ГОСТЕХКОМИССИЯ РОССИИ

РУКОВОДЯЩИЙ ДОКУМЕНТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Критерии оценки безопасности информационных технологий

Часть 3. Требования доверия к безопасности

2002

СОДЕРЖАНИЕ

1 Область применения

Эта часть ОК определяет требования доверия к безопасности и включает в себя оценочные уровни доверия (ОУД), определяющие шкалу для измерения доверия, собственно компоненты доверия, из которых составлены уровни доверия, и критерии для оценки ПЗ и ЗБ.

1.1 Структура

Часть 3 ОК состоит из следующих разделов:

1 – введение и парадигма;

2 – структура представления классов, семейств и компонентов доверия, оценочных уровней доверия и их взаимосвязь, а также краткая характеристика классов и семейств доверия, представленных в разделах 8–14;

3–5 – краткое введение в критерии оценки ПЗ и ЗБ, сопровождаемое детализированными объяснениями семейств и компонентов, которые применяют для этих оценок;

6 – детализированные определения оценочных уровней доверия;

7 – краткое введение в классы доверия;

8–14 – детализированные определения классов доверия;

15–16 – краткое введение в критерии оценки поддержки доверия с детализированными определениями применяемых семейств и компонентов.

Приложение А содержит сводку зависимостей между компонентами доверия.

Приложение Б содержит перекрестные ссылки между ОУД и компонентами доверия.

1.2 Парадигма доверия

Цель данного подраздела состоит в изложении основных принципов и подходов к установлению доверия к безопасности. Данный подраздел позволит читателю понять логику построения требований доверия в ОК.

1.2.1 Основные принципы ОК

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

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

1.2.2 Подход к доверию

Основная концепция ОК – обеспечение доверия, основанное на оценке (активном исследовании) продукта или системы ИТ, которым предполагается доверять. Оценка была традиционным способом обеспечения доверия и являлась основой предшествующих критериев оценки. Для согласования с существующими подходами в ОК принят тот же самый основной принцип. ОК предполагают, что проверку правильности документации и разработанного продукта или системы ИТ будут проводить опытные оценщики, уделяя особое внимание области, глубине и строгости оценки.

ОК не отрицают и при этом не комментируют относительные достоинства других способов получения доверия. Продолжаются исследования альтернативных путей достижения доверия. Если в результате этих исследований будут выявлены другие отработанные альтернативные подходы, то они могут в дальнейшем быть включены в ОК, которые структурно организованы так, что предусматривают такую возможность.

1.2.2.1 Значимость уязвимостей

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

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

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

а) устранены, т.е. следует предпринять активные действия для выявления, а затем удаления или нейтрализации всех уязвимостей, которые могут проявиться;

б) минимизированы, т.е. следует предпринять активные действия для уменьшения до допустимого остаточного уровня возможного ущерба от любого проявления уязвимостей;

в) отслежены, т.е. следует предпринять активные действия для обнаружения любой попытки использовать оставшиеся уязвимости с тем, чтобы ограничить ущерб.

1.2.2.2 Причины уязвимостей

Уязвимости могут возникать из-за недостатков:

а) требований, т.е. продукт или система ИТ могут обладать требуемыми от них функциями и свойствами, но все же содержать уязвимости, которые делают их непригодными или неэффективными в части безопасности;

б) проектирования, т.е. продукт или система ИТ не отвечают спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

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

1.2.2.3 Доверие в ОК

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

1.2.2.4 Доверие через оценку

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

а) анализ и проверку процессов и процедур;

б) проверку, что процессы и процедуры действительно применяются;

в) анализ соответствия между представлениями проекта ОО;

г) анализ соответствия каждого представления проекта ОО требованиям;

д) верификацию доказательств;

е) анализ руководств;

ж) анализ разработанных функциональных тестов и полученных результатов;

и) независимое функциональное тестирование;

к) анализ уязвимостей, включающий предположения о недостатках;

л) тестирование проникновения.

1.2.3 Шкала оценки доверия в ОК

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

а) области охвата, т.е. увеличении рассматриваемой части продукта или системы ИТ;

б) глубине, т.е. детализации рассматриваемых проектных материалов и реализации;

в) строгости, т.е. применении более структурированного и формального подхода.

2 Требования доверия к безопасности

2.1 Структуры

Следующие подразделы описывают конструкции, используемые в представлении классов, семейств и компонентов доверия, оценочных уровней доверия (ОУД), и их взаимосвязь.

На рисунке 2.1 показаны требования доверия, определенные в части 3 ОК. Наиболее общую совокупность требований доверия называют классом. Каждый класс содержит семейства доверия, которые разделены на компоненты доверия, содержащие, в свою очередь, элементы доверия. Классы и семейства используют для обеспечения таксономии классифицируемых требований доверия, в то время как компоненты применяют непосредственно для спецификации требований доверия в ПЗ/ЗБ.

2.1.1 Структура класса

Рисунок 2.1 иллюстрирует структуру класса доверия.

2.1.1.1 Имя класса

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

Представлена также уникальная краткая форма имени класса доверия. Она является основным средством для ссылки на класс доверия. Принятое условное обозначение включает в себя букву "А", за которой следуют еще две буквы латинского алфавита, относящиеся к имени класса.

2.1.1.2 Представление класса

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

2.1.1.3 Семейства доверия

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

Рисунок 2.1 – Иерархическая структура представления требований доверия: класс-семейство-компонент-элемент

2.1.2 Структура семейства доверия

Рисунок 2.1 иллюстрирует структуру семейства доверия.

2.1.2.1 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.

2.1.2.2 Цели

Подраздел целей семейства доверия представляет назначение семейства доверия.

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

2.1.2.3 Ранжирование компонентов

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

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

2.1.2.4 Замечания по применению

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

2.1.2.5 Компоненты доверия

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

2.1.3 Структура компонента доверия

Рисунок 2.2 иллюстрирует структуру компонента доверия.

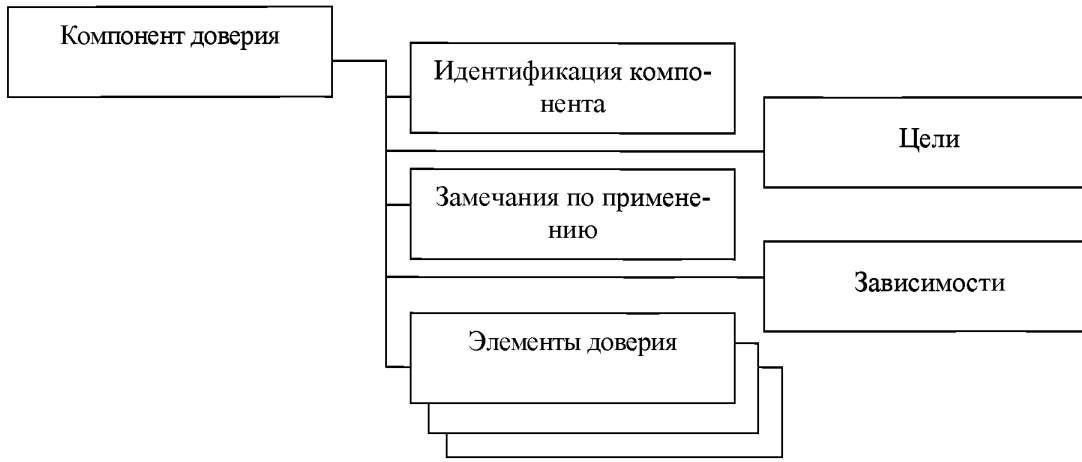


Рисунок 2.2 – Структура компонента доверия

Связь между компонентами внутри семейства показана с использованием соглашения о шрифтовом выделении. Для частей требований, которые являются новыми, расширенными или модифицированными по сравнению с требованиями предыдущего по иерархии компонента, применен полужирный шрифт. Такое же соглашение о шрифтовом выделении использовано и для зависимостей.

