения и предоставления дополнительных примеров по темам, поднимаемым в семьях класса ADV: Разработка.

Архитектура безопасности является набором свойств, которые представляют ФБО; эти свойства включают в себя собственную защиту, разделение доменов и невозможность обхода. Наличие этих свойств дает основу для уверенности в том, что ФБО предоставляют сервисы безопасности. Данное приложение содержит дополнительный материал об этих свойствах, а также в нем рассматривается содержание описания архитектуры безопасности.

В остальной части настоящего подраздела вначале объясняются эти свойства, а затем рассматриваются виды информации, необходимые для описания способа реализации ФБО данных свойств.

**А.1.2 Свойства архитектуры безопасности**

Собственная защита относится к способности ФБО противостоять манипуляциям внешних сущностей, которые могут привести к изменениям в ФБО. Без этих свойств выполнение сервисов безопасности для ФБО может стать невозможным.

Зачастую 00 использует сервисы или ресурсы, предоставляемые другими ИТ-сущностями, для выполнения своих функциональных возможностей (например, приложение, которое полагается на лежащую в его основе операционную систему). В этих случаях ФБО не защищают себя полностью, поскольку зависят от других ИТ-сущностей для защиты используемых сервисов.

Разделение доменов является свойством, посредством которого ФБО создает отдельные домены безопасности для каждой недоверенной активной сущности, чтобы совершать действия над ее ресурсами, а затем сохраняет эти домены разделенными друг от друга так, что ни одна сущность не может работать в домене любой другой. Например, ОО, являющийся операционной системой, поддерживает домен (адресное пространство, попроцессные переменные среды) для каждого процесса, связанного с недоверенными сущностями.

Для некоторых ОО таких доменов не существует, потому что все действия недоверенных сущностей находятся под наблюдением ФБО. Межсетевой экран с пакетной фильтрацией является примером такого ОО, где нет доменов недоверенных сущностей; есть только структуры данных, поддерживаемые ФБО. Наличие доменов, таким образом, зависит от 1) типа 00 и 2) ФТБ, предъявляемым к 00. В тех случаях, когда ОО предоставляет домены для недоверенных сущностей, по требованиям данного семейства необходимо, чтобы эти домены были изолированы друг от друга таким образом, чтобы недоверенные сущности в одном домене были ограждены от вмешательства (влияющего без участия ФБО) другого домена недоверенных сущностей.

Невозможность обхода — это свойство, заключающееся в том, что функциональные возможности безопасности ФБО (как специфицировано в ФТБ) всегда активны, и их невозможно обойти применительно к этому конкретному механизму. Например, если управление доступом к файлам определяется как возможность ФБО через ФТБ, то не должно быть никаких интерфейсов, через которые файлы могут быть доступны без вызова механизма контроля доступа ФБО (примером такого недопустимого интерфейса может быть интерфейс, через который возможен прямой доступ к диску в обход файловой системы).

Как и в случае собственной защиты, сама суть некоторых ОО может зависеть от их среды, которая играет роль в невозможности обхода ФБО. Например, ОО, который является приложением безопасности, содержит требование, чтобы это приложение вызывалось базовой операционной системой. Аналогично межсетевой экран зависит от факта отсутствия прямых связей между внутренней и внешней сетями и от того, что весь трафик между ними должен проходить через межсетевой экран.

**А.1.3 Описание архитектуры безопасности**

В «Описании архитектуры безопасности» объясняется, как указанные выше свойства представлены в ФБО.

Оно содержит описание механизмов определения и разделения доменов посредством ФБО; мер защиты ФБО от несанкционированного доступа и модификации со стороны недоверенных процессов; а также описание мер, обеспечивающих надлежащую защиту всех ресурсов под контролем ФБО и выполнение ФБО роли посредника в действиях, связанных с ФТБ. Также в «Описании архитектуры безопасности» объясняется роль среды в любом из этих процессов (например, если процесс корректно вызывается его базовой средой, то как вызываются его функциональные возможности безопасности?).

В «Описании архитектуры безопасности» представляются свойства собственной защиты ФБО, разделения доменов и невозможности обхода в терминах описаний декомпозиции. Уровень такого описания соизмерим с описанием ФБО, требуемым по заявленным семействам ADV\_FSP, ADV\_TDS и ADVJMP. Например, если семейство ADV\_FSP является единственным доступным описанием ФБО, то будет трудно предоставить какой-либо значимый архитектурный проект, поскольку не будут доступны подробности внутреннего содержания ФБО.

Однако если бы был доступен еще и проект ОО, даже на самом базовом уровне (ADV\_TDS.1), то была бы доступна и некоторая информация, касающаяся подсистем, составляющих ФБО, и описание того, как они реализуют собственную защиту, разделение доменов и невозможность обхода. Предположим, например, что все взаимодействия пользователя с ОО ограничены неким процессом, который действует от лица пользователя и перенимает все присущие ему атрибуты безопасности; тогда в проекте архитектуры должна быть описана реализация подобного процесса, то, каким образом функционирование процесса ограничивается ФБО (благодаря чему он не может нарушить ФБО) и как ФБО участвуют во всех действиях этого процесса (тем самым поясняется, почему ФБО нельзя обойти) и т. д.

Если доступный оценщику проект ОО более детализирован (например, описан на уровне модулей) или оценщику предоставлено и представление реализации, то описание архитектурного проекта будет, соответственно, более детализированным. В нем будет объясняться, каким образом пользовательские процессы сообщаются с процессами ФБО, как различные запросы обрабатываются ФБО, какие параметры принимаются, какие программные средства защиты (для предотвращения переполнения буфера, проверки границ параметров, проверки соотношения между временем проверки и временем использования и т.д.) применяются. Аналогично ОО, в ЗБ которого заявлен компонент семейства ADVJMP, будет детализироваться вплоть до аспектов реализации.

Ожидается, что пояснения, представленные в «Описании архитектуры безопасности», предоставят достаточно детализированную информацию для того, чтобы можно было протестировать их точность. Это значит, что простые утверждения (например, «ФБО поддерживают разделение доменов») не дают никакой полезной информации, способной убедить читателя, что ФБО действительно создают домены и проводят их разделение.

А.1.3.1 Разделение доменов

В случаях, когда ОО осуществляет разделение доменов только своими средствами, должно быть простое описание того, каким образом это достигается. В «Описании архитектуры безопасности» будет приводиться пояснение различных видов доменов, которые определены ФБО, как они определены (т. е. то, какие ресурсы выделены для каждого домена), каким образом достигается отсутствие незащищенных ресурсов и как поддерживается разделение доменов, чтобы активные сущности одного домена не могли влиять на ресурсы другого домена.

В случаях, когда ОО зависит от других ИТ-сущностей, участвующих в разделении доменов, распределение ролей должно быть четким. В качестве примера можно рассмотреть случай, когда ОО, являющийся исключительно прикладным программным обеспечением, полагается на базовую операционную систему для правильного утверждения доменов, определенных ОО; если ОО определяет отдельные пространства обработки данных, области памяти и т.д. для каждого домена, то от базовой операционной системы зависит правильность и следование полномочиям при функционировании (например, разрешение на выполнение процесса только в рамках пространства выполнения, которое запрашивается программным обеспечением ОО).

Например, механизмы, которые реализуют разделение доменов (управление памятью, предоставленные аппаратными средствами защищенные режимы обработки данных и т.д.) должны быть идентифицированы и описаны. Или в ФБО могут быть реализованы структуры программной защиты или стандарты кодирования, которые способствуют реализации разделения доменов программного обеспечения, к примеру, путем отделения адресного пространства пользователя от адресного пространства системы.

Желательно, чтобы действия по анализу уязвимостей и тестированию (см. AVA\_VAN) включали попытки обойти установленное разделение доменов ФБО путем мониторинга или прямой атаки на ФБО.

А.1.3.2 Собственная защита ФБО

В случаях, когда ОО осуществляет собственную защиту только своими средствами, должно быть простое описание того, каким образом эта собственная защита достигается. Механизмы, обеспечивающие разделение доменов с целью определения домена ФБО, который защищен от других (пользовательских) доменов, должны быть идентифицированы и описаны.

В случаях, когда ОО зависит от других ИТ-сущностей, участвующих в обеспечении собственной защиты, распределение ролей должно быть четким. Например, ОО, являющийся исключительно прикладным программным обеспечением, полагается на базовую операционную систему для правильного функционирования и чтобы не допускать превышения полномочий; приложение при этом не может защитить себя от вредоносного влияния операционной системы в случае, если она подрывает функционирование приложения (например, путем перезаписи кода исполняемого файла или данных ФБО).

«Описание архитектуры безопасности» также охватывает то, как вводимые пользователем данные обрабатываются ФБО таким образом, чтобы ФБО не могли быть повреждены вводимыми пользователем данными.

Например, ФБО могут реализовать понятие привилегий и защитить себя путем включения привилегированного режима для обработки пользовательских данных. ФБО могут использовать основанный на процессах механизм разделения (например, по уровню или рангу привилегий), чтобы отделить код и данные ФБО от кода и данных пользователя. ФБО может реализовать структуры программной защиты или стандарты кодирования, которые способствуют реализации разделения программного обеспечения, к примеру, путем отделения адресного пространства пользователя от адресного пространства системы.

Для ОО, которые запускаются в режиме минимума функциональных возможностей (например, однопользовательский режим, доступный только для установщиков или администраторов), а затем переводятся в оцененную безопасную конфигурацию (режим, в котором недоверенные пользователи имеют возможность входа в систему с использованием логина и использования сервисов и ресурсов ОО), «Описание архитектуры безопасности» также включает в себя объяснение того, как ФБО защищена от кода инициализации, который не запускается в оцененной конфигурации. Для таких ОО в «Описании архитектуры безопасности» объясняется, что именно позволяет предотвратить в оцененной конфигурации доступ к сервисам, к которым следует предоставлять доступ только во время инициализации (например, прямой доступ к ресурсам). В нем же объясняется, что позволяет предотвратить запуск кода инициализации, когда ОО находится в оцененной конфигурации.

Там также должно быть объяснение того, как доверенный код инициализации будет поддерживать целостность ФБО (и процессов их инициализации). Например, процесс инициализации может выявить какие-либо изменения, которые приведут к тому, что ФБО будут обманным образом выданы за функционирующие в первоначальном безопасном состоянии.

Действия по анализу уязвимостей и тестированию (см. AVA\_VAN) скорее всего будут включать в себя попытки нарушить описанную собственную защиту ФБО путем вмешательства, прямой атаки или мониторинга ФБО.

А.1.3.3 Невозможность обхода ФБО

Свойство невозможности обхода касается интерфейсов, которые позволяют обойти механизмы, осуществляющие безопасность. В большинстве случаев это является последствием реализации, когда если программист пишет интерфейс, который осуществляет доступ к объекту или воздействует на объект, то он несет ответственность за то, что будет использовать интерфейсы, являющиеся частью осуществляющего выполнение ФТБ механизма, а не пытаться обойти их. Таким образом, описанием, относящимся к невозможности обхода, следует охватить две широких области.

К первой относятся интерфейсы, осуществляющие ФТБ. Свойством этих интерфейсов является то, что они не содержат никаких операций или режимов, которые позволяют использовать их для обхода ФБО. Скорее всего, что для вынесения такого заключения могут в значительной степени использоваться свидетельства для ADV\_FSP и ADV\_TDS. Поскольку рассматривается невозможность обхода, то если задокументирована только часть определенных операций, доступных через ИФБО (поскольку они осуществляют ФТБ), а другие операции не документированы, разработчику следует рассмотреть, необходима ли дополнительная информация (как представлено в ADV\_FSP и ADV\_TDS) для вынесения заключения, что поддерживающие ФТБ и не влияющие на ФТБ операции ИФБО не позволяют недоверенным сущностям получить возможность обойти действующую политику безопасности. Если такая информация необходима, она включается в «Описание архитектуры безопасности».

Ко второй области, касающейся невозможности обхода, относятся те интерфейсы, чьи взаимодействия не связаны с осуществлением ФТБ. В зависимости от заявленных компонентов ADV\_FSP и ADV\_TDS, часть информации об этих интерфейсах может содержаться или не содержаться в функциональной спецификации и проектной документации ОО. Информации, представленной для таких интерфейсов (или для группы интерфейсов), следует быть достаточной для того, чтобы читатель мог сделать заключение (на уровне детализации, соизмеримом с остальными свидетельствами, предоставленными в классе ADV: «Разработка»), что эти осуществляющие ФТБ механизмы нельзя обойти.

Свойство невозможности обхода ФБО распространяется на все функциональные возможности безопасности в равной степени. Это значит, что в описании проекта следует охватывать объекты, которые защищаются по ФТБ (например, компоненты FDP\_\*) и функциональные возможности (например, аудит), предоставляемые ФБО. В описании следует также идентифицировать интерфейсы, которые связаны с функциональными возможностями безопасности; для этого может быть использована информация из функциональной спецификации. В этом описании следует также рассмотреть любые структуры проекта, такие как механизмы управления объектами, и способ их использования. Например, если процедуры должны использовать стандартный макрос для создания записи аудита, эта установка является частью проекта, который способствует невозможности обхода механизма аудита. Важно отметить, что невозможность обхода в этом контексте не является попыткой ответить на вопрос «может ли часть реализации ФБО, если она вредоносна, обойти функциональные возможности безопасности», а скорее рассматривается для документирования того, как реализация не обходит функциональные возможности безопасности.

Действия по анализу и тестированию уязвимости (см. AVA\_VAN), скорее всего, будут включать попытки нарушить описанную невозможность обхода путем обхода ФБО.

**А.2 ADV\_FSP: Дополнительный материал по ИФБО**

**А.2.1 Общие положения**

Целью спецификации ИФБО является предоставление необходимой информации для проведения тестирования; не зная возможных средств взаимодействия с ФБО, невозможно адекватно протестировать режим ФБО.

В спецификации ИФБО две части: идентификация и описание. Из-за разнообразия возможных ОО, а также различных ФБО в них, не существует стандартного набора интерфейсов, которые представляют собой ИФБО. В данном приложении представлено руководство по факторам, которые определяют, какие интерфейсы являются ИФБО.

**А.2.2 Часть ОО, не относящаяся к ФБО**

ФБО включают в себя все части ОО, на которые пользователь может положиться, чтобы доверять функциям безопасности.

Другими словами: те части ОО, которые не принадлежат ФБО, могут быть изменены злоумышленником без какого-либо влияния на функциональность безопасности ОО. Если это не так, эти части ОО должны быть включены в ФБО.

Если определены ФБО и реализация ФБО, то становится ясно, существуют ли дополнительные части ОО, которые можно классифицировать как части ОО, не относящиеся к ФБО. Такие части не обязательно должны быть частью ФБО, но они все равно являются частью ОО.

Взаимосвязь между ФБО и частями ОО, не относящимися к ФБО, определяется их определениями и свойствами ARC следующим образом:

— части, не относящиеся к ФБО, не обходят ФБО;

— части ФБО защищаются от несанкционированного доступа.

Подсистема ОО, которая не является частью ФБО, должна удовлетворять следующему условию (описанному в качестве практического правила 12)): Подсистема не должна оказывать какого-либо воздействия на безопасность ОО, даже если она была заменена злоумышленником.

Поэтому между частями, не относящимися к ФБО, и частями ФБО представляется целесообразным какой-то «механизм разделения»13), поскольку такой «механизм разделения» может создать основу для оценки отсутствия воздействия на части ФБО со стороны не-ФБО. Части ФБО. Возможны части ФБО. Такой «механизм разделения» может быть реализован архитектурой безопасности или явно реализованной частью реализации (например, межсетевой экран между ФБО и частями ОО, не относящимися к ФБО). Анализ «механизма разделения» затем является предметом оценки уязвимости, поскольку он должен противостоять атакам злоумышленника соответствующей силы в соответствии с уровнем VAN оценки. Разработчик должен предоставить доказательства необходимости и самозащиты в своем описании архитектуры безопасности и оценщик должен проанализировать это свидетельство в поддействии для ADV\_ARC.1 и оценить эффективность оценки уязвимости. Целью проектной документации ОО является предоставление достаточной информации для определения границы ФБО и описания того, как ФБО реализуют ФТБ. Дальнейшего внимания требует тот факт, что семейство ADV\_TDS требует только идентификации подсистем ОО, не относящихся к ФБО. Для этих подсистем в ADV\_FSP или ADV\_TDS не предусмотрено описание интерфейса. Невмешательство SFR в эти подсистемы предполагается, но не демонстрируется разработчиком и не исследуется подробно оценщиком. Однако с точки зрения проектирования ОО это не так важно, пока существует вышеупомянутый механизм разделения и оценка уязвимости подтверждает, что он достаточно силен. Следовательно, этот «механизм разделения» реализует ФБО или применяет свойства ARC в качестве функции безопасности. Но невозможность обхода также может обеспечиваться «свойствами чистой архитектуры». Части ОО, классифицированные как не-ФБО, не должны предоставлять средства для обхода ФБО (независимо от того, использует ли эти части действительный пользователь или даже злоумышленник). и не должны вносить вклад в ФБО. Важно, чтобы разработчик предоставил четкие доказательства и продемонстрировал, как выполняется это требование. Поэтому разработчик должен продемонстрировать, а оценщик должен проверить, что идентификация ОО подсистем как не ФБО (см. ADV\_TDS.x.1) правильна и, следовательно, подробное описание этих подсистем не требуется. Проверка оценщика должна включать в себя необходимость и самозащиту свойств ARC, описанных в документации ADV\_ARC, предоставленной разработчиком (см. пункты выше).

**А.2.3 Определение ИФБО**

Чтобы идентифицировать интерфейсы ФБО, прежде всего должны быть идентифицированы части ОО, составляющие ФБО. Идентификация на самом деле является частью анализа семейства «Проект ОО» (ADV\_TDS), но также осуществляется

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

12) Это правило справедливо только до некоторой степени, поскольку фактическое требование «Часть, не относящаяся к ФБО, не должна обходить ФБО». не так сильно, как данное эмпирическое правило.

13) «Механизм разделения» здесь является лишь предложением. Разработчик может предоставить доказательства, используя другой вид реализации безопасности, при условии, что выполняется требование, показывающее непереходимость части ОО, относящейся к ФБО, от части ОО, не относящейся к ФБО.

разработчиком и неявно (через идентификацию и описание ИФБО) в случаях, когда семейство «Проект ОО» (ADV\_TDS) не включается в пакет доверия. В этом анализе часть ОО должна считаться входящей в ФБО, если это требуется для удовлетворения ФТБ из ЗБ (в целом или частично). Это включает, например, все в ОО, что способствует инициализации во время выполнения ФБО, к примеру, программное обеспечение, которое запускается до момента, когда ФБО способны обеспечить собственную защиту, так как выполнение ФТБ еще не началось (например, в процессе запуска). Также включаются в ФБО все части ОО, которые вносят вклад в архитектурные принципы собственной защиты ФБО, разделения доменов и невозможности обхода (см. семейство ADV\_ARC «Архитектура безопасности»).

После того, как ФБО были определены, идентифицируются ИФБО. ИФБО включают в себя все возможности пользователей по вызову сервиса ФБО (путем предоставления данных, которые обрабатываются ФБО) и соответствующих реакций на запросы сервисов. Все запросы сервисов и реакции являются способами пересечения границ ФБО. Хотя многие из них являются очевидными, другие могут быть не столь очевидны. Вопрос, который следует задавать при определении ИФБО, имеет следующий вид: «Как может потенциальный нарушитель взаимодействовать с ФБО при попытке компрометировать ФТБ?» Приведенные ниже обсуждения иллюстрируют применение определения ИФБО в различных контекстах.

А.2.3.2 Электрические интерфейсы

В таких 00, как смарт-карты, где нарушитель имеет не только логический, но и полный физический доступ к ОО, граница ФБО является физически очерченной. Следовательно, уязвимые электрические интерфейсы считаются ИФБО, поскольку манипуляции с ними могут повлиять на режим ФБО. Таким образом, все эти интерфейсы (электрические контакты) должны быть описаны: например, различные применимые напряжения и т.д.

А.2.3.3 Стек сетевых протоколов

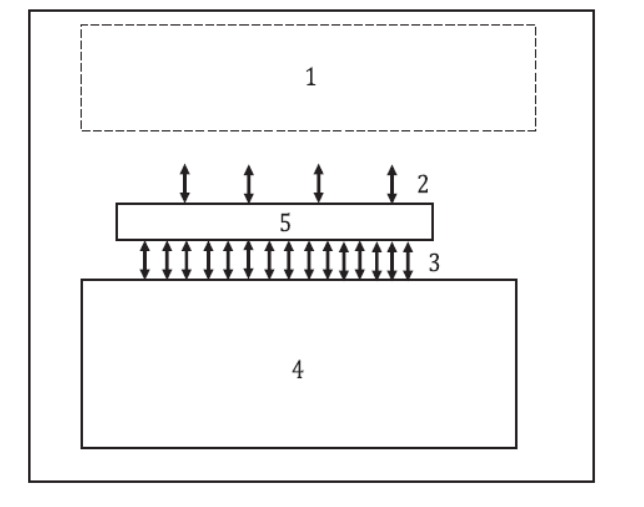
ИФБО для 00, который выполняет обработку протокола, будут те уровни протокола, к которым потенциальный нарушитель имеет прямой доступ. Это не обязательно весь стек (набор) протоколов, но и такое признается возможным.

Например, если 00 — некое сетевое устройство, которое позволяет потенциальным нарушителям влиять на все уровни стека протоколов (например, для отправки произвольных сигналов, произвольного напряжения, произвольных пакетов, произвольных дейтаграмм и т.д.), то граница ФБО существовала бы на каждом уровне стека протоколов. Таким образом, в функциональной спецификации необходимо бы было обращаться к каждому протоколу на каждом уровне стека протоколов.

Однако если бы 00 был межсетевым экраном, который защищает внутреннюю сеть от сети Интернет, потенциальный нарушитель не имел бы возможности непосредственных манипуляций с напряжениями, которые входят в ОО; любые чрезмерные напряжения просто не будут переданы через межсетевой уровень, т.е. нарушитель будет иметь доступ только к протоколам межсетевого уровня или выше. Границы ФБО существуют на каждом уровне стека протоколов. Таким образом, в функциональной спецификации следовало бы обращаться только к протоколам межсетевого уровня или выше его: в ней следовало бы описать каждый из различных уровней взаимодействия, на которых межсетевой экран уязвим в плане того, что составляет правильно сформированные исходные данные на линии; это может привести к тому, что могут существовать одновременно и правильно и неправильно сформированные исходные данные. Например, в описании протокола на межсетевом уровне описывается, что представляет собой правильно сформированный IP-пакет и что происходит при получении правильно сформированного и неправильно сформированного пакетов. А в описании на уровне протокола TCP (транспортный уровень) будет описываться успешное соединение по протоколу TCP, а также что происходит как в случае успешного установления соединения, так и в случае, когда соединение не может быть установлено или было случайно прервано. Если, как предполагается, задачей межсетевого экрана является фильтрация команд на прикладном уровне (например, по протоколу FTP или Telnet), описание на прикладном уровне будет описывать команды прикладного уровня, распознаваемые и фильтруемые межсетевым экраном, а также результаты обнаружения неизвестных команд.

Описания этих уровней, скорее всего, будут содержать ссылки на используемые изданные стандарты связи (Telnet, FTP, TCP и т.д.) с указанием того, какие определяемые пользователем опции были выбраны.

А.2.3.4 Адаптеры интерфейса



**Условные обозначения**

1 приложение

2 API

3 система

4 ядро (ФБО)

5 адаптеры интерфейса

**Рисунок А.1 – Адаптеры интерфейса**

Адаптеры интерфейса переводят сложный ряд взаимодействий к виду упрощенных общих сервисов, например, когда операционные системы создают интерфейсы прикладного программирования для использования приложениями (как показано на рисунке А.1). Будут ли ИФБО вызваны системой или интерфейсами прикладного программирования, зависит от того, что доступно для приложения: если приложение может напрямую осуществлять запрос к системе, то системные вызовы являются ИФБО. Если же что-либо препятствует их использованию напрямую и требуется, чтобы все связи осуществлялись через интерфейсы прикладного программирования, то интерфейсы прикладного программирования будут являться ИФБО.

Схожая ситуация с графическим интерфейсом пользователя: он переводит машинные команды в вид, удобный для пользователя. Аналогично к ИФБО относились бы команды, если бы пользователи имели к ним доступ или графические объекты (выпадающее меню, флажки, текстовые поля), если пользователи ограничены в использовании команд напрямую.

Стоит отметить, что в обоих этих примерах, если пользователю запрещено использовать более примитивные интерфейсы (т.е. запросы к системе или команды), описание этого ограничения и его осуществления будет включено в описание архитектуры безопасности (см. А.1). Кроме того, программа-адаптер интерфейсов будет частью ФБО.

А.2.3.5 Недоступные интерфейсы

Для конкретного ОО могут быть доступны не все интерфейсы, т.е. цели безопасности для среды функционирования (из ЗБ) могут предотвратить или ограничить доступ к этим интерфейсам так, что они станут практически недоступны. Такие интерфейсы не будут считаться ИФБО. Вот несколько примеров:

a) Если с целью безопасности для среды функционирования автономного межсетевого экрана указывается, что «межсетевой экран будет функционировать в серверном помещении, куда имеют доступ только доверенные лица и обученный персонал, и которая будет оснащена источником бесперебойного питания (на случай сбоя энергоснабжения)», то физические интерфейсы и интерфейсы энергоснабжения не будут доступны, поскольку доверенный и квалифицированный персонал не будет пытаться демонтировать межсетевой экран и/или отключить его от питания.

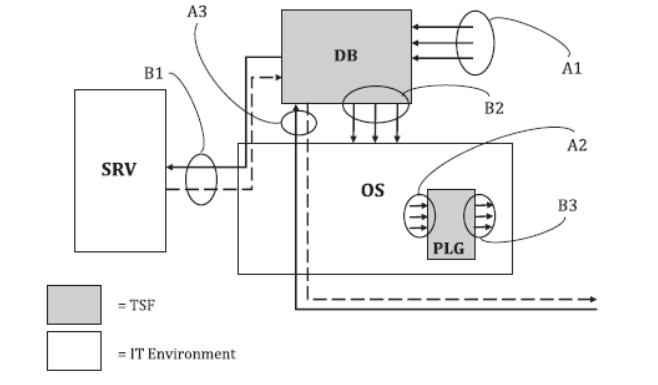
b) Если с целью безопасности для среды функционирования программного межсетевого экрана (приложения) указывается, что «ОС и аппаратные средства предоставят домен безопасности для приложения, свободный от воздействия других программ», то интерфейсы, через которые межсетевой экран может быть доступен для других приложений ОС (например, удаление или изменение исполняемого файла межсетевого экрана, чтение или запись напрямую в области памяти межсетевого экрана), не будут доступны, поскольку ОС/аппаратная часть среды функционирования не позволяют получить доступ к интерфейсу.

c) Если с целью безопасности для среды функционирования программного межсетевого экрана дополнительно указывается, что ОС и аппаратное обеспечение будут добросовестно исполнять команды ОО и не будут вмешиваться в ОО любым способом, интерфейсы, посредством которых межсетевой экран получает простейшие функциональные возможности ОС и аппаратного обеспечения (выполнение инструкций машинного кода, ИПП ОС, такие как создание, чтение, запись или удаление файлов, графический интерфейс пользователя и т.д.), не будут доступны, поскольку ОС/аппаратное обеспечение являются единственными сущностями, имеющими доступ к интерфейсам, и они являются полностью доверенными.

Во всех этих примерах недоступные интерфейсы не будут являться ИФБО.

**А.2.4 Пример: сложная СУБД**

На рисунке А.2 представлен сложный ОО: система управления базами данных, полагающаяся на аппаратные и программные средства, находящиеся за пределами границы ОО (в дальнейшем — среда ИТ). Для упрощения в этом примере ОО идентичен ФБО. Закрашенные прямоугольники представляют ФБО, в то время как незакрашенные представляют ИТ-сущности в среде функционирования. ФБО состоит из процессора базы данных и управления ГИП (на рисунке представлен прямоугольником «БД») и модуля ядра, который функционирует как часть ОС, выполняющая некоторые функциональные возможности безопасности (на рисунке представлен прямоугольником «ПЛГ»), Модуль ядра ФБО имеет точки входа, определенные в спецификации ОС, которые определяют, что ОС будет вызывать некоторые функциональные возможности (это может быть драйвер устройства или модуль аутентификации и т. д.). Суть в том, что подключаемый модуль ядра предоставляет сервисы безопасности, специфицированные функциональными требованиями из ЗБ.