2.1.3.1 Идентификация компонента

Подраздел идентификации 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.

2.1.3.2 Цели

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

2.1.3.3 Замечания по применению

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

2.1.3.4 Зависимости

Зависимости среди компонентов доверия возникают, когда компонент не самодостаточен, а предполагает присутствие другого компонента.

Для каждого компонента доверия приведен полный список зависимостей от других компонентов доверия. При отсутствии у компонента идентифицированных зависимостей вместо списка указано: "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.

2.1.3.5 Элементы доверия

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

Каждый элемент доверия принадлежит к одному из трех типов.

а) *Элементы действий разработчика,* определяющие действия, которые должны выполняться разработчиком. Этот набор действий далее уточняется доказательным материалом, упоминаемым в следующем наборе элементов. Требования к действиям разработчика обозначены буквой "D" после номера элемента.

б) *Элементы содержания и представления свидетельств,* определяющие требуемые свидетельства и отражаемую в них информацию. Требования к содержанию и представлению свидетельств обозначены буквой "C" после номера элемента.

в) *Элементы действий оценщика,* определяющие действия, которые должны выполняться оценщиком. Этот набор действий непосредственно включает в себя подтверждение того, что требования, предписанные элементами содержания и представления свидетельств, выполнены, а также конкретные действия и анализ, выполняемые в дополнение к уже проведенным разработчиком. Должны также выполняться не указанные явно действия оценщика, необходимые вследствие элементов действий разработчика, но не охваченные в требованиях к содержанию и представлению свидетельств. Требования к действиям оценщика обозначены буквой "E" после номера элемента.

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

Действия оценщика определяют его ответственность по двум аспектам. Первый аспект – проверка правильности ПЗ/ЗБ в соответствии с требованиями классов APE/ASE из

разделов 4 и 5. Второй аспект – верификация соответствия ОО его функциональным требованиям и требованиям доверия. Демонстрируя, что ПЗ/ЗБ правильны, и их требования выполняются ОО, оценщик может предоставить основание для уверенности в том, что ОО будет отвечать поставленным целям безопасности.

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

2.1.4 Элементы доверия

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

В тексте элементов использованы, как правило, термины, имеющие обычное словарное значение, которые не могут привести к неоднозначному толкованию требований.

В отличие от функциональных элементов из части 2 ОК к элементам доверия из части 3 ОК не применимы операции назначения и выбора; однако, при необходимости, допустимо применение операции уточнения.

2.1.5 Структура ОУД

Рисунок 2.3 иллюстрирует ОУД и их структуру, определенную в части 3 ОК. Компоненты доверия, содержание которых показано на рисунке, включены в ОУД посредством ссылок на компоненты, приведенные в части 3 ОК.

2.1.5.1 Имя ОУД

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

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

2.1.5.2 Цели

В подразделе целей ОУД приведено назначение ОУД.

2.1.5.3 Замечания по применению

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

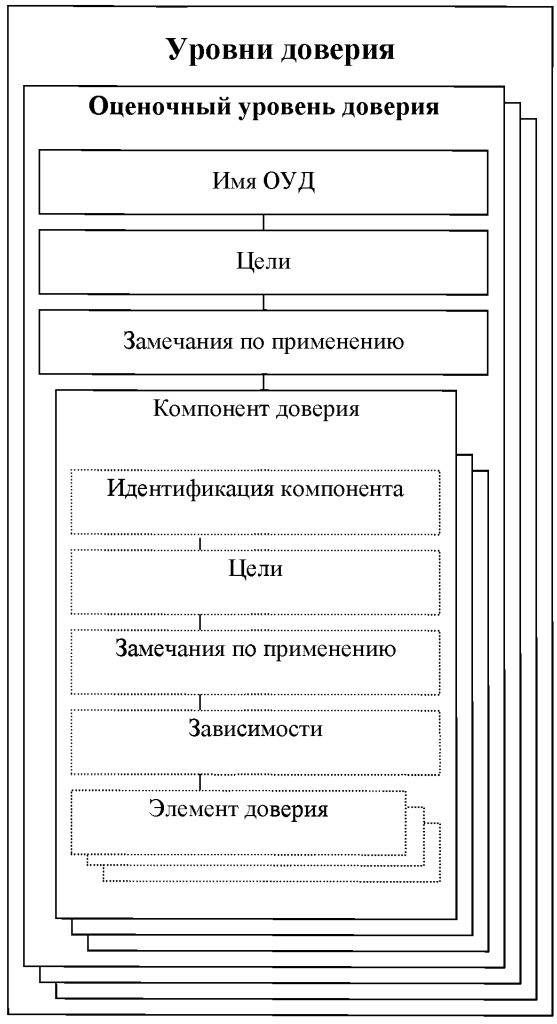


Рисунок 2.3 – Структура ОУД

2.1.5.4 Компоненты доверия

Для каждого ОУД выбран набор компонентов доверия.

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

а) включением дополнительных компонентов доверия из других семейств доверия;

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

2.1.6 Связь между требованиями и уровнями доверия

Рисунок 2.4 иллюстрирует связь между требованиями и уровнями доверия, определенными в части 3 ОК. Компоненты доверия состоят из элементов, но последние не могут

по отдельности быть включены в уровни доверия. Стрелка на рисунке отображает ссылку в ОУД на компонент доверия внутри класса, где он определен.