Среда IT

**Рисунок А.2 – Взаимодействия в СУБД**

Среда IT состоит из самой операционной системы (прямоугольник «ОС»), а также внешнего сервера (на рисунке представлен прямоугольником «СРВ»), Этот внешний сервер, как и ОС, предоставляет сервисы, от которых зависит ФБО, и, следовательно, должен находиться в среде ИТ. Интерфейсы ИФБО обозначены на рисунке как Ах, прочие интерфейсы, которые были бы документированы в классе АСО «Композиция» — как Вх. Ниже приводится рассмотрение каждой из этих групп интерфейсов.

Группа интерфейсов А1 представляет собой наиболее очевидный набор ИФБО. Эти интерфейсы используются пользователями для непосредственного доступа к базе данных, ее функциональным возможностям безопасности и ресурсам.

Группа интерфейсов А2 представляет ИФБО, которые вызываются ОС с целью получения функциональных возможностей, предоставляемых подключаемым модулем. Это контрастирует с группой интерфейсов ВЗ, которая представляет вызовы, посылаемые подключаемым модулем с целью получения сервисов от среды IT.

Группа интерфейсов АЗ представляет ИФБО, которые проходят через среду IT. В этом случае СУБД взаимодействует по сети с помощью собственного протокола прикладного уровня. В то время как среда ИТ отвечает за обеспечение поддержки различных протоколов (например, Ethernet, IP, TCP), протокол прикладного уровня, который используется для получения сервисов СУБД, является ИФБО и должен быть задокументирован как таковой.

Пунктирной линией на рисунке указываются возвращаемые значения/сервисы ФБО через сетевое подключение.

Интерфейсы, отмеченные как Вх, представляют интерфейсы функций в среде IT. Эти интерфейсы не являются ИФБО и должны рассматриваться и анализироваться только при условии, что ОО используется в оценке композиции как часть действий, связанных с классом АСО.

**А.2.5 Пример функциональной спецификации**

Рассмотрим, как пример межсетевой экран, который используется между внутренней сетью и внешней сетью. Он верифицирует адрес источника полученных данных (с целью удостовериться, что внешние данные не пытаются замаскироваться под внутренние данные); в случае обнаружения любых таких попыток он сохраняет сведения об этом в журнале аудита Администратор связывается с межсетевым экраном путем установления Telnet-соединения из внутренней сети Действия администратора включают в себя аутентификацию, изменение паролей, исследование журнала аудита, а также настройку или смену адресов внутренних и внешних сетей.

В приведенном примере межсетевого экрана представлены следующие интерфейсы внутренней сети:

а) IP-дейтаграммы (пакеты данных IP и связанная с ними адресная информация);

b) команды администратора и следующие интерфейсы для внешней сети:

c) IP-дейтаграммы.

Описание интерфейсов: 1Р-дейтаграммы

Дейтаграммы находятся в формате, специфицированном в RFC 791.

- Назначение — передать блоки данных («дейтаграммы») от источника к целевым узлам сети, идентифицированным по фиксированной длине адреса; при необходимости предоставить фрагментацию и повторную сборку длинных дейтаграмм для передачи по сетям небольших пакетов.

- Метод использования — поставляются протоколом более низкого уровня (например, канального).

- Параметры — следующие поля заголовка IP-дейтаграммы: адрес отправителя, адрес получателя, метка нефрагментирования.

- Описание параметров — [В соответствии с определением из RFC 791, подразделом 3.1 («Формат интернет-заголовка»)].

- Действия — передача дейтаграмм, которые не являются подмененными; фрагментирование больших дейтаграмм в случае необходимости; повторная сборка фрагментов в дейтаграммы.

- Сообщения об ошибках — (нет). Нет надежной гарантии (уверенности, предоставленной протоколом более высокого уровня), что недоставленные дейтаграммы (например, те, которые должны быть фрагментированы для передачи, но для которых установлена метка «не фрагментировать») будут отброшены.

Описание интерфейсов: команды администратора

Команды администратора предоставляют администратору средства взаимодействия с межсетевым экраном.

Эти команды и реакции на запросы происходят поверх Telnet-соединения (RFC 854), установленного с любого узла внутренней сети. Доступные команды:

Passwd

- Назначение — устанавливает пароль администратора.

- Метод использования — Passwd <password>.

- Параметры — пароль.

- Описание параметров — значение нового пароля.

- Действия — изменение пароля в соответствии с новым предложенным значением.

Ограничения отсутствуют.

- Сообщения об ошибках — нет.

Readaudit

- Назначение — предоставляет администратору журнал аудита.

- Метод использования — Readaudit.

- Параметры — отсутствуют.

- Описание параметров — отсутствует.

- Действия — предоставляет текст журнала аудита.

- Сообщения об ошибках — отсутствуют.

Setintaddr

- Назначение — устанавливает адрес для внутреннего адреса.

- Метод использования — Setintaddr <address>.

- Параметры — адрес.

- Описание параметров — первые три поля IP-адреса (как определено в RFC 791).

Например: 123.123.123

- Действия — изменение внутреннего значения переменной, определяющей внутреннюю сеть, значение которой используется для оценки попытки фальсификации.

- Сообщения об ошибках — «адрес занят»: указывает, что идентифицированная внутренняя сеть совпадает с внешней сетью.

Setextaddr

- Назначение — устанавливает адрес для внешнего адреса.

- Метод использования — Setextaddr <address>.

- Параметры — адрес.

- Описание параметров — первые три поля IP-адреса (как определено в RFC 791).

Например: 123.123.123

- Действия — изменение значения внутренней переменной, определяющей внешнюю сеть.

- Сообщения об ошибках — «адрес занят»: указывает, что идентифицированная внутренняя сеть совпадает с внешней сетью.

**А.3 ADV\_INT: Дополнительный материал по внутренней структуре ФБО**

**А.3.1 Общие положения**

Из-за широкого диапазона типов ОО невозможно присвоить ОО более конкретное определение, чем «с полностью определенной внутренней структурой» или «минимальной сложности». Заключения по структуре и сложности должны быть получены исходя из конкретных технологий, используемых в ОО. Например, программное обеспечение может считаться программным обеспечением с полностью определенной внутренней структурой, если в нем представлены характеристики, перечисленные в технических принципах разработки программного обеспечения.

Данное приложение содержит дополнительные материалы по оценке структуры и сложности процедурно-ориентированных частей программного обеспечения ФБО. Этот материал основан на информации, доступной в литературе, посвященной принципам разработки программных средств. Для других видов внутренних структур (например, аппаратное обеспечение; не относящееся к процедурному программное обеспечение —такое как объектно-ориентированный код и т.д.) следует обратиться к соответствующей литературе по хорошим практикам в данной области.

**А.3.2 Структура процедурного программного обеспечения**

А.3.2.1 Общие положения

Структура процедурного программного обеспечения обычно оценивается в соответствии с его модульностью. Программное обеспечение, написанное по модульному проекту, помогает достичь большей понятности путем уточнения зависимости модулей друг от друга (связанность) и включения в модули только тех задач, которые тесно связаны друг с другом (связность). Использование модульного проекта снижает взаимозависимость между элементами ФБО и таким образом уменьшает риск того, что внесение изменений или ошибки в одном модуле повлияют на весь ОО. Его использование также повышает прозрачность и степень понятности проекта и предусматривает увеличение доверия тому, что не возникнут неожиданные последствия. Дополнительными и желательными свойствами модульной декомпозиции является уменьшение объема избыточного или ненужного кода.

Минимизация количества функций в ФБО позволяет оценщикам и разработчикам сосредоточить усилия только на тех функциях, которые необходимы для осуществления ФТБ, способствуя таким образом увеличению понятности и еще больше снижая вероятность ошибок проектирования или реализации.

Включение модульной декомпозиции, ранжирования и минимизации в процессы проектирования и реализации должно сопровождаться выполнением правильных соображений и принципов разработки программного обеспечения. На практике пригодная для использования система программного обеспечения, как правило, влечет за собой некоторую нежелательную связанность между модулями, наличие некоторых модулей, включающих в себя слабо относящиеся друг к другу функциональные возможности, а также некоторые другие тонкости и сложности модульного проекта. Подобные отклонения от идеальной модульной декомпозиции часто считаются необходимыми для достижения некоторой цели или выполнения ограничений, связанных с производительностью, совместимостью, планируемой функциональностью или некоторыми другими факторами, и могут быть приемлемыми в случае, если для них имеется предоставленное разработчиком логическое обоснование. При применении требований этого класса следует уделять должное внимание правильным принципам разработки программного обеспечения. При этом главное —достичь основной цели, заключающейся в понятности.

А.3.2.2 Связность

Связность представляет собой вид и степень зависимости друг от друга задач, выполняемых одним модулем программного обеспечения; связность подразделяется на случайную, коммуникативную, функциональную, логическую, последовательную и временную. Типы связности, охарактеризованные ниже, расположены в порядке убывания их желательности:

a) функциональная связность — модуль с функциональной связностью выполняет действия, связанные с единственной задачей. Модуль с функциональной связностью, такой как менеджер стека протоколов или менеджер очереди задач, преобразует один тип исходных данных в соответствующий тип данных на выходе;

b) последовательная связность — модуль с последовательной связностью содержит функциональные возможности, данные на выходе каждой из которых являются исходными для следующей функциональной возможности модуля. Примером модуля с последовательной связностью является модуль, который содержит функциональные возможности для фиксирования записей в журнале аудита и обеспечения подсчета нарушений процедуры аудита указанного типа;

c) коммуникативная (информационная) связность — модуль с коммуникативной связностью содержит функциональные возможности, которые производят данные на выходе для или используют данные на выходе из других функциональных возможностей в рамках модуля. Примером модуля с коммуникационной связностью является модуль проверки доступа, который включает мандатные, дискреционные проверки, а также проверки возможностей субъекта;

d) временная связность — модуль с временной связностью содержит функциональные возможности, которые должны быть выполнены примерно в одно и то же время. Пример модулей с временной связностью: модули инициализации (сброса настроек), восстановления и отключения;

e) логическая (или процедурная) связность — модуль с логической связностью производит схожие действия над разными структурами данных. Модуль демонстрирует логическую связность, если его функциональные возможности выполняют взаимосвязанные, но различные операции над разными входными данными;

f) случайная связность — модуль со случайной связностью выполняет не связанные или слабо связанные между собой действия.

А.3.2.3 Связанность

Связанность является видом и степенью взаимозависимости между программными модулями; типы связанности включают в себя связанность по запросу, по общей области и по содержимому. Типы связанности, охарактеризованные ниже, расположены в порядке убывания их желательности:

а) по запросу: два модуля являются связанными по запросу, если они взаимодействуют строго посредством использования задокументированных запросов от своих функций; примерами связанности по запросу является связанность данных, метки и управления. Они определены ниже:

l) данные: два модуля являются связанными по данным, если они взаимодействуют строго посредством параметров запроса, которые отображают отдельные элементы данных;

2) метка: два модуля являются связанными по метке, если они взаимодействуют посредством параметров запроса, включающих несколько полей или имеющих значимые внутренние структуры;

3) управление: два модуля являются связанными по управлению, если один передает информацию, которая предназначена для влияния на внутреннюю логическую структуру другого;

b) по общей области: два модуля являются связанными по общей области, если у них есть общая область данных или общий системный ресурс. Глобальные переменные показывают, что модули, использующие их, являются связанными по общей области. Связанность по общей области через глобальные переменные, как правило, допускается, но лишь в ограниченной степени. Например, переменные, которые размещаются в глобальной области, но используются только в одном модуле, являются неправильно размещенными, и их следует удалить.

При оценке пригодности глобальных переменных следует учитывать и другие факторы:

1) Количество модулей, которые изменяют глобальную переменную: обычно только одному модулю следует отвечать за контроль над содержимым глобальной переменной, но могут быть ситуации, в которых второй модуль может разделять эту ответственность. В таком случае должно быть предоставлено логическое обоснование. Разделение ответственности на более чем два модуля недопустимо (при оценке особое внимание следует уделять определению модуля, фактически отвечающего за содержимое переменной; например, если одна процедура используется для изменения переменных, но это процедура просто выполняет модификацию по запросу второй стороны, то отвечает за содержимое именно запрашивающий модуль. В таком случае возможно применение более чем одного такого модуля). Кроме того, в рамках определения сложности, если два модуля отвечают за содержимое глобальной переменной, рекомендуется, чтобы были четкие указания о том, как все изменения согласовываются между ними.

2) Количество модулей, которые ссылаются на глобальные переменные: несмотря на то что, как правило, количество модулей, которые ссылаются на глобальную переменную, неограниченно, в случаях, когда множество модулей представляют такие ссылки, следует проводить проверки на предмет их обоснованности и необходимости.

c) по содержимому: два модуля являются связанными по содержимому, если можно дать прямую ссылку от одного модуля на внутренние компоненты другого (например, изменить код или сослаться на внутреннюю структуру другого модуля). В результате часть или же все содержимое одного модуля эффективно включено в другой.

Связанность по содержимому может рассматриваться как использование недекларируемых интерфейсов модулей в отличие от сцепления по запросу, где используются только декларированные интерфейсы модулей.

**А.3.3 Сложность процедурного программного обеспечения**

Сложность является мерой количества точек принятия решений и логических путей исполнения, присущих коду. Техническая литература по разработке программного обеспечения определяет сложность как отрицательную характеристику программного обеспечения, поскольку она препятствует пониманию логики и строения кода. Другим препятствием для понимания кода является наличие кода, который не является необходимым, т.е. он не используется или является избыточным.

Использование ранжирования для разделения уровней представления и минимизации циклических зависимостей дополнительно позволяет улучшить понимание ФБО, обеспечивая большее доверие тому, что функциональные требования безопасности 00 точно и полно отражены в реализации.

Уменьшение сложности также включает в себя снижение или устранение взаимных зависимостей, которые относятся как к модулям одного уровня, так и к модулям отдельных уровней. Модули, взаимно зависящие друг от друга, могут полагаться друг на друга для получения одного результата, который может привести к состоянию блокировки, или, что еще хуже, состоянию гонки (например, к проблеме отношения времени проверки к времени использования), где окончательное решение может быть неопределенным и зависеть от вычислительной среды в конкретный момент времени.

Минимизация сложности проекта — ключевая характеристика механизма проверки ссылок, назначение которого заключается в том, чтобы подтвердить, что ФБО доступны пониманию и потому могут быть полностью проанализированы (существуют и другие важные характеристики механизма проверки ссылок, такие как собственная защита ФБО и невозможность обхода; к этим характеристикам выдвинуты требования в семействе ADV\_ARC).

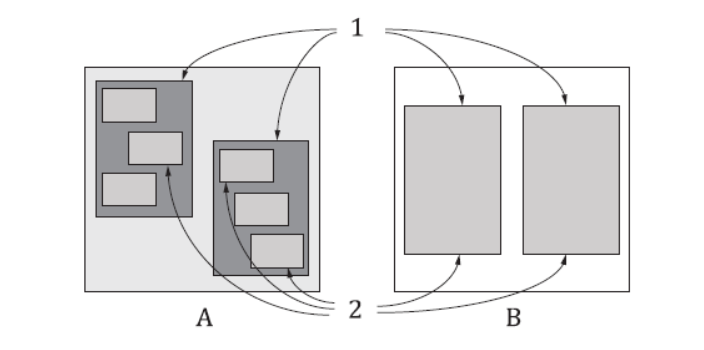
**A.4 ADV\_TDS: Подсистемы и модули**

**А.4.1 Общие положения**

Этот подраздел содержит дополнительные указания к семейству ADV\_TDS «Проект ОО» и к использованию терминов «подсистема» и «модуль». Далее рассматривается, как при возможности большей детализации снижаются требования к меньшей детализации.

**А.4.2 Подсистемы**

На рисунке А.З показано, что, в зависимости от сложности ФБО, проект может быть описан в терминах подсистем и модулей (где подсистемы находятся на более высоком уровне представления, чем модули), или он может быть описан в терминах одного уровня представления (например, подсистемы на более низком уровне доверия, модули на более высоких уровнях). В случаях, когда представлен более низкий уровень представления (модули), требования, применимые к более высокому уровню представления (подсистемы), должны выполняться по умолчанию. Эта концепция будет подробнее рассмотрена при обсуждении подсистем и модулей.



**Условные обозначения**

А ОО 1 (сложный)

B ОО 2 (простой)

1 подсистемы

2 модули

**Рисунок А.3 – Подсистемы и модули**

От разработчика ожидается описание проекта ОО в терминах подсистем. Термин «подсистемы» был намеренно выбран как нечеткий, чтобы можно было ссылаться на соответствующие единицы ОО (например, подсистемы, модули). Подсистемы могут быть даже неравномерными по области охвата, если при этом выполняются требования к описанию подсистем.

Первый вариант использования подсистем — определение границ ФБО, т. е. частей ОО, которые составляют ФБО. Обычно подсистема является частью ФБО, если она имеет возможность (будь-то проектная возможность или возможность реализации) повлиять на правильность работы любого ФТБ. Например, для программного обеспечения, зависящего от различных режимов работы оборудования, обеспечивающего разделение доменов (см. А.1), где осуществляющий ФТБ код выполняется в одном домене, все подсистемы, которые выполняются в этом домене, будут рассматриваться как часть ФБО. Кроме того, если сервер за пределами данного домена реализует ФТБ (например, обеспечивает поддержку политики контроля доступа над объектами), то он тоже будет считаться частью ФБО.

Второй вариант использования подсистем — предоставить структуру для описания ФБО на таком уровне описания, что в ней описывается, как работают ФБО, но не обязательно содержится детализация реализации на низком уровне из описания модулей (см. ниже); подсистемы описываются либо на верхнем уровне (где отсутствует разнообразие детальной информации о реализации), либо на детализированном уровне (при условии возможности более глубокого изучения реализации). Уровень описания, предоставляемого для подсистем, определяется тем, в какой степени подсистема отвечает за реализацию ФТБ.

Осуществляющая ФТБ подсистема является подсистемой, которая предоставляет механизмы осуществления элемента любого ФТБ или непосредственно поддерживает подсистему, которая несет ответственность за осуществление выполнения ФТБ. Если подсистема предоставляет (реализует) ИФБО, осуществляющий ФТБ, то она является осуществляющей ФТБ подсистемой.

Подсистемы также могут быть идентифицированы как поддерживающие ФТБ или не влияющие на выполнение ФТБ. От поддерживающей ФТБ подсистемы зависит осуществляющая выполнение ФТБ подсистема с целью реализации ФТБ, но поддерживающая осуществление ФТБ подсистема не играет такой прямой роли, как осуществляющая ФТБ. Подсистема, не влияющая на ФТБ, является независимой от других подсистем, как осуществляющих, так и поддерживающих, с целью реализации ФТБ.

**А.4.3 Модули**

Модуль, как правило, является относительно небольшой архитектурной единицей, которая может быть охарактеризована в терминах свойств внутренней структуры ФБО (ADV\_INT). Тогда как и требования ADV\_TDS.3 «Базовый модульный проект» (или выше) и требования внутренней структуры ФБО (те. семейства ADV\_INT) присутствуют в ПЗ или ЗБ, «модуль» сточки зрения требований семейства «Проект ОО» (ADV\_TDS), ссылается на ту же сущность, что и «модуль» по требованиям семейства «Внутренняя структура ФБО» (ADV\_INT). В отличие от подсистем, модули описывают реализацию на таком уровне детализации, который может служить в качестве руководства по рассмотрению представления реализации.

Важно отметить, что, в зависимости от ОО, модули и подсистемы могут относиться к тому же уровню представления. Для ADV\_TDS.1 «Базовый проект» и ADV\_TDS.2 «Архитектурный проект» (которые не требуют описания на уровне модулей) описание на уровне подсистем обеспечивает низкий уровень детализации ФБО. Для ADV\_TDS.3 «Базовый модульный проект» (для которого требуется описание модуля) эти описания обеспечивают низкий уровень детализации, в то время как описания на уровне подсистем (если они существуют в виде отдельных сущностей) служат лишь для описания модуля в общем контексте. Т. е. не является необходимым предоставлять подробные описания на уровне подсистем при наличии модульного описания. В ОО, которые являются достаточно простыми, отдельные «описания подсистем» также не являются необходимыми, требования могут быть удовлетворены за счет документации, предоставляемой модулями. Для сложных ОО цель описания подсистемы (по отношению к ФБО) заключается в предоставлении читателю контекста, обеспечивающего возможность проведения фокусированного на определенной области анализа. Это различие показано на рисунке А.З.

Модуль, осуществляющий выполнение ФТБ, является модулем, который непосредственно реализует функциональные требования безопасности (ФТБ) из ЗБ. Такие модули обычно реализуют ИФБО, осуществляющие выполнение ФТБ, но некоторые функциональные возможности, отраженные в ФТБ (например, аудит и функции для повторного использования объекта), могут не быть напрямую связаны с одним ИФБО. Как и в случае подсистем, модулями, поддерживающими выполнение ФТБ, являются те модули, которые зависят от модуля, осуществляющего выполнение ФТБ, но не несут ответственности за непосредственное осуществление ФТБ. Модули, не влияющие на выполнение ФТБ — это те модули, которые не связаны прямо или косвенно с осуществлением ФТБ.

Важно отметить, что определение «непосредственно реализует» несколько субъективно. В узком смысле оно может быть истолковано как одна или две строки кода, непосредственно выполняющие сравнение, операции обнуления и т.д. для реализации выполнения требования. Более широкое толкование состоит в том, что система включает в себя модуль, который вызывается в ответ на запрос ИФБО, осуществляющего выполнение ФТБ, и все модули, которые в свою очередь могут быть вызваны этим модулем (и так далее до завершения запроса). Ни одна из этих интерпретаций не является удовлетворительной, так как узость первого толкования может привести к тому, что важные модули будут неправильно классифицированы как модули, поддерживающие выполнение ФТБ, а второе приводит к тому, что модули, фактически не являющиеся модулями осуществления выполнения ФТБ, могут быть отнесены к таковым.

Следует, чтобы описание модуля было таким, чтобы можно было создать реализацию модуля на основании описания, и полученная реализация была бы: 1) идентична фактической реализации ФБО в терминах интерфейсов, представленных и используемых модулем, и 2) алгоритмически идентична модулю ФБО. Так, например, в RFC 793 представлено описание верхнего уровня протокола TCP. Это обязательно следует считать независимой реализацией. Несмотря на достаточно подробную детализацию, такое описание не подходит для описания проекта, так как не отражает специфику реализации. Фактическая реализация может содержать дополнения по отношению к описанию протокола в RFC, а также в ней может быть выполнен выбор реализации (например, использование глобальных данных или локальных в различных частях реализации), что может повлиять на проводимый анализ.

В описании проекта модуля TCP будет перечислен список интерфейсов, представленных в реализации (не только тех, которые определены в RFC 793), а также описание алгоритма обработки, связанной с модулями, реализующими TCP (при условии, что они были частью ФБО).

В проекте модули детально описываются в терминах предоставляемых ими функциональных возможностей (их назначения); представленных в них интерфейсов; возвращаемых значений от интерфейсов; используемых ими интерфейсов (предоставленных другими модулями), и того, как они предоставляют свои функции (один из возможных способов описания функций — алгоритмическое описание).

Назначение модуля следует подробно описать в терминах функциональных возможностей, которые предоставляет модуль. Следует, чтобы читатель мог получить общее представление о том, какие функциональные возможности есть у модуля в данной архитектуре.

Интерфейсы, представленные модулем, представляют собой интерфейсы, используемые другими модулями для вызова предусмотренных функциональных возможностей. Интерфейсы включают в себя как явные интерфейсы (например, последовательность запросов, вызываемую другими модулями), так и неявные интерфейсы (например, глобальные данные, на которые воздействует модуль). Интерфейсы описываются в терминах того, каким образом они вызываются, а также любых возвращаемых значений. Это описание включает в себя список параметров и описания этих параметров. Если параметры будут включать множество значений (например, параметр «флажок»), то должен быть указан полный набор значений параметра, который может оказать влияние на модуль. Кроме того, параметры, характеризующие структуры данных, описываются таким образом, чтобы каждое поле структур данных было идентифицировано и описано. Глобальные данные следует описать вне зависимости от того, производит ли модуль их чтение и/или запись.

Следует отметить, что разные языки программирования могут иметь дополнительные «интерфейсы», которые не всегда очевидны; примером может служить перегрузка оператора/функции в C++. Этот «неявный интерфейс» в описании класса должен быть также описан как часть модульного проекта. Отметим, что хотя в модуле может присутствовать только один интерфейс, чаще встречаются модули, представляющие собой небольшой набор взаимосвязанных интерфейсов.

С другой стороны, интерфейсы, используемые модулем, должны быть определены так, чтобы можно было идентифицировать, какой модуль вызывается посредством описанного модуля. Из описания проекта должно быть понятно, в чем алгоритмическая причина вызова модуля. Например, для случая, когда есть описанный модуль А и он использует процедуру сортировки пузырьковым методом модуля В, алгоритмического описания «Модуль А вызывает интерфейс double\_bubble () модуля В для выполнения сортировки пузырьковым методом» будет недостаточно. Адекватное алгоритмическое описание должно быть следующим: «Модуль А вызывает процедуру double\_bubble со списком записей контроля доступа; double\_bubble () в ответ на запрос возвращает вначале отобранные по имени пользователя записи, затем по полю access\_allowed, согласно следующим правилам...». Описание модуля в проекте должно быть достаточно детализированным для того, чтобы было понятно, какие результаты модуль А ожидает от интерфейса сортировки пузырьковым методом. Следует отметить, что согласно одному из способов представления эти вызываемые интерфейсы отображаются посредством дерева вызовов, а затем алгоритмическое описание может быть включено в алгоритмическое описание вызываемого модуля.

Как упоминалось ранее, в алгоритмическое описание модуля следует включать описание реализации модуля в виде алгоритма. Это может быть сделано через псевдо-код, через блок-схемы, либо (в ADV\_TDS.3 «Базовый модульный проект») посредством неформального текста. В описании рассматривается, как функциональные возможности ввода и запросов модуля используются для выполнения функциональных возможностей модуля. Также отмечаются изменения глобальных данных, состояния системы и возвращаемых модулем значений. Описание составляется на таком уровне детализации, чтобы могла быть получена реализацию, которая была бы очень похожа на фактическую реализацию ОО.

Следует отметить, что исходный код не соответствует требованиям по документации модуля. Хотя модульный проект описывает реализацию, он не является реализацией. Комментарии к исходному коду могут быть достаточной документацией, если в них предоставлено объяснение назначения исходного кода. Односложные комментарии, поясняющие назначение каждой строчки, бесполезны, поскольку они не предоставляют объяснения того, что должно быть результатом выполнения модуля.

В представленных ниже элементах маркировка (осуществляющие ФТБ, поддерживающие ФТБ и не влияющие на ФТБ), которая присваивается подсистемам и модулям, используется для описания количества и типа информации, которая должна быть предоставлена разработчиком. Элементы были структурированы так, чтобы не ожидалось, что разработчик предоставит только специфицированную информацию, т. е., если документация разработчика по ФБО предоставляет информацию в соответствии с требованиями, представленными ниже, от разработчика не требуется обновлять документацию и маркировать свои подсистемы и модули как осуществляющие ФТБ, поддерживающие ФТБ и не влияющие на ФТБ. Основная цель этой маркировки — позволить разработчикам с менее «зрелыми» методологиями разработки (и связанными с ними элементами, например, детализированной документации по интерфейсам и проекту) предоставить необходимые свидетельства без лишних затрат.

**А.4.4 Подход к ранжированию**

Поскольку существует некоторая субъективность в определении того, что является осуществляющим ФТБ, а что поддерживающим ФТБ (а в некоторых случаях даже при определении того, что является не влияющим на ФТБ), для этого семейства была принята следующая парадигма. В первых компонентах данного семейства разработчик делает заключение о классификации подсистем на осуществляющие ФТБ и т.д., поставляя соответствующую информацию. Оценщику в таком случае предоставляется малый объем дополнительных свидетельств для подтверждения утверждений о соответствии. По мере увеличения уровня желаемого доверия заключение о классификации по-прежнему делает разработчик, но оценщик получает все больше и больше свидетельств, используемых для подтверждения классификации, выполненной разработчиком.