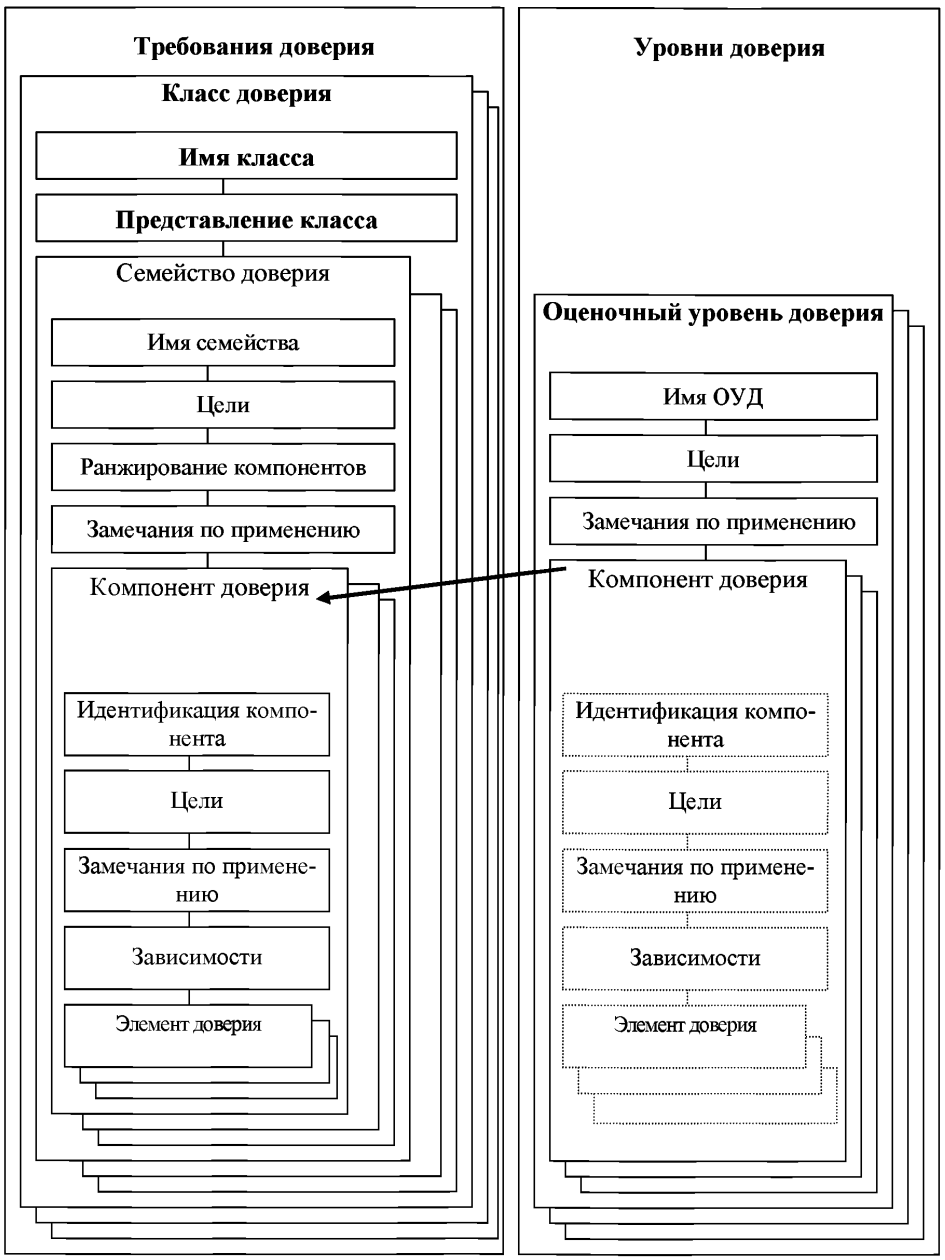


Рисунок 2.4 – Связь требований и уровня доверия

2.2 Классификация компонентов

Часть 3 ОК содержит классы семейств и компонентов, которые сгруппированы на основе, связанной с доверием. В начале каждого класса представлена диаграмма, которая указывает семейства в классе и компоненты в каждом семействе.

На рисунке 2.5 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 части 3 ОК – линейно иерархичные, хотя линейность не обязательна для семейств доверия, которые могут быть добавлены в дальнейшем.

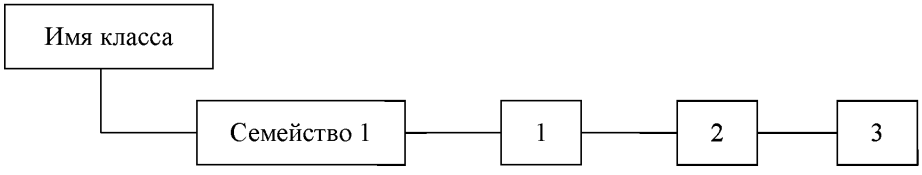


Рисунок 2.5 – Образец декомпозиции класса

2.3 Структура класса критериев оценки профиля защиты и задания по безопасности

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

В таблицах 3.1–3.4 приведены названия каждого из классов APE и ASE, составляющих их семейств и их краткие имена. Содержание разделов ПЗ, рассматриваемых в семействах класса APE, представлено в части 1 ОК, приложение Б, подразделы Б.2.2–Б.2.6, а разделов ЗБ, рассматриваемых в семействах класса ASE, – в части 1 ОК, приложение В, подразделы В.2.2–В.2.8.

2.4 Использование терминов в части 3 ОК

В части 3 ОК определенным образом используются термины, список которых приведен ниже. Они не включены в глоссарий ОК (раздел 2 части 1 ОК), потому что являются общеупотребительными терминами, и их использование, хотя и ограничено приведенными разъяснениями, согласуется со словарными определениями. Однако именно такое толкование терминов применялось при разработке части 3 ОК, и поэтому оно полезно для понимания. В скобках приведены эквиваленты терминов на английском языке.

верифицировать(verify): Аналогичен термину "подтверждать" ("confirm"), но имеет более глубокий смысл. При использовании в контексте действий оценщика указывает, что требуются независимые усилия оценщика.

взаимно поддерживающие (mutually supportive): Описывает взаимосвязь в группе сущностей, указывая, что последние обладают некоторыми свойствами, которые не находятся в противоречии со свойствами других сущностей и могут способствовать выполнению другими сущностями их задач. Нет необходимости определять, что каждая из рас-

сматриваемых отдельных сущностей непосредственно поддерживает другие сущности в этой группе; достаточно, если сделано обобщенное заключение.

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

делать (независимое) заключение (determine): Требуется независимый анализ для достижения конкретного заключения. Термин отличается от "подтверждать"("confirm") или "верифицировать"("verify"), так как последние подразумевают, что требует проверки анализ, проведенный ранее, в то время как "делать (независимое) заключение" подразумевает совершенно независимый анализ, обычно при отсутствии любого предшествующего анализа.

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

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

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

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

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

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

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

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

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

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

проверять (check): Аналогичен, но менее строг, чем "подтверждать"("confirm") или "верифицировать"("verify"). Требует, чтобы оценщиком было сделано оперативное заключение, возможно лишь с поверхностным анализом или вообще без него.

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

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

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

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

2.5 Классификация доверия

Классы и семейства доверия, а также их краткие имена приведены в таблице 2.1.

2.6 Краткий обзор классов и семейств доверия

Ниже приведены краткие характеристики классов и семейств доверия из разделов 8-14.