С целью сфокусировать анализ, проводимый оценщиком, на имеющих значение для ФТБ частях ОО, особенно на более низких уровнях доверия, компоненты семейства ранжированы таким образом, чтобы первоначально детализированная информация требовалась только для осуществляющих ФТБ элементов архитектуры. По мере увеличения уровня доверия требуется больше информации, необходимой для поддерживающих ФТБ сущностей и (в итоге) для не влияющих на ФТБ. Следует отметить, что даже в случае, когда требуется полная информация, не является необходимым проводить анализ всей этой информации с той же степенью детализации. Обращать внимание всегда следует на то, была ли предоставлена и проанализирована необходимая информация.

**Таблица А.1 – Обобщает информацию, необходимую для каждого компонента семейства с целью описания архитектурных сущностей**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Компонент семейства** | **Подсистема TSF** | | | **Модуль TSF** | | |
| **Осуществляющая TSF** | **Поддерживающая TSF** | **Не влияющая на TSF** | **Осуществляющий TSF** | **Поддерживающий TSF** | **Не влияющий на TSF** |
| ADV\_TDS.1 Базовый проект (неформальное представление) | Структура, аннотация осуществляющего TSF режима функционирования, взаимодействия | Поддержка проекта а | Поддержка проекта |  |  |  |
| ADV\_TDS.2 Архитектурный проект (неформальное представление) | Структура, детальное описание осуществляющего TSF режима функционирования, аннотация прочих режимов, взаимодействия | Структура, аннотация прочих режимов, взаимодействия | Поддержка проекта, взаимодействия |  |  |  |
| ADV\_TDS.3 Базовый модульный проект | Описание, взаимодействия | Описание, взаимодействия | Описание, взаимодействия | Назначение, интерфейсы TSF b | Взаимодействие, назначение | Взаимодейcтвие, назначение |
|  | | | | | | |
|  | | | | | | |
| *Продолжение таблицы А.1* | | | | | | |
| **Компонент семейства** | **Подсистема TSF** | **Модуль TSF** | **Компонент семейства** | **Подсистема TSF** | **Модуль TSF** | **Компонент семейства** |
| (неформальное представление) |  |  |  |  |  |  |
| ADV\_TDS.4 Полуформальный модульный проект (полуформальное представление) | Описание, взаимодействия | Описание, взаимодействия | Описание, взаимодействия | Назначение интерфейсы ФТБ | Назначение, интерфейсы ФТБ | Взаимодействие, назначение |
| ADV\_TDS.5 Полный полуформальный модульный проект (полуформальное представление) | Описание, взаимодействия | Описание, взаимодействия | Описание, взаимодействия | Назначение, все интерфейсыc | Назначение, все интерфейсы | Назначение, все интерфейсы |
| ADV\_TDS.6 Полный полуформальный модульный проект с формальным высокоуровневым представлением (полуформальное представление; дополнительное формальное представление) | Описание, взаимодействия | Описание, взаимодействия | Описание, взаимодействия | Назначение, все интерфейсы | Назначение, все интерфейсы | Назначение, все интерфейсы |
| а Поддержка проекта означает, что нужна только достаточная документация для поддержания классификации подсистемы/модуля.  b Интерфейсы ФТБ— означает, что описание модуля содержит для каждого осуществляющего выполнение ФТБ модуля возвращаемые значения и вызываемые интерфейсы других модулей.  c Все интерфейсы — означает, что описание модуля содержит для каждого интерфейса возвращаемые значения и вызываемые интерфейсы других модулей. | | | | | | |

**A.4.5 Соответствие безопасности**

Серия стандартов ISO/IEC 15408 концентрирует описание, доказательства и анализ функциональных возможностей безопасности ОО. Это требует характеристики значимости безопасности функциональных и физических частей ОО. Интерфейсы, подсистемы и модули можно разделить (неявно или явно) на «обеспечивающие SFR», «поддерживающие SFR» или «невлияющие на SFR».

Свидетельства разработчика и оценочный анализ относятся к ОО и сосредоточены на ФБО и их реализации, обеспечивающей и поддерживающей ФТБ. Описание архитектуры безопасности должно демонстрировать, что идентифицированные подсистемы ОО, не относящиеся к ФБО, не обходят ФБО, а ФБО защищают себя от повреждения кодом или объектами, не относящимися к ФБО. Разработчик должен описать невлияющие на ФТБ интерфейсы, подсистемы и модули в проекте ОО и продемонстрировать, что они не мешают ФБО из-за своих целей, взаимодействия или разделения ресурсов.

Интерфейс, подсистема или модуль – это:

— Обеспечение соблюдения ФТБ, если оно непосредственно реализует ФТБ.

— Поддержка ФТБ, если она должна работать функционально правильно, чтобы поддерживать правильное функционирование ФТБ.

— невмешательство в ФТБ, если оно не связано с реализацией ФТБ.

Сосредоточение внимания на функциях обеспечения безопасности и поддержки безопасности требует доказательств невмешательства в другие функции. Даже правильно реализованные функции и механизмы обеспечения безопасности могут быть обойдены, деактивированы, повреждены или напрямую атакованы. Невмешательство подразумевает, что ФБО не могут быть использованы не по назначению, а несанкционированный доступ к ресурсам реализации ФБО предотвращен или невозможен. Таким образом, аспекты архитектуры безопасности, такие как необходимость и самозащита, имеют решающее значение, если значимость безопасности интерфейсов, подсистем и модулей классифицирована, и эта категоризация используется в анализе уязвимостей.

Самозащита ФБО — это свойство архитектуры безопасности, согласно которому ФБО не могут быть повреждены кодом или объектами, не относящимися к ФБО. Сюда входят подсистемы ОО, не относящиеся к ФБО, и части продукта ИТ, не относящиеся к ОО. Это аналогично свидетельству о невлияющих на SFR подсистемах/модулях.

Домены безопасности — это среды, предоставляемые ФБО для использования недоверенными объектами таким образом, что эти среды изолированы и защищены друг от друга.

Поэтому анализ невмешательства во время оценки требует изучения архитектуры безопасности ОО (ADV\_ARC) и может потребовать дополнительной информации о подсистемах, не относящихся к ФБО, а не только о структуре ОО с точки зрения подсистем, как предусмотрено в ADV\_TDS.x.1. Разработчики должны предоставить обоснование правильности определения ФБО и анализ невлияющего на ФТБ модуля с точки зрения его назначения и взаимодействия с другими модулями:

— цель: как модуль обеспечивает свою функциональность, никаких дополнительных проектных решений не требуется.

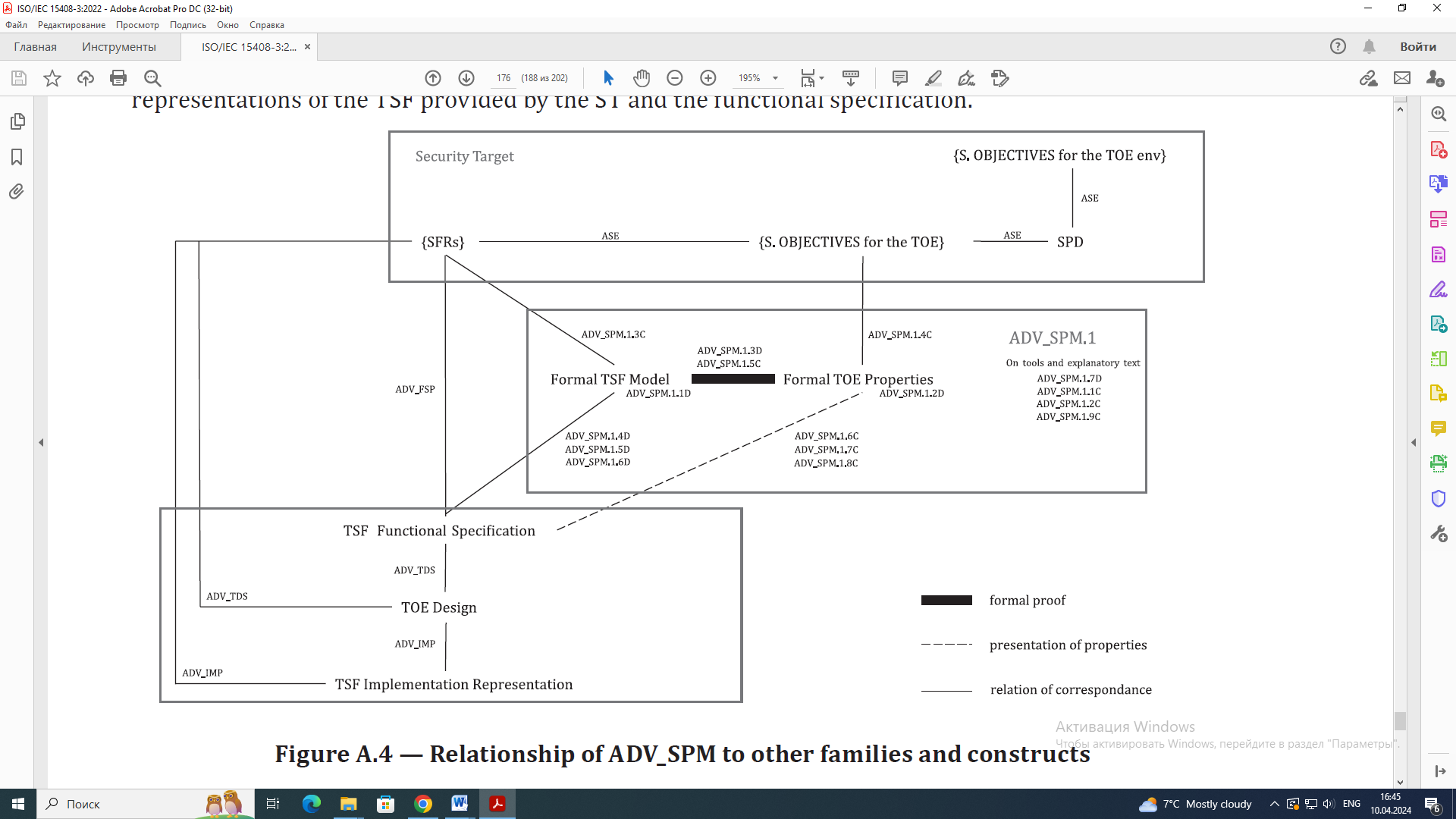
— взаимодействие: причина, по которой подсистемы или модули взаимодействуют, и характеризующая передаваемую информацию (меньше подробностей, чем для интерфейсов).

Во время оценки невмешательство должно быть проанализировано как часть изучения функциональной спецификации и проекта ОО, а также анализа уязвимостей. Классификация интерфейсов, подсистем и модулей на обеспечивающие SFR, поддерживающие SFR и невлияющие на SFR, подразумевает конкретное изучение функциональной спецификации, проектирования и тестирования. Интерпретация ФБО как всех доступных внешних интерфейсов ФБО могла бы помочь в этом анализе. Функциональные тесты всех подсистем ФБО (начиная с ATE\_DPT.1) и всех модулей ФБО (ATE\_DPT.3 и выше) должны предоставить доказательства правильности их категоризации безопасности.

**А.4.5 Дополнительный материал по формальным методам**

Формальные методы обеспечивают математическое представление ФБО и их поведения и требуются ADV\_SPM.1 (Формальная модель ФБО), а также ADV\_FSP.6 (Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией) и ADV\_TDS.6 (Полная полуформальная модульная конструкция), с формальной презентацией проекта высокого уровня). В ISO/IEC 18045:2022, формальный стиль Приложения C, представлен дополнительный материал по формальным методам.

На рисунке A.4 показаны взаимосвязи между SPM, как указано в ADV\_SPM.1, и представлениями ФБО, предоставляемыми ЗБ и функциональной спецификацией.



Об инструментах и пояснительном тексте

Формальная модель TSF

Формальные свойства TOE

ЦЕЛИ БЕЗОПАСНОСТИ

для TOE

ЦЕЛИ БЕЗОПАСНОСТИ для среды TOE

Проект TOE

Представление реализации TSF

Отношение соответствия

Представление свойства

Формальная модель

Задания по безопасности

**Рисунок А.4 – Связь ADV\_SPM с другими семействами и конструкциями**

Класс ASE определяет требования к соответствию между ФТБ и целями безопасности ОО, а также требования к соответствию между элементами SPD и целями безопасности для ОО и целями безопасности для операционной среды соответственно.

Каждое семейство доверия специфично для представления ФБО, т.е. Функциональная спецификация (ADV\_FSP), проект ОО (ADV\_TDS) и представление реализации ФБО (ADV\_IMP) определяют как требования, относящиеся к действиям разработчика по обеспечению соответствия этому конкретному представлению ФБО и представлению непосредственно над ним, так и требования к оценке соответствия этого представления. конкретное представление ФБО для набора ФТБ.

Семейство ADV\_SPM фокусируется на формальной модели безопасности, которая является формальным представлением существенных аспектов безопасности (т. е. ФБО) и их взаимосвязи с поведением ОО. В частности, формальная модель ФБО представляет собой формальное описание оцениваемой системы, определенное всем набором ФТБ, описанных в ЗБ. Набор формальных свойств ОО, определенных для этой формальной модели, охватывает все цели безопасности ОО. С этой целью семейство ADV\_SPM определяет:

— требования, относящиеся к действиям разработчика по формальному моделированию ФБО (ADV\_SPM.1.1D) и набора формальных свойств ОО (ADV\_SPM.1.2D);

— требования к содержанию и оформлению переписки между:

— формальная модель ФБО и полный набор ФТБ (ADV\_SPM.1.3C);

— формальные свойства ОО и цели безопасности для ОО (ADV\_SPM.1.4C).

Гарантия обеспечивается путем формального доказательства того, что формальная модель ФБО удовлетворяет формальным свойствам ОО. С этой целью семейство ADV\_SPM определяет требования для этого формального доказательства (ADV\_SPM.1.3D и ADV\_SPM.1.5C). Доверие, полученное путем формального доказательства свойств формальной модели, сопровождается доверием, полученным путем определения обоснования соответствия между формальной моделью и функциональной спецификацией ФБО (ADV\_SPM.1.4D). Обоснование соответствия состоит из формального доказательства при отображении на формальные аспекты функциональной спецификации ФБО (ADV\_SPM.1.6D). Он состоит из полуформальной демонстрации, когда функциональная спецификация описывается в полуформальном стиле (ADV\_SPM.1.5D). Семейство ADV\_SPM определяет требования к содержанию для обоснования соответствия, касающегося сохранения формальных свойств ОО функциональной спецификацией ФБО (ADV\_SPM.1.6C/7C/8C).

Семейство ADV\_SPM включает требования, касающиеся базовой математической теории (ADV\_SPM.1.1C), инструментов, используемых для формального моделирования и доказательства (ADV\_SPM.1.7D и ADV\_SPM.1.9C), а также требований к пояснительному тексту, поддерживающему и документирующему каждый элемент. (ADV\_SPM.1.2C).

ADV\_FSP требует, чтобы разработчик установил соответствие между функциональной спецификацией ФБО и ФТБ. Хотя это требование не зависит от SPM, при использовании ADV\_SPM.1 это соответствие является побочным продуктом соответствия между ФТБ и формальной моделью ФБО, с одной стороны, и между моделью и функциональной спецификацией, с другой стороны.

На рисунке А.4 показана роль формальной модели ФБО во взаимосвязи между функциональной спецификацией и ЗБ (свойствами ФТБ и ОО), которая впоследствии распространяется по представлениям проекта и реализации посредством семейств требований ADV\_TDS и ADV\_IMP.

## **Приложение В**

*(информационное)*

**Композиция (АСО)**

**В.1 Общие положения**

Целью данного приложения является объяснение принципов оценки композиции и критериев класса АСО. В данном приложении не определяются критерии класса ASE; данное определение приведено в разделе 9.

**В.2 Необходимость оценки составных ОО**

В целом рынок ИТ составляют производители, предлагающие отдельные продукты/технологии. Хотя бывают и случаи, когда производители аппаратного обеспечения ПК могут также предлагать прикладное программное обеспечение и/или операционные системы, а производитель микросхем (чипов) может также разработать специализированную ОС под свой чипсет, но в основном имеет место ситуация, когда ИТ-решения реализуются несколькими производителями.

Иногда существует потребность в доверии к объединению (композиции) компонентов в дополнение к доверию, полученному для каждого отдельного компонента. И хотя между производителями существует кооперация (сотрудничество), тем не менее в рамках распространения материала, необходимого для технической интеграции компонентов, соглашения между производителями редко распространяются вплоть до предоставления информации о деталях проектирования и свидетельствах процессов/процедур разработки. Недостаточность информации, предоставленной разработчиком компонента, на который полагается другой компонент, приводит к тому, что разработчик зависимого компонента не имеет доступа к информации, необходимой для оценки базового и зависимого компонентов по ОУД2 и выше. Таким образом, хотя оценка зависимого компонента может быть проведена на любом уровне доверия, для объединения нескольких компонентов с ОУД2 и выше необходимо повторно использовать свидетельства и результаты оценки, проведенной разработчиком.

Предполагается, что критерии класса АСО применимы в случае, если одна сущность ИТ зависит от другой для предоставления сервисов безопасности. Сущность, предоставляющая такие сервисы, называется «базовым компонентом», получающая сервисы — «зависимым компонентом». Такие взаимоотношения могут существовать в различных условиях. Например, приложение (зависимый компонент) может использовать сервисы, предоставляемые операционной системой (базовый компонент). Взаимоотношения могут быть и пиринговыми (равноправными), когда два связанных приложения могут быть запущены в общей операционной среде или на различных аппаратных платформах. Если один из равноправных пользователей/узлов сети предоставляет сервисы другому узлу/пользователю, то он считается базовым компонентом, тогда как получатель сервисов — зависимым. Если же пользователи/узлы сети взаимно предоставляют друг другу сервисы, они будут считаться базовыми компонентами для предоставляемых сервисов и зависимыми —для получаемых. Это потребует повтора компонентов АСО, причем к каждому из таких компонентов будут предъявляться требования как к базовому, и одновременно как к зависимому компоненту.

Предполагается, что критерии будет постепенно применимы и в более широком смысле (например, когда составной ОО, состоящий из зависимого и базового компонента, сам становится базовым компонентом другого составного ОО), в более сложных взаимоотношениях, но это может потребовать дальнейшего анализа трактовок.

Для проведения оценки ОО необходимо оценить каждый компонент независимо, так как оценка составного ОО основывается на результатах оценки каждого из компонентов по отдельности. Оценка зависимых компонентов может продолжаться и после начала оценки составного ОО. Однако эта оценка должна быть закончена до завершения оценки ОО.

Действия по оценке составного ОО могут проходить вместе с оценкой зависимых компонентов по двум причинам:

a) Экономический/деловой фактор — разработчик независимых компонентов будет или спонсировать действия по оценке составного ОО или поддерживать эти действия, так как такая оценка комплектуется оценкой зависимых компонентов, требуемой для действий по оценке составного ОО.

b) Технический фактор — в компонентах рассматривается, предоставляется ли требуемое доверие базовым компонентом (например, с учетом изменений базового компонента после завершения оценки) с учетом того, что зависимый компонент недавно прошел оценку (или проходит в настоящее время) и имеются в наличии все комплектующие, необходимые для проведения оценки. Таким образом, никакие действия при объединении компонентов не требуют пересмотра и повторного утверждения результатов оценки зависимых компонентов. Кроме того, подтверждается, что базовым компонентом формируется (одна из) тестовых конфигураций зависимого компонента во время проведения оценки этого зависимого компонента, благодаря чему в семействе АСО\_СТТ рассматривается базовый компонент в данной конфигурации.

Свидетельство оценки зависимого компонента, предоставляемое оценщиком, является необходимым для проведения действий по оценке составного ОО. Единственный материал по оценке базового компонента, требуемый для проведения оценки составного ОО, это:

а) остаточные уязвимости базового компонента, выявленные во время его оценки. Это требуется для действий семейства ACO\_VUL.

Никаких других свидетельств оценки базового компонента для проведения оценки составного ОО не требуется, так как результаты оценки базового компонента следует использовать повторно. Дополнительная информация по базовому компоненту может потребоваться в случае, если ФБО составного ОО включает больше базовых компонентов, чем было учтено в ФБО во время проведения оценки базового компонента.

Предполагается, что оценка базового и зависимого компонента будет завершена ко времени получения заключительного решения по компонентам АСО.

В компонентах семейства ACO\_VUL рассматривается противостояние нарушителям с потенциалом атаки до Усиленного базового включительно. Объясняется это тем, какой уровень информации по проекту может быть представлен о том, как базовый компонент предоставляет сервисы, на которые полагается зависимый компонент при применении действий, описанных в семействе ACO\_DEV. Таким образом, уровень доверия, получаемый при оценке составного ОО с использованием СоПД ограничен тем уровнем, который приобретается от оценки ОО-компонентов по ОУД4. Хотя доверие компонента, являющегося частью составного ОО, может быть выше, чем ОУД4.

**В.3 Выполнение оценки ЗБ для составного ОО**

Для оценки составного ОО (т.е. базового и зависимого компонента) разработчиком предоставляется ЗБ.

В этом ЗБ идентифицируются все пакеты доверия, которые применимы к составному ОО, предоставляя доверие составной сущности путем получения доверия, достигнутого при оценке компонентов.

Цель рассмотрения композиции компонентов в ЗБ — подтвердить совместимость компонентов сточки зрения среды функционирования и требований, а также оценить соответствие ЗБ составного ОО заданиям по безопасности его компонентов и представленных в этих ЗБ политик безопасности. Это включает и определение того, что ЗБ компонентов и политики безопасности, представленные в них, являются совместимыми.

ЗБ составного ОО может ссылаться на содержание ЗБ компонентов или разработчик ЗБ может повторить материал ЗБ компонентов в ЗБ составного ОО, предоставив обоснование тому, как ЗБ компонентов представлено в ЗБ составного ОО.

Вовремя проведения действий по оценке составного ОО, описанных в семействе ASE\_CCL оценщик определяет, что ЗБ компонентов точно представлены в ЗБ составного ОО. Это достигается путем определения, что ЗБ составного ОО явно соответствует ЗБ ОО-компонентов. Кроме того, оценщику нужно подтвердить, что зависимости зависимого компонента от среды функционирования адекватно выполняются в составном ОО.

Описание составного ОО содержит решение о композиции. Описываются логическая и физическая области и границы решения о композиции, а также идентифицируется логическая граница (или границы) между компонентами. Описание идентифицирует функциональные возможности безопасности, которые должны быть предоставлены каждым компонентом.

Изложение ФТБ для составного ОО идентифицирует, какой компонент удовлетворяет ФТБ. Если ФТБ выполняются обоими компонентами, тогда в изложении указывается, какие аспекты ФТБ выполняет каждый из них.

Также и в краткой спецификации составного ОО указывается, какой компонент обеспечивает описанные функциональные возможности безопасности.

Следует, чтобы пакет требований класса ASE: «Оценка ЗБ», применяемый к ЗБ составного ОО, соответствовал пакету требований этого семейства, используемому при оценке ОО-компонентов.

Повторное использование результатов оценки ЗБ компонентов может применяться в случаях, когда ЗБ составного ОО напрямую ссылается на ЗБ компонента. Например, если ЗБ составного ОО ссылается на ЗБ компонента в части изложения ФТБ к нему, оценщик сможет понять, что требования по выполнению всех заданий и операций по выбору (как установлено в ASE\_REQ.\*.3C) были удовлетворены при оценке компонента.

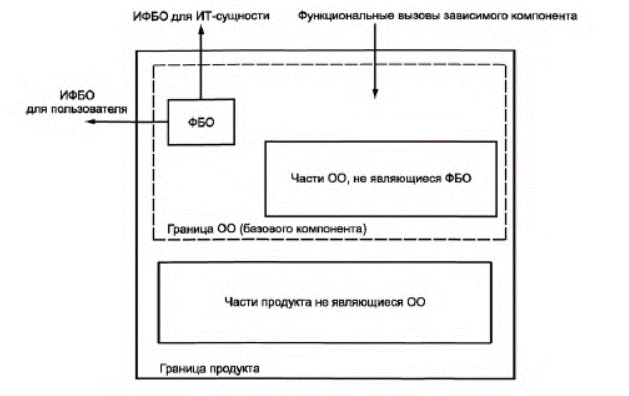
**В.4 Взаимодействия между объединенными сущностями ИТ**

ФБО базового компонента часто определяются без знания о зависимостях возможных приложений, которые могут быть объединены с этим компонентом. ФБО базового компонента определяется таким образом, чтобы включать в себя все части базового компонента, на которые необходимо полагаться для осуществления выполнения ФТБ базового компонента. Это включает и те части базового компонента, необходимые для реализации его ФТБ.

ИФБО данного базового компонента представляет интерфейсы, предоставленные ФБО внешним сущностям в изложении ФТБ для вызова сервисов ФБО. Это включает интерфейсы как для пользователя-человека, так и для внешних ИТ-сущностей. Однако ИФБО лишь добавляет данные интерфейсы к ФБО, а потому вовсе не обязательна полная спецификация всех возможных взаимодействий между базовым компонентом и внешней сущностью. Базовый компонент может представлять интерфейсы к тем сервисам, которые не рассматриваются значимыми для безопасности либо из-за назначения сервиса (например, настройка шрифта), либо потому, что связанные с настоящим стандартом ФТБ не предъявлялись в ЗБ базового компонента (например, интерфейс ввода логина в случае, когда согласно ИСО/МЭК 15408-2 не предъявляются ФТБ к идентификации и аутентификации).

Функциональные интерфейсы обеспечиваются базовым компонентом в дополнение к интерфейсам безопасности (ИФБО), и их не требуется рассматривать при проведении оценки базового компонента. К таким интерфейсам часто относятся и используемые зависимым компонентом для вызова сервисов базового компонента.

Базовый компонент может содержать и некоторые косвенные интерфейсы, через которые можно вызвать ИФБО, например интерфейсы прикладного программирования, которые могут быть использованы для вызова сервиса ФБО, не рассматривающегося в процессе оценки базового компонента.



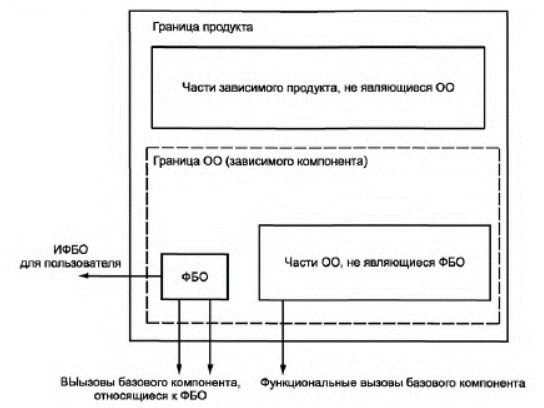
**Рисунок В.1 – Обобщенное представление базового компонента**

Зависимый по отношению к базовому компонент определяется схожим образом: взаимодействия с внешними сущностями, определенные ФТБ в ЗБ компонента, относят к ИФБО и исследуют в семействе ADV\_FSP.

Любой запрос от зависимых ФБО к среде функционирования в поддержку ФТБ покажет, что зависимым ФБО необходимо получение некоторых сервисов от среды для осуществления заявленного зависимого компонента ФТБ.

Такие сервисы находятся за границей зависимого компонента, а базовый компонент скорее всего не будет определен в ЗБ зависимого компонента как внешняя сущность. Поэтому вызов сервисов зависимыми ФБО к базовой платформе (базовому компоненту) не будет подвергаться анализу в части действий семейства «Функциональная спецификация» (ADV\_FSP). Такие зависимости от базового компонента отражаются в ЗБ зависимого компонента в качестве целей безопасности для среды функционирования.

Обобщенное представление зависимого компонента и его взаимодействий представлено на рисунке В.2.



**Рисунок В.2 – Обобщенное представление зависимого компонента**

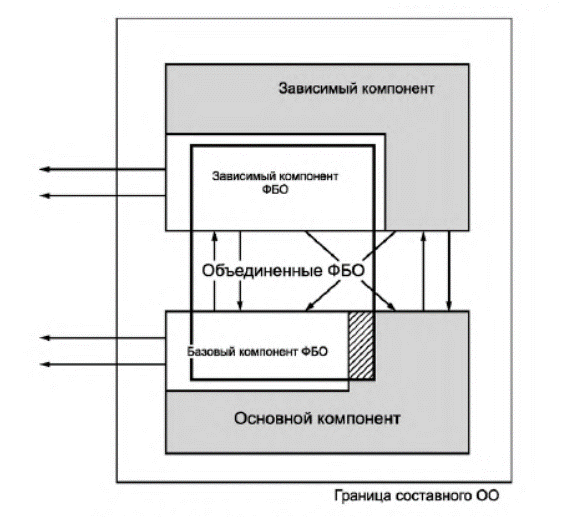
При рассмотрении композиции базового и зависимого компонента, если ФБО зависимого компонента требуют сервисы базового компонента для поддержки реализации ФТБ, необходимо определить интерфейс для этих сервисов. Если такой сервис предоставляется ФБО базового компонента, тогда интерфейс следует считать ИФБО базового компонента и определять в функциональной спецификации базового компонента.