2.6.1 Класс ACM: Управление конфигурацией

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

Таблица 2.1 – Семейства доверия

Класс доверия	Семейство доверия	Краткое имя
ACM – Управление конфигурацией	Автоматизация УК	ACM_AUT
	Возможности УК	ACM_CAP
	Область УК	ACM_SCP
ADO – Поставка и эксплуатация	Поставка	ADO_DEL
	Установка, генерация и запуск	ADO_IGS
ADV – Разработка	Функциональная спецификация	ADV_FSP
	Проект верхнего уровня	ADV_HLD
	Представление реализации	ADV_IMP
	Внутренняя структура ФБО	ADV_INT
	Проект нижнего уровня	ADV_LLD
	Соответствие представлений	ADV_RCR
	Моделирование политики безопасности	ADV_SPM
AGD – Руководства	Руководство администратора	AGD_ADM
	Руководство пользователя	AGD_USR
ALC – Поддержка жизненного цикла	Безопасность разработки	ALC_DVS
	Устранение недостатков	ALC_FLR
	Определение жизненного цикла	ALC_LCD
	Инструментальные средства и методы	ALC_TAT
ATE – Тестирование	Покрытие	ATE_COV
	Глубина	ATE_DPT
	Функциональное тестирование	ATE_FUN
	Независимое тестирование	ATE_IND
AVA – Оценка уязвимостей	Анализ скрытых каналов	AVA_CCA
	Неправильное применение	AVA_MSU
	Стойкость функций безопасности ОО	AVA_SOF
	Анализ уязвимостей	AVA_VLA

2.6.1.1 Автоматизация УК (ACM_AUT)

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

2.6.1.2 Возможности УК (ACM_CAP)

Семейство "Возможности управления конфигурацией" определяет характеристики системы управления конфигурацией.

2.6.1.3 Область УК (ACM_SCP)

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

2.6.2 Класс ADO. Поставка и эксплуатация

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

2.6.2.1 Поставка (ADO_DEL)

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

2.6.2.2 Установка, генерация и запуск (ADO_IGS)

Семейство "Установка, генерация и запуск" предусматривает, чтобы копия ОО была конфигурирована и активизирована администратором так, чтобы показать те же самые свойства защиты, что и у оригинала ОО. Процедуры установки, генерации и запуска предоставляют уверенность в том, что администратор будет осведомлен о параметрах конфигурации ОО и о том, как они способны повлиять на ФБО.

2.6.3 Класс ADV. Разработка

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

2.6.3.1 Функциональная спецификация (ADV_FSP)

Функциональная спецификация описывает ФБО, и необходимо, чтобы она была полным и точным отображением функциональных требований безопасности ОО. Функциональная спецификация также детализирует внешний интерфейс ОО. Предполагают, что пользователи ОО взаимодействуют с ФБО через этот интерфейс.

2.6.3.2 Проект верхнего уровня (ADV_HLD)

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

2.6.3.3 Представление реализации (ADV_IMP)

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

2.6.3.4 Внутренняя структура ФБО (ADV_INT)

Требования к внутренней структуре ФБО определяют необходимое внутреннее структурирование ФБО.

2.6.3.5 Проект нижнего уровня (ADV_LLD)

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

2.6.3.6 Соответствие представлений (ADV_RCR)

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

2.6.3.7 Моделирование политики безопасности (ADV_SPM)

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

2.6.4 Класс AGD. Руководства

Класс доверия AGD определяет требования, направленные на обеспечение понятности, достаточности и законченности эксплуатационной документации, представляемой разработчиком. Эта документация, которая содержит две категории информации (для пользователей и администраторов), является важным фактором безопасной эксплуатации ОО.

2.6.4.1 Руководство администратора (AGD_ADM)

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

2.6.4.2 Руководство пользователя (AGD_USR)

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

последовательно и действенно защищать свою информацию. Во-вторых, требуется разъяснить роль пользователя в поддержании безопасности ОО.

2.6.5 Класс ALC. Поддержка жизненного цикла

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

2.6.5.1 Безопасность разработки (ALC_DVS)

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

2.6.5.2 Устранение недостатков (ALC_FLR)

Семейство "Устранение недостатков" обеспечивает, чтобы недостатки, обнаруженные потребителями ОО, отслеживались и исправлялись, пока ОО сопровождается разработчиком. Несмотря на то, что при оценке ОО не может быть принято решение о потенциальном соответствии требованиям устранения недостатков, можно оценить политики и процедуры, которые разработчик предусмотрел для выявления и устранения недостатков и распространения исправлений потребителям.

2.6.5.3 Определение жизненного цикла (ALC_LCD)

Семейство "Определение жизненного цикла" устанавливает, что технология разработки, используемая разработчиком для создания ОО, включает в себя положения и действия, указанные в требованиях к процессу разработки и поддержке эксплуатации. Уверенность в соответствии ОО требованиям больше, когда анализ безопасности и подготовка свидетельств осуществляются на регулярной основе как неотъемлемая часть процесса разработки и поддержки эксплуатации. В задачи этого семейства не входит предопределение какого-либо конкретного процесса разработки.

2.6.5.4 Инструментальные средства и методы (ALC_TAT)

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

2.6.6 Класс ATE. Тестирование

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

2.6.6.1 Покрытие (ATE_COV)

Семейство "Покрытие" имеет дело с полнотой функциональных тестов, выполненных разработчиком для ОО. Оно связано со степенью тестирования функций безопасности ОО.

2.6.6.2 Глубина (ATE_DPT)

Семейство "Глубина" имеет дело с уровнем детализации, на котором разработчик проверяет ОО. Тестирование функций безопасности основано на увеличивающейся глубине информации, получаемой из анализа представлений ФБО.

2.6.6.3 Функциональное тестирование (ATE_FUN)

Семейство "Функциональное тестирование" устанавливает, что ФБО действительно демонстрируют свойства, необходимые для удовлетворения требований своего ЗБ. Функциональное тестирование обеспечивает доверие, что ФБО удовлетворяют, по меньшей мере, требованиям выбранных функциональных компонентов. Однако функциональные тесты не устанавливают, что ФБО не выполняют больше, чем от них ожидается. Это семейство сосредоточено на функциональном тестировании, выполняемом разработчиком.

2.6.6.4 Независимое тестирование (ATE_IND)

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

2.6.7 Класс AVA. Оценка уязвимостей

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

2.6.7.1 Анализ скрытых каналов (AVA_CCA)

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

2.6.7.2 Неправильное применение (AVA_MSU)

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

2.6.7.3 Стойкость функций безопасности ОО (AVA_SOF)

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

2.6.7.4 Анализ уязвимостей (AVA_VLA)

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

1) полноты ФБО (противостоят ли ФБО всем ожидаемым угрозам?);
2) зависимостей между всеми функциями безопасности.

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

2.7 Классификация поддержки

Требования по поддержке доверия, трактуемые как класс доверия, представлены с использованием структуры класса, определенной выше.

Семейства поддержки доверия и их краткие имена приведены в таблице 2.2.

Таблица 2.2 – Декомпозиция класса AMA "Поддержка доверия"

Класс	Семейство доверия	Краткое имя
AMA – Поддержка доверия	План поддержки доверия	AMA_AMP
	Отчет о категорировании компонентов ОО	AMA_CAT
	Свидетельство поддержки доверия	AMA_EVD
	Анализ влияния на безопасность	AMA_SIA

2.8 Краткий обзор класса и семейств поддержки доверия

Ниже приведены краткие характеристики класса и семейств поддержки доверия из раздела 16.

2.8.1 Класс AMA. Поддержка доверия

Класс AMA предназначен для поддержки уровня доверия, что ОО продолжит отвечать своему ЗБ при изменениях в ОО или его среде. Каждое из семейств этого класса определяет действия разработчика и оценщика, выполняемые *после* того, как ОО был успешно оценен, хотя некоторые требования применимы и при оценке.

2.8.1.1 План поддержки доверия (AMA_AMP)

Семейство "План поддержки доверия" идентифицирует планы и процедуры, которые выполняет разработчик для обеспечения поддержки доверия, установленного к оцененному ОО, после изменений в ОО или его среде.

2.8.1.2 Отчет о категорировании компонентов ОО (AMA_CAT)

Семейство "Отчет о категорировании компонентов ОО" представляет категорирование компонентов ОО (например, подсистем ФБО) по их отношению к безопасности. Это категорирование занимает центральное место в анализе разработчиком влияния на безопасность.

2.8.1.3 Свидетельство поддержки доверия (AMA_EVD)

Семейство "Свидетельство поддержки доверия" направлено на то, чтобы убедиться в поддержке разработчиком доверия к ОО в соответствии с планом поддержки доверия.

2.8.1.4 Анализ влияния на безопасность (AMA_SIA)

Семейство "Анализ влияния на безопасность" направлено на то, чтобы убедиться в поддержке доверия к ОО посредством проводимого разработчиком анализа влияния на безопасность ОО всех изменений после его оценки.

3 Критерии оценки профиля защиты и задания по безопасности

3.1 Краткий обзор

Настоящий раздел знакомит с критериями оценки для ПЗ и ЗБ, полностью представленными в классах APE "Оценка профиля защиты" и ASE "Оценка задания по безопасности" (разделы 4 и 5 соответственно).

Эти критерии – первые требования оценки, представленные в части 3 ОК, потому что, как правило, оценку ПЗ и ЗБ выполняют до оценки ОО. Они играют особую роль в оценке информации об ОО и оценке функциональных требований и требований доверия для выяснения, являются ли ПЗ и ЗБ содержательной основой для оценки ОО.

Хотя данные критерии оценки несколько отличаются от требований в разделах 8–14, они представлены аналогичным образом, потому что действия разработчика и оценщика при оценке сопоставимы для ПЗ, ЗБ и ОО.

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

Критерии оценки для ПЗ и ЗБ основаны на информации, приведенной в приложениях Б и В к части 1 ОК. Там можно найти полезную информацию о происхождении требований классов APE и ASE.

3.2 Краткий обзор критериев профиля защиты

3.2.1 Оценка профиля защиты

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

3.2.2 Соотношение с критериями оценки задания по безопасности

Как показано в приложениях Б и В к части 1 ОК, имеется много совпадений в структуре и содержании ПЗ, ориентированного на определенный тип ОО, и ЗБ, разработанного для конкретного ОО. Поэтому многие критерии для оценки ПЗ содержат требования, которые подобны аналогичным для ЗБ и представлены таким же образом.

3.2.3 Задачи оценщика

Оценщики ПЗ, который содержит требования только из ОК, должны применять требования класса APE, приведенные в таблице 3.1.

Таблица 3.1 – Семейства оценки профиля защиты, содержащего требования только из ОК

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

Оценщики ПЗ, который содержит требования не из ОК, должны применять требования класса APE, приведенные в таблице 3.2.

Таблица 3.2 – Семейства оценки профиля защиты с требованиями, расширяющими ОК

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

3.3 Краткий обзор критериев задания по безопасности

3.3.1 Оценка задания по безопасности

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

3.3.2 Соотношение с другими критериями оценки из ОК

При оценке ОО различают две стадии: оценка ЗБ и непосредственно оценка ОО, к которому относится данное ЗБ. Требования для оценки ЗБ полностью представлены в разделе 5, а требования для оценки ОО содержатся в разделах 8–14.

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

3.3.3 Задачи оценщика

Оценщики ЗБ, которое содержит требования только из ОК, должны применять требования класса ASE, приведенные в таблице 3.3.

Таблица 3.3 – Семейства оценки задания по безопасности, содержащего требования только из ОК

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

Оценщики ЗБ, которое содержит требования не из ОК, должны применять требования класса ASE, приведенные в таблице 3.4.

Таблица 3.4 – Семейства оценки задания по безопасности с требованиями, расширяющими ОК

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

4 Класс APE. Оценка профиля защиты

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

На рисунке 4.1 показаны семейства этого класса.

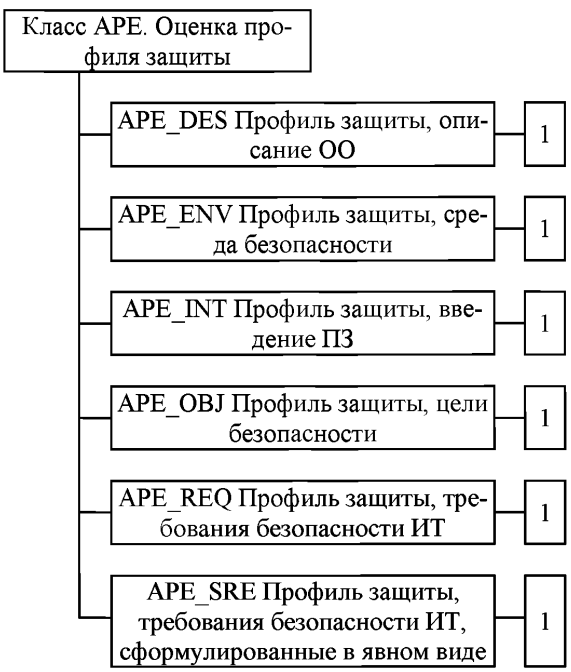


Рисунок 4.1 – Декомпозиция класса "Оценка профиля защиты"

4.1 Описание ОО (APE_DES)

Цели

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

APE_DES.1 Профиль защиты, описание ОО, требования оценки

Зависимости

APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

APE_INT.1 Профиль защиты, введение ПЗ, требования оценки

APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки

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

Элементы действий разработчика

APE_DES.1.1D **Разработчик ПЗ должен представить описание ОО как часть ПЗ.**

Элементы содержания и представления свидетельств

APE_DES.1.1C **Описание ОО, как минимум, должно включать в себя тип продукта и общие свойства ИТ, присущие ОО.**

Элементы действий оценщика

APE_DES.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_DES.1.2E **Оценщик должен подтвердить, что описание ОО является логически последовательным и внутренне непротиворечивым.**

APE_DES.1.3E **Оценщик должен подтвердить, что описание ОО согласуется с другими частями ПЗ.**

4.2 Среда безопасности (APE_ENV)

Цели

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

APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

Зависимости отсутствуют

Элементы действий разработчика

APE_ENV.1.1D **Разработчик ПЗ должен представить изложение среды безопасности ОО как часть ПЗ.**

Элементы содержания и представления свидетельств

APE_ENV.1.1C **Изложение среды безопасности ОО должно идентифицировать и объяснить любые предположения о предполагаемом применении ОО и среде использования ОО.**