Если же сервисы, запрашиваемые ФБО зависимого компонента, не предоставляются ФБО базового компонента (те. они реализуются в части базового компонента, не являющейся ФБО, или даже в части базового компонента, не относящейся к ОО — на рисунке В.З такая часть не представлена), то вряд ли будет ИФБО базового компонента, относящийся к данному сервису, если только сервис не служит связующим звеном для ФБО базового компонента. Интерфейсы зависимого компонента с функциональной средой для получения таких сервисов рассматривается в семействе «Зависимости зависимых компонентов» (ACO\_REL).

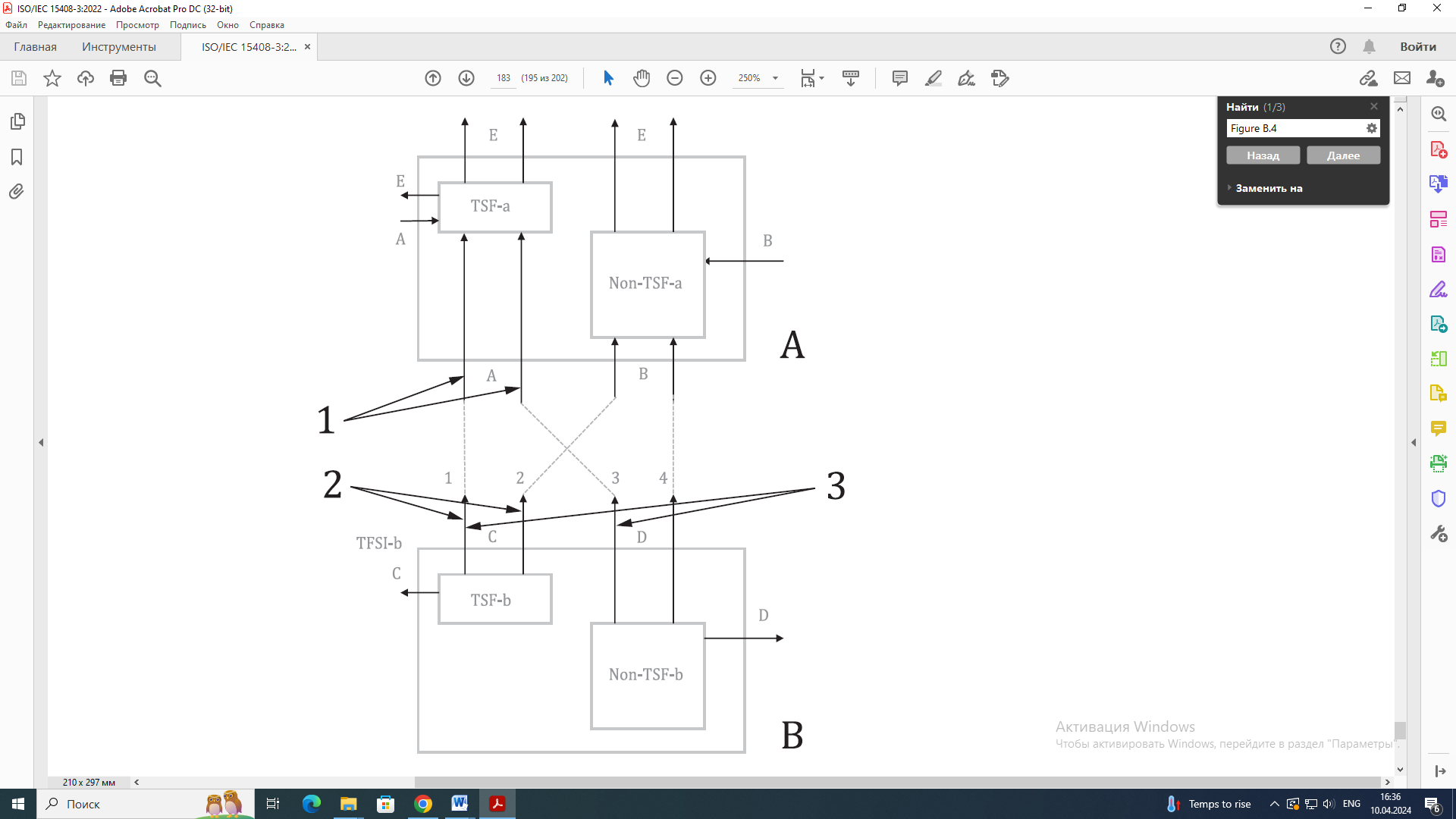
Части базового компонента, не являющиеся ФБО, включаются в ФБО составного ОО по причине зависимости зависимого компонента от базового для поддержки ФТБ зависимого компонента. В таких случаях ФБО составного ОО будет включать больше, чем просто совокупность ФБО его компонентов.

Возможны случаи, когда к ИФБО базового компонента обращаются способом, который не учитывался при проведении оценки базового компонента. Это требует дальнейшего тестирования ИФБО базового компонента.

Возможные взаимодействия описываются подробнее на следующей схеме (рисунок В.4) и во вспомогательном тексте.



**Рисунок В.3 – Обобщенное представление составного ОО**



**Условные обозначения**

А зависимый компонент-a

В базовый компонент-b

1 ACO\_REL (компонент-а)

2 ADV\_FSP (компонент-b)

3 ACO\_DEV (компонент-b)

**Рисунок В.4 – Взаимодействие объединенных компонентов**

a) стрелки, входящие в «Зависимый компонент а» (т. е. А и В) = компонент ожидает реакции среды на запрос сервиса (произведенный зависимым компонентом)

b) выходящие от «Базового компонента b» стрелки (С и D) = интерфейсы сервисов и сервисов, предоставляемых базовым компонентом функциональной среде;

c) пунктирные стрелки =типы взаимодействий между парами интерфейсов;

d) другие стрелки (серого цвета) = взаимодействия, обозначенные в данном критерии.

Дальнейшее является упрощением, но объясняет, что следует принимать во внимание.

Для компонентов а («Зависимый компонент а») и b («Базовый компонент b»): стрелки, выходящие от ФБО-а, это сервисы, предоставляемые ФБО-а и таким образом являющиеся ИФБО(а), так же и выходящие от ФБО-b («С») являются ИФБО(Ь). Все они детализируются в соответствующих функциональных спецификациях. Компонент а запрашивает от среды сервисы: те, которые необходимы для ФБО(а) — помечены буквой «А», остальные (не относящиеся к ФБО-а) — «В».

Когда компонент а и компонент b объединяются, существуют четыре возможных комбинации {сервисов, требуемых компонентом а} и {сервисов, предоставляемых компонентом b }, показанные пунктирными стрелками (типы взаимодействий между интерфейсами). Любой такой набор может существовать для конкретной композиции:

a) ФБО-а нуждается в сервисах, предоставляемых ФБО-b («А» соединяется с «С») — тогда все достаточно просто: детализация «С» производится в функциональной спецификации компонента b. При этом все взаимодействия следует определить в функциональных спецификациях компонента b;

b) не-ФБО-а нуждается в сервисах, предоставляемых ФБО-b («В» соединяется с «С»). Это тоже довольно простой случай (опять же, детализация «С» приводится в функциональных спецификациях компонента b), но имеющий небольшое значение;

c) не-ФБО-а нуждается в сервисах, предоставляемых не-ФБО-b («В» соединяется «D») — нет детализации D, но нет и включения безопасности в использование этих интерфейсов, поэтому их необязательно рассматривать при оценке, хотя они являются результатом интеграции, проведенной разработчиком;

d) ФБО-а нуждается в сервисах, предоставляемых не-ФБО-b («А» соединяется с «D») — это происходит, когда у компонента а и компонента b разные понятия «сервиса безопасности». Возможно, компонент b предъявляет требования идентификации и аутентификации (которых нет среди ФТБ класса FIA в его ЗБ), но для компонента а необходима аутентификация, предоставляемая его средой. Нет доступной детализированной информации об интерфейсах «D» (они не относятся к ИФБО(b), потому и не включаются в функциональную спецификацию компонента b).

Замечание: если существует взаимодействие, описанное выше в подпункте d), тогда ФБО составного ОО будет представлять собой ФБО-а + ФБО-b + не-ФБО-b. В иных случаях ФБО составного ОО будет ФБО-а + ФБО- b.

Типы взаимодействий 2 и 4 рисунка В.4 не связаны напрямую с оценкой составного ОО.

Типы взаимодействий 1 и 3 будут рассматриваться при приложении различных семейств:

а) в семействе «Функциональная спецификация» (ADV\_FSP) для компонента b будут описываться взаимодействия С;

b) «Зависимости зависимых компонентов» (ACO\_REL) будет описывать взаимодействия А;

c) «Свидетельство разработки» (ACO\_DEV) будет описывать взаимодействия С типа 1 и взаимодействия D типа 3.

Типичный пример использования такой композиции — система управления базой данных (СУБД), которая зависит от операционной системы (ОС). В процессе оценки компонента СУБД будет проводиться оценка характеристик безопасности данной СУБД (на уровне строгости, требуемом компонентами доверия, используемыми при оценке): определение границы ФБО; оценка функциональной спецификации для определения того, описываются ли в ней должным образом интерфейсы сервисов и сервисов безопасности, предоставляемые ФБО; возможно приведение дополнительной информации по ФБО (по проекту, архитектуре, внутренней структуре), затем будет произведено тестирование ФБО, оценка аспектов жизненного цикла и руководств.

Однако оценка СУБД не требует свидетельств относительно зависимости СУБД от ОС. В ЗБ для СУБД будут перечислены предположения по 00 в подразделе «Предположения» и установлены цели безопасности ОС в подразделе «Среда функционирования». ЗБ для СУБД может даже приписывать эти цели всей среде функционирования в терминах ФТБ для ОС. Однако для ОС не предусмотрена спецификация, которая отражала бы детали функциональной спецификации, описание архитектуры или другие свидетельства класса ADV, как для СУБД. Эту информацию представит семейство «Зависимости зависимых компонентов» (ACO\_REL).

В указанном семействе описываются интерфейсы зависимых ОО, которые вызывают базовые компоненты для предоставления сервисов. Это такие интерфейсы, на запросы которых отвечает базовый компонент. Описания интерфейсов представляется с точки зрения зависимого компонента.

Семейство «Свидетельство разработки» (ACO\_DEV) описывает интерфейсы, предоставляемые базовым компонентом, который отвечает на запросы зависимых компонентов. Такие интерфейсы прослеживаются к значимым интерфейсам зависимых компонентов, которые определяются в относящейся к ним информации. (Полнота прослеживания, т.е. описывают ли интерфейсы базового компонента все интерфейсы зависимого компонента, удостоверяется не этим семейством, а семейством ACO\_COR «Обоснование композиции». На более высоких уровнях ACO\_DEV описываются подсистемы, предоставляющие эти интерфейсы.

Для любых интерфейсов, требуемых зависимым компонентом, которые не были описаны в базовым компоненте, приводится обоснование в «Обосновании композиции» (ACO\_COR). В этом же обосновании приводится информация о том, рассматривались ли интерфейсы базового компонента, на которые полагается зависимый компонент, при проведении оценки базового компонента. Для каждого интерфейса, не рассмотренного при оценке базового компонента, приводится обоснование влияния использования этого интерфейса на ФБО базового компонента.

**Приложение С**

*(информационное)*

**Перекрестные ссылки между компонентами доверия**

Зависимости между компонентами, приведенные в разделах 8 - 18, являются прямыми зависимостями между компонентами доверия.

Приведенные ниже таблицы зависимостей для компонентов доверия показывают их прямые и косвенные зависимости. Все компоненты, от которых зависят какие-либо другие компоненты доверия, указываются в заголовках столбцов. Каждый компонент доверия указывается в заголовке какой-либо строки. Конкретное значение в ячейке таблицы указывает, требуется ли прямо (обозначено «X») или косвенно (обозначено « – ») компонент, указанный в заголовке столбца, для компонента, указанного в заголовке строки. Если в ячейке никаких символов нет, то компонент, указанный в заголовке строки, не зависит от компонента, указанного в заголовке столбца.