APE_ENV.1.2C **Изложение среды безопасности ОО должно идентифицировать и объяснить любые известные или допускаемые угрозы активам, от которых будет требоваться защита посредством ОО или его среды.**

APE_ENV.1.3C **Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.**

Элементы действий оценщика

APE_ENV.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_ENV.1.2E **Оценщик должен подтвердить, что описание среды безопасности ОО является логически последовательным и внутренне непротиворечивым.**

4.3 Введение ПЗ (APE_INT)

Цели

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

APE_INT.1 Профиль защиты, введение ПЗ, требования оценки

Зависимости

APE_DES.1 Профиль защиты, описание ОО, требования оценки

APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

APE_ODJ.1 Профиль защиты, цели безопасности, требования оценки

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

Элементы действий разработчика

APE_INT.1.1D **Разработчик ПЗ должен представить введение ПЗ как часть ПЗ.**

Элементы содержания и представления свидетельств

APE_INT.1.1C **Введение ПЗ должно содержать данные идентификации ПЗ, которые предоставляют маркировку и описательную информацию, необходимые, для идентификации, каталогизации, регистрации ПЗ и ссылок на него.**

APE_INT.1.2C **Введение ПЗ должно содержать аннотацию ПЗ с общей характеристикой ПЗ в описательной форме.**

Элементы действий оценщика

APE_INT.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_INT.1.2E **Оценщик должен подтвердить, что введение ПЗ является логически последовательным и внутренне непротиворечивым.**

APE_INT.1.3E **Оценщик должен подтвердить, что введение ПЗ согласуется с другими частями ПЗ.**

4.4 Цели безопасности (APE_OBJ)

Цели

Цели безопасности – краткое изложение предполагаемой реакции на задачу безопасности. Оценка целей безопасности требуется для демонстрации, что установленные цели адекватны проблеме безопасности. Существуют цели безопасности для ОО и цели безо-

пасности для среды. Необходимо сопоставить цели безопасности для ОО и среды с идентифицированными угрозами, которым они противостоят, и/или с политикой и предположениями, которым они соответствуют

APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки

Зависимости

APE_ENV.1 Профиль защиты, среда безопасности, требования оценки

Элементы действий разработчика

APE_OBJ.1.1D **Разработчик ПЗ должен представить изложение целей безопасности как часть ПЗ.**

APE_OBJ.1.2D **Разработчик ПЗ должен представить логическое обоснование целей безопасности.**

Элементы содержания и представления свидетельств

APE_OBJ.1.1C **Изложение целей безопасности должно определить цели безопасности для ОО и его среды.**

APE_OBJ.1.2C **Цели безопасности для ОО должны быть четко изложены и сопоставлены с идентифицированными угрозами, которым будет противостоять ОО, и/или с политикой безопасности организации, которая будет выполняться ОО.**

APE_OBJ.1.3C **Цели безопасности для среды должны быть четко изложены и сопоставлены с теми аспектами идентифицированных угроз, которым ОО противостоит не полностью, и/или с политикой безопасности организации или предположениями, не полностью выполняемыми ОО.**

APE_OBJ.1.4C **Логическое обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.**

APE_OBJ.1.5C **Логическое обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.**

Элементы действий оценщика

APE_OBJ.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_OBJ.1.2E **Оценщик должен подтвердить, что описание целей безопасности является полным, логически последовательным и внутренне непротиворечивым.**

4.5 Требования безопасности ИТ (APE_REQ)

Цели

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

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

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

Замечания по применению

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

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

В компоненте APE_REQ.1 использованы несколько значений термина "appropriate" ("соответствующий", "необходимый", "приемлемый", "целесообразный") для указания, что данные элементы допускают выбор в определенных случаях. Какой выбор является приемлемым, зависит от контекста ПЗ. Подробная информация по этим аспектам содержится в приложении Б к части 1 ОК.

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

Зависимости

APE_OBJ.1 Профиль защиты, цели безопасности, требования оценки

Элементы действий разработчика

APE_REQ.1.1D Разработчик ПЗ должен представить изложение требований безопасности ИТ как часть ПЗ.

APE_REQ.1.2D Разработчик ПЗ должен представить логическое обоснование требований безопасности.

Элементы содержания и представления свидетельств

APE_REQ.1.1C Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований из части 2 ОК.

APE_REQ.1.2C **Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия из части 3 ОК.**

APE_REQ.1.3C **В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в части 3 ОК.**

APE_REQ.1.4C **Свидетельство должно содержать строгое обоснование, что изложение требований доверия к ОО является соответствующим.**

APE_REQ.1.5C **ПЗ должен, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.**

APE_REQ.1.6C **Все завершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.**

APE_REQ.1.7C **Любые незавершенные операции над требованиями безопасности ИТ, включенными в ПЗ, должны быть идентифицированы.**

APE_REQ.1.8C **Зависимости между требованиями безопасности ИТ, включенными в ПЗ, следует удовлетворить.**

APE_REQ.1.9C **Свидетельство должно содержать строгое обоснование каждого неудовлетворения зависимостей.**

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

APE_REQ.1.11C **ПЗ должен идентифицировать все конкретные функциональные требования безопасности ОО, для которых целесообразно явное указание стойкости функции, так же как и конкретной метрики.**

APE_REQ.1.12C **Логическое обоснование требований безопасности должно демонстрировать, что минимальный уровень стойкости функции в ПЗ, как и каждое явное указание стойкости функции согласуются с целями безопасности ОО.**

APE_REQ.1.13C **Логическое обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.**

APE_REQ.1.14C **Логическое обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.**

Элементы действий оценщика

APE_REQ.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_REQ.1.2E **Оценщик должен подтвердить, что описание требований безопасности ИТ является полным, логически последовательным и внутренне непротиворечивым.**

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

Цели

Если после тщательного рассмотрения окажется, что ни один из компонентов требований частей 2 или 3 ОК не применим непосредственно ко всем или к части требований безопасности ИТ, разработчик ПЗ может сформулировать другие требования, которые не ссылаются на ОК. Использование таких требований должно быть строго обосновано.

Это семейство содержит требования оценки, которые позволяют оценщику сделать заключение, что сформулированные в явном виде требования четко и однозначно выражены. Оценка требований, выбранных из ОК и используемых наряду со сформулированными в явном виде допустимыми требованиями безопасности, определяется семейством APE_REQ.

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

Замечания по применению

Формулировка в явном виде требований по структуре, сопоставимой со структурой существующих компонентов и элементов из ОК, включает в себя выбор аналогичного маркирования, способа выражения и уровня детализации.

Использование требований ОК как образца означает, что требования могут быть четко идентифицированы, что они автономны, и применение каждого требования возможно и даст значимый результат оценки, основанный на анализе соответствия ОО этому конкретному требованию.