**Таблица С.1 –** **Таблица зависимостей для класса AGD: Руководящие документы**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ADV** | **ADV\_ FSP.1** | **ADV\_ FSP.2** | **ADV\_ FSP.3** | **ADV\_ FSP.4** | **ADV\_ FSP.5** | **ADV\_ FSP.6** | **ADV\_ IMP.1** | **ADV\_ TDS.1** | **ADV\_ TDS.3** | **ALC\_ CMC.5** | **ALC\_ CMS.1** | **ALC\_ DVS.2** | **ALC\_ LCD.1** | **ALC\_ TAT.1** |
| ADV\_ARC.1 | X | **–** |  |  |  |  |  | X |  |  |  |  |  |  |
| ADV\_ COMP.1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ADV\_FSP.1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ADV\_FSP.2 |  | **–** |  |  |  |  |  | X |  |  |  |  |  |  |
| ADV\_FSP.3 |  | **–** |  |  |  |  |  | X |  |  |  |  |  |  |
| ADV\_FSP.4 |  | **–** |  |  |  |  |  | X |  |  |  |  |  |  |
| ADV\_FSP.5 |  | **–** |  | **–** |  |  | X | X | **–** |  |  |  |  | **–** |
| ADV\_FSP.6 |  | **–** |  | **–** |  |  | X | X | **–** |  |  |  |  | **–** |
| ADV\_IMP.1 |  | **–** |  | **–** |  |  | **–** | **–** | X |  |  |  |  | X |
| ADV\_IMP.2 |  | **–** |  | **–** |  |  | **–** | **–** | X | X | **–** | **–** | **–** | X |
| ADV\_INT.1 |  | **–** |  | **–** |  |  | X | **–** | X |  |  |  |  | X |
| ADV\_INT.2 |  | **–** |  | **–** |  |  | X | **–** | X |  |  |  |  | X |
| ADV\_INT.3 |  | **–** |  | **–** |  |  | X | **–** | X |  |  |  |  | X |
| ADV\_SPM.1 |  |  |  | X |  |  |  | **–** |  |  |  |  |  |  |
| ADV\_TDS.1 |  | X |  |  |  |  |  | **–** |  |  |  |  |  |  |
| ADV\_TDS.2 |  | **–** | X |  |  |  |  | **–** |  |  |  |  |  |  |
| ADV\_TDS.3 |  | **–** |  | X |  |  |  | **–** |  |  |  |  |  |  |
| ADV\_TDS.4 |  | **–** |  | **–** | X |  | **–** | **–** | **–** |  |  |  |  | **–** |
| ADV\_TDS.5 |  | **–** |  | **–** | X |  | **–** | **–** | **–** |  |  |  |  | **–** |
| ADV\_TDS.6 |  | **–** |  | **–** |  | X | **–** | **–** | **–** |  |  |  |  | **–** |

**Таблица С.2 – Таблица зависимостей для класса AGD: Руководящие документы**

|  |  |
| --- | --- |
| **AGD** | **ADV\_FSP.1** |
| AGD\_OPE.1 | X |
| AGD\_PRE.1 |  |

**Таблица С.3 – Таблица зависимостей для класса ALC: Поддержка жизненного цикла**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ALC** | **ADV\_ FSP.2** | **ADV\_ FSP.4** | **ADV\_ IMP.1** | **ADV\_ TDS.1** | **ADV\_ TDS.3** | **ALC\_**  **CMS.1** | **ALC\_ CMS.3** | **ALC\_ DVS.1** | **ALC\_ DVS.2** | **ALC\_ LCD.1** | **ALC\_ TAT.1** |
| ALC\_CMC.1 |  |  |  |  |  | X |  |  |  |  |  |
| ALC\_CMC.2 |  |  |  |  |  | X |  |  |  |  |  |
| ALC\_CMC.3 |  |  |  |  |  | X |  | X |  | X |  |
| ALC\_CMC.4 |  |  |  |  |  | X |  | X |  | X |  |
| ALC\_CMC.5 |  |  |  |  |  | X |  |  | X | X |  |
| ALC\_CMS.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_CMS.2 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_CMS.3 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_CMS.4 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_CMS.5 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_COMP.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_DEL.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_DVS.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_DVS.2 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_FLR.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_FLR.2 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_FLR.3 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_LCD.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_LCD.2 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_TAT.1 | **–** | **–** | X | **–** | **–** |  |  |  |  |  | **–** |
| ALC\_TAT.2 | **–** | **–** | X | **–** | **–** |  |  |  |  |  | **–** |
| ALC\_TAT.3 | **–** | **–** | X | **–** | **–** |  |  |  |  |  | **–** |
| ALC\_TDA.1 |  |  |  |  |  |  |  |  |  |  |  |
| ALC\_TDA.2 |  |  |  |  |  |  | X |  |  |  |  |
| ALC\_TDA.3 | **–** | **–** | X | **–** | **–** |  | X |  |  |  | X |

**Таблица С.4 – Таблица зависимостей для класса APE: оценка профиля защиты**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **APE** | **APE\_ ECD.1** | **APE\_ INT.1** | **APE\_**  **OBJ.2** | **APE\_**  **REQ.1** | **APE\_ SPD.1** |
| APE\_CCL.1 | X | X |  | X |  |
| APE\_ECD.1 |  |  |  |  |  |
| APE\_INT.1 |  |  |  |  |  |
| APE\_OBJ.1 |  |  |  |  |  |
| APE\_OBJ.2 |  |  |  |  | X |
| APE\_REQ.1 | X |  |  |  |  |
| APE\_REQ.2 | X |  | X |  | – |
| APE\_SPD.1 |  |  |  |  |  |

**Таблица С.5 – Таблица зависимостей для класса ACE: оценка конфигурации PP**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ACE** | **ACE\_ CCL.1** | **ACE\_ ECD.1** | **ACE\_ INT.1** | **ACE\_ MCO.1** | **ACE**  **—**  **OBJ.1** | **ACE\_**  **OBJ.2** | **ACE\_**  **REQ.1** | **ACE\_**  **REQ.2** | **ACE\_ SPD.1** | **APE\_ ECD.1** |
| ACE\_CCL.1 |  | X | X |  | – |  | O | O | – | – |
| ACE\_CCO.1 | X | X | X | X | O | O | O | O | X | – |
| ACE\_ECD.1 |  |  |  |  |  |  |  |  |  |  |
| ACEJNT.1 |  |  |  |  |  |  |  |  |  |  |
| ACE\_MCO.1 |  | – | X |  | O | O | O | O | X | – |
| ACE\_OBJ.1 |  |  |  |  |  |  |  |  |  |  |
| ACE\_OBJ.2 |  |  |  |  |  |  |  |  | X |  |
| ACE\_REQ.1 |  |  |  |  |  |  |  |  | X | X |
| ACE\_REQ.2 |  | X |  |  |  | X |  |  |  |  |
| ACE\_SPD.1 |  |  |  |  |  |  |  |  |  |  |

**Таблица С.6 – Таблица зависимостей для класса ASE: оценка цели**

**безопасности (ST)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ASE** | **ADV\_**  **ARC.1** | **ADV\_**  **FSP.1** | **ADV\_ FSP.2** | **ADV\_ TDS.1** | **ASE\_ ECD.1** | **ASE\_ INT.1** | **ASE\_**  **OBJ.2** | **ASE\_**  **REQ.1** | **ASE\_ SPD.1** |
| ASE\_CCL.1 |  |  |  |  | X | X |  | X |  |
| ASE\_COMP.1 |  |  |  |  |  |  |  |  |  |
| ASE\_ECD.1 |  |  |  |  |  |  |  |  |  |
| ASE\_INT.1 |  |  |  |  |  |  |  |  |  |
| ASE\_OBJ.1 |  |  |  |  |  |  |  |  |  |
| ASE\_OBJ.2 |  |  |  |  |  |  |  |  | X |
| ASE\_REQ.1 |  |  |  |  | X |  |  |  |  |
| ASE\_REQ.2 |  |  |  |  | X |  | X |  | – |
| ASE\_SPD.1 |  |  |  |  |  |  |  |  |  |
| ASE\_TSS.1 |  | X |  |  | – | X |  | X |  |
| ASE\_TSS.2 | X | – | – | – | – | X |  | X |  |

**Таблица С.7 – Таблица зависимостей для класса ATE: тестирование**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ATE** | **ADV\_ ARC.1** | **ADV\_ FSP.1** | **ADV\_ FSP.2** | **ADV\_ FSP.3** | **ADV\_ FSP.4** | **ADV\_ FSP.5** | **ADV\_ IMP.1** | **ADV\_ TDS.1** | **ADV\_ TDS.2** | **ADV\_ TDS.3** | **ADV\_ TDS.4** | **AGD\_ OPE.1** | **AGD\_ PRE.1** | **ALC TAT.1** | **ATE COV.1** | **ATE\_ FUN.1** |
| ATE\_COMP.1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ATE\_COV.1 |  |  | X |  |  |  |  | – |  |  |  |  |  |  | – | X |
| ATE\_COV.2 |  |  | X |  |  |  |  | – |  |  |  |  |  |  | – | X |
| ATE\_COV.3 |  |  | X |  |  |  |  | – |  |  |  |  |  |  | – | X |
| ATE\_DPT.1 | X | – | – | – |  |  |  | – | X |  |  |  |  |  | – | X |
| ATE\_DPT.2 | X | – | – |  | – |  |  | – |  | X |  |  |  |  | – | X |
| ATE\_DPT.3 | X | – | – |  | – | – | – | – |  | – | X |  |  | – | – | X |
| ATE\_DPT.4 | X | – | – |  | – | – | X | – |  | – | X |  |  | – | – | X |
| ATE\_FUN.1 |  |  | – |  |  |  |  | – |  |  |  |  |  |  | X | – |
| *Продолжение таблицы С.7* | | | | | | | | | | | | | | | | |
| **ATE** | **ADV\_ ARC.1** | **ADV\_ FSP.1** | **ADV\_ FSP.2** | **ADV\_ FSP.3** | **ADV\_ FSP.4** | **ADV\_ FSP.5** | **ADV\_ IMP.1** | **ADV\_ TDS.1** | **ADV\_ TDS.2** | **ADV\_ TDS.3** | **ADV\_ TDS.4** | **AGD\_ OPE.1** | **AGD\_ PRE.1** | **ALC TAT.1** | **ATE COV.1** | **ATE\_ FUN.1** |
| ATE\_FUN.2 |  |  | – |  |  |  |  | – |  |  |  |  |  |  | X | – |
| ATE\_IND.1 |  | X |  |  |  |  |  |  |  |  |  | X | X |  |  |  |
| ATE\_IND.2 |  | – | X |  |  |  |  | – |  |  |  | X | X |  | X | X |
| ATE\_IND.3 |  | – | – |  | X |  |  | – |  |  |  | X | X |  | X | X |

**Таблица С.8 – Таблица зависимостей для класса AVA: анализ уязвимости**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **AVA** | **ADV** | **ADV** | **ADV** | **ADV** | **ADV** | **ADV** | **ADV** | **ADV** | **ADV** | **AGD** | **AGD** | **ALC** | **ATE** | **ATE** | **ATE** |
|  | **ARC.1** | **FSP.1** | **FSP.2** | **FSP.3** | **FSP.4** | **IMP.1** | **TDS.1** | **TDS.2** | **TDS.3** | **OPE.1** | **PRE.1** | **TAT.1** | **COV.1** | **DPT.1** | **FUN.1** |
| AVA\_COMP.1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| AVA\_VAN.1 |  | X |  |  |  |  |  |  |  | X | X |  |  |  |  |
| AVA\_VAN.2 | X | – | X |  |  |  | X |  |  | X | X |  |  |  |  |
| AVA\_VAN.3 | X | – | – | – | X | X | – | – | X | X | X | – | – | X | – |
| AVA\_VAN.4 | X | – | – | – | X | X | – | – | X | X | X | – | – | X | – |
| AVA\_VAN.5 | X | – | – | – | X | X | – | – | X | X | X | – | – | X | – |

**Таблица С.9 – Таблица зависимостей для класса АСО: Композиция**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ACO** | **ACO\_ DEV.1** | **ACO\_ DEV.2** | **ACO\_ DEV.3** | **ACO\_ REL.1** | **ACO\_ REL.2** | **ALC\_**  **CMC.1** | **ALC\_**  **CMS.1** |
| ACO\_COR.1 | X |  |  | X |  | X | – |
| ACO\_CTT.1 | X |  |  | X |  |  |  |
| ACO\_CTT.2 |  | X |  | – | X |  |  |
| ACO\_DEV.1 |  |  |  | X |  |  |  |
| ACO\_DEV.2 |  |  |  | X |  |  |  |
| ACO\_DEV.3 |  |  |  |  | X |  |  |
| ACO\_REL.1 |  |  |  |  |  |  |  |
| ACO\_REL.2 |  |  |  |  |  |  |  |
| ACO\_VUL.1 | X |  |  | – |  |  |  |
| ACO\_VUL.2 |  | X |  | – |  |  |  |
| ACO\_VUL.3 |  |  | X |  | – |  |  |

## **Библиография**

[1] ISO 10007:2017 Quality management. Guidelines for configuration management (Менеджмент качества. Руководящие указания по семействам требований управления конфигурацией).

## **Приложение В.А**

*(информационное)*

**Таблица В.А.1 – Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

|  |  |  |
| --- | --- | --- |
| **Обозначение и наименование международного, регионального стандартов, стандарта иностранного государства** | **Степень соответствия** | **Обозначение и наименование национального стандарта, межгосударственного стандарта** |
| ISO/IEC 15408-1:2022 Information security. Evaluation criteria for IT security. Part 1: Introduction and general model (Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель) | IDT | СТ РК ISO/IEC 15408-1\* «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»\* |
| ISO/IEC 15408-2-2022 Information security. Evaluation criteria for IT security. Part 2: Security functional components (Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования) | IDT | СТ РК ISO/IEC 15408-2\* «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования»\* |
| \_\_\_\_\_\_\_\_\_\_\_\_\_  \* на стадии разработки | | |

**Таблица В.А.2 – Сведения о соответствии стандартов, ссылочным международным, региональным стандартам, стандартам иностранных государств другого года издания**

|  |  |  |  |
| --- | --- | --- | --- |
| **Обозначение и наименование ссылочного международного, регионального стандартов, стандартов иностранного государств документа** | **Обозначение и наименование международного, регионального стандартов, стандартов иностранного государств** | **Степень соответствия** | **Обозначение и наименование национального стандарта, межгосударственного стандарта** |
| ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Methodology for IT security evaluation | ISO/IEC 18045:2008 (Е) Information technology. Security techniques. Methodology for IT security evaluation (Технологии информационные. Методы защиты. Методология оценки защиты информационных технологий) | IDT | СТ РК ИСО/МЭК 18045-2009 «Технологии информационные. Методы защиты. Методология оценки защиты информационных технологий» |
| ISO/IEC IEEE 24765-2017 Systems and software engineering. Vocabulary | ISO/IEC/IEEE 23026:2015 Systems and software engineering. Engineering and management of websites for systems, software, and services information (Разработка систем и программного обеспечения. Разработка и администрирование веб-сайтов для систем, программного обеспечения и информации о службах) | IDT | СТ РК ISO/IEC/IEEE 23026-2017 «Разработка систем и программного обеспечения. Разработка и администрирование веб-сайтов для систем, программного обеспечения и информации о службах» |

**МКС 35.030 (IDT)**

**Ключевые слова:** модуль, структура класса доверия, компоненты, безопасность, архитектурный проект.

**МКС 35.030 (IDT)**

**Ключевые слова:** модуль, структура класса доверия, компоненты, безопасность, архитектурный проект.

**Разработчик:**

**РГП на ПХВ «Казахстанский институт стандартизации и метрологии»**

|  |  |
| --- | --- |
| Заместитель  Генерального директора | И. Хамитов |
| Руководитель  Департамента разработки стандартов | А. Сопбеков |
| Ведущий специалист | Ж. Туяков |