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

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

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

Зависимости

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

Элементы действий разработчика

APE_SRE.1.1D **Разработчик ПЗ должен представить изложение требований безопасности ИТ как часть ПЗ.**

APE_SRE.1.2D **Разработчик ПЗ должен представить логическое обоснование требований безопасности.**

Элементы содержания и представления свидетельств

APE_SRE.1.1C **Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ОК, должны быть идентифицированы.**

APE_SRE.1.2C **Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ОК, должны быть идентифицированы.**

APE_SRE.1.3C **Свидетельство должно содержать строгое обоснование, почему требования безопасности должны быть сформулированы в явном виде.**

APE_SRE.1.4C **Сформулированные в явном виде требования безопасности ИТ должны использовать компоненты, семейства и классы требований ОК как образец для представления.**

APE_SRE.1.5C **Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать объективные требования оценки, такие, что соответствие или несоответствие им ОО может быть определено и последовательно продемонстрировано.**

APE_SRE.1.6C **Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.**

APE_SRE.1.7C **Логическое обоснование требований безопасности должно демонстрировать, что требования доверия применимы и пригодны для поддержки каждого из сформулированных в явном виде функциональных требований безопасности ОО.**

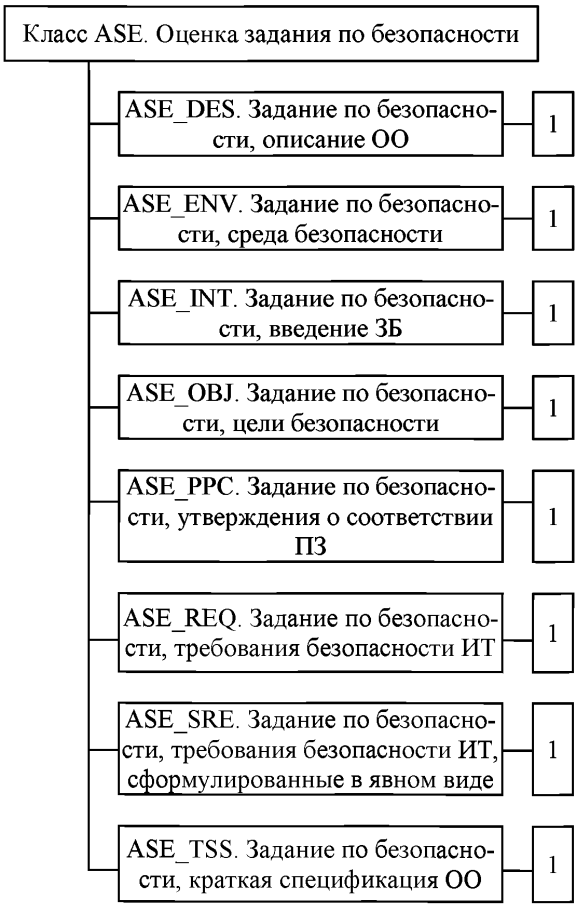
Элементы действий оценщика

APE_SRE.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

APE_SRE.1.2E **Оценщик должен определить, что все зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.**

5 Класс ASE. Оценка задания по безопасности

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



На рисунке 5.1 показаны семейства этого класса.

Рисунок 5.1 – Декомпозиция класса "Оценка задания по безопасности"

5.1 Описание ОО (ASE_DES)

Цели

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

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

Зависимости

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

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

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

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

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

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

Элементы действий разработчика

ASE_DES.1.1D **Разработчик должен представить описание ОО как часть ЗБ.**

Элементы содержания и представления свидетельств

ASE_DES.1.1C **Описание ОО, как минимум, должно включать в себя тип продукта или системы, а также область и ограничения применения ОО в общеупотребительных терминах, как в физическом, так и в логическом смысле.**

Элементы действий оценщика

ASE_DES.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ASE_DES.1.2E **Оценщик должен подтвердить, что описание ОО является логически последовательным и внутренне непротиворечивым.**

ASE_DES.1.3E **Оценщик должен подтвердить, что описание ОО согласуется с другими частями ЗБ.**

5.2 Среда безопасности (ASE_ENV)

Цели

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

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

Зависимости отсутствуют.

Элементы действий разработчика

ASE_ENV.1.1D **Разработчик должен представить изложение среды безопасности ОО как часть ЗБ.**

Элементы содержания и представления свидетельств

ASE_ENV.1.1C **Изложение среды безопасности ОО должно идентифицировать и объяснить любые предположения о предполагаемом применении ОО и среде использования ОО.**

ASE_ENV.1.2C **Изложение среды безопасности ОО должно идентифицировать и объяснить любые известные или допускаемые угрозы активам, от которых будет требоваться защита посредством ОО или его среды.**

ASE_ENV.1.3C **Изложение среды безопасности ОО должно идентифицировать и объяснить каждую политику безопасности организации, соответствие которой для ОО необходимо.**

Элементы действий оценщика

ASE_ENV.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ASE_ENV.1.2E **Оценщик должен подтвердить, что описание среды безопасности ОО является логически последовательным и внутренне непротиворечивым.**

5.3 Введение ЗБ (ASE_INT)

Цели

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

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

Зависимости

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

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

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

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

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

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

Элементы действий разработчика

ASE_INT.1.1D **Разработчик должен представить введение ЗБ как часть ЗБ.**

Элементы содержания и представления свидетельств

ASE_INT.1.1C **Введение ЗБ должно содержать данные идентификации ЗБ, которые предоставляют маркировку и описательную информацию, необходимые для идентификации и применения ЗБ и ОО, к которому оно относится.**

ASE_INT.1.2C **Введение ЗБ должно содержать аннотацию ЗБ с общей характеристикой ЗБ в описательной форме.**

ASE_INT.1.3C **Введение ЗБ должно содержать утверждение о соответствии ОК, излагающее все оцениваемые утверждения для ОО о соответствии ОК.**

Элементы действия 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 введение ЗБ является логически последовательным и внутренне непротиворечивым.**

ASE_INT.1.3E **Оценщик должен подтвердить, что введение ЗБ согласуется с другими частями ЗБ.**

5.4 Цели безопасности (ASE_OBJ)

Цели

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

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

Зависимости

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

Элементы действий разработчика

ASE_OBJ.1.1D **Разработчик должен представить изложение целей безопасности как часть ЗБ.**

ASE_OBJ.1.2D **Разработчик должен представить логическое обоснование целей безопасности.**

Элементы содержания и представления свидетельств

ASE_OBJ.1.1C **Изложение целей безопасности должно определить цели безопасности для ОО и его среды.**

ASE_OBJ.1.2C **Цели безопасности для ОО должны быть четко изложены и сопоставлены с идентифицированными угрозами, которым будет противостоять ОО, и/или с политикой безопасности организации, которая будет выполняться ОО.**

ASE_OBJ.1.3C **Цели безопасности для среды должны быть четко изложены и сопоставлены с теми аспектами идентифицированных угроз, которым ОО противостоит не полностью, и/или с политикой безопасности организации или предположениями, не полностью выполняемыми ОО.**

ASE_OBJ.1.4C **Логическое обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для противостояния всем идентифицированным угрозам безопасности.**

ASE_OBJ.1.5C **Логическое обоснование целей безопасности должно демонстрировать, что изложенные цели безопасности пригодны для охвата всех установленных положений политики безопасности организации и предположений.**

Элементы действий оценщика

ASE_OBJ.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ASE_OBJ.1.2E **Оценщик должен подтвердить, что описание целей безопасности является полным, логически последовательным и внутренне непротиворечивым.**

5.5 Утверждения о соответствии ПЗ (ASE_PPC)

Цели

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

Замечания по применению

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

Хотя при наличии утверждений о соответствии ПЗ необходимы дополнительные действия по оценке, затраты на оценку ЗБ обычно все-таки меньше, чем в случае, когда никакой ПЗ не применяется, потому что при оценке ЗБ можно использовать результаты оценки этого ПЗ.

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

Зависимости

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

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

Элементы действий разработчика

ASE_PPC.1.1D Разработчик должен представить каждое утверждение о соответствии ПЗ как часть ЗБ.

ASE_PPC.1.2D Разработчик должен представить логическое обоснование утверждений о соответствии ПЗ для каждого представленного утверждения о соответствии ПЗ.

Элементы содержания и представления свидетельств

ASE_PPC.1.1C Каждое утверждение о соответствии ПЗ должно идентифицировать ПЗ, соответствие которому утверждается, включая необходимые уточнения, связанные с этим утверждением.

ASE_PPC.1.2C Каждое утверждение о соответствии ПЗ должно идентифицировать формулировки требований безопасности ИТ, в которых завершены разрешенные операции или иначе выполнено дальнейшее уточнение требований ПЗ.

ASE_PPC.1.3C Каждое утверждение о соответствии ПЗ должно идентифицировать формулировки содержащихся в ЗБ целей безопасности и требований безопасности ИТ, которые дополняют имеющиеся в ПЗ.

Элементы действий оценщика

ASE_PPC.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ASE_PPC.1.2E Оценщик должен подтвердить, что утверждения о соответствии профилям защиты являются корректным отображением соответствующих ПЗ.

5.6 Требования безопасности ИТ (ASE_REQ)

Цели

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

Это семейство представляет требования оценки, которые позволяют оценщику принять решение, что ЗБ пригодно для использования в качестве изложения требований к соответствующему ОО. Дополнительные критерии, необходимые для оценки требований, сформулированных в явном виде, приведены в семействе ASE_SRE.

Замечания по применению

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

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

В компоненте ASE_REQ.1 использованы несколько значений термина «appropriate» («соответствующий», «необходимый», «приемлемый», «целесообразный») для указания, что данные элементы допускают выбор в определенных случаях. Какой выбор является приемлемым, зависит от контекста ЗБ. Подробная информация по этим аспектам содержится в приложении В к части 1 ОК.

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

Зависимости

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

Элементы действий разработчика

ASE_REQ.1.1D **Разработчик должен представить изложение требований безопасности ИТ как часть ЗБ.**

ASE_REQ.1.2D **Разработчик должен представить логическое обоснование требований безопасности.**

Элементы содержания и представления свидетельств

ASE_REQ.1.1C **Изложение функциональных требований безопасности ОО должно идентифицировать функциональные требования безопасности ОО, составленные из компонентов функциональных требований из части 2 ОК.**

ASE_REQ.1.2C **Изложение требований доверия к ОО должно идентифицировать требования доверия к ОО, составленные из компонентов требований доверия из части 3 ОК.**

ASE_REQ.1.3C **В изложение требований доверия к ОО следует включить оценочный уровень доверия (ОУД), как определено в части 3 ОК.**

ASE_REQ.1.4C **Свидетельство должно содержать строгое обоснование, что изложение требований доверия к ОО является соответствующим.**

ASE_REQ.1.5C **ЗБ должно, при необходимости, идентифицировать каждое требование безопасности для среды ИТ.**

ASE_REQ.1.6C **Операции, предусмотренные в требованиях безопасности ИТ, включенных в ЗБ, должны быть идентифицированы и выполнены.**

ASE_REQ.1.7C **Зависимости между требованиями безопасности ИТ, включенными в ЗБ, следует удовлетворить.**

ASE_REQ.1.8C **Свидетельство должно содержать строгое обоснование каждого неудовлетворения зависимостей.**

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

ASE_REQ.1.10C **ЗБ должно идентифицировать все конкретные функциональные требования безопасности ОО, для которых целесообразно явное указание стойкости функции, так же как и конкретной метрики.**

ASE_REQ.1.11C **Логическое обоснование требований безопасности должно демонстрировать, что минимальный уровень стойкости функции в ЗБ, как и каждое явное указание стойкости функции согласуются с целями безопасности ОО.**

ASE_REQ.1.12C **Логическое обоснование требований безопасности должно демонстрировать, что требования безопасности ИТ пригодны для достижения целей безопасности.**

ASE_REQ.1.13C **Логическое обоснование требований безопасности должно демонстрировать, что совокупность требований безопасности ИТ образует взаимно согласованное и внутренне непротиворечивое целое.**

Элементы действий оценщика

ASE_REQ.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ASE_REQ.1.2E **Оценщик должен подтвердить, что описание требований безопасности ИТ является полным, логически последовательным и внутренне непротиворечивым.**

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

Цели

Если, после тщательного рассмотрения, окажется, что ни один из компонентов требований частей 2 или 3 ОК не применим непосредственно ко всем или к части требований безопасности ИТ, разработчик ЗБ может сформулировать другие требования, которые не ссылаются на ОК. Использование таких требований должно быть строго обосновано.

Это семейство содержит требования оценки, которые позволяют оценщику сделать заключение, что сформулированные в явном виде требования четко и однозначно выражены. Оценка требований, выбранных из ОК и используемых наряду со сформулированными в явном виде допустимыми требованиями безопасности, определяется семейством ASE_REQ.

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

Замечания по применению

Формулировка в явном виде требований по структуре, сопоставимой со структурой существующих компонентов и элементов из ОК, включает в себя выбор аналогичного маркирования, способа выражения и уровня детализации.

Использование требований ОК как образца означает, что требования могут быть четко идентифицированы, что они автономны, и применение каждого требования возможно и даст значимый результат оценки, основанный на изложении соответствия ОО этому конкретному требованию.

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

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

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

Зависимости

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

Элементы действий разработчика

ASE_SRE.1.1D Разработчик должен представить изложение требований безопасности ИТ как часть ЗБ.

ASE_SRE.1.2D Разработчик должен представить логическое обоснование требований безопасности.

Элементы содержания и представления свидетельств

ASE_SRE.1.1C Все требования безопасности ОО, которые сформулированы в явном виде без ссылки на ОК, должны быть идентифицированы.

ASE_SRE.1.2C Все требования безопасности для среды ИТ, которые сформулированы в явном виде без ссылки на ОК, должны быть идентифицированы.

ASE_SRE.1.3C Свидетельство должно содержать строгое обоснование, почему требования безопасности должны быть сформулированы в явном виде.

ASE_SRE.1.4C Сформулированные в явном виде требования безопасности ИТ должны использовать компоненты, семейства и классы требований ОК как образец для представления.

ASE_SRE.1.5C Сформулированные в явном виде требования безопасности ИТ должны быть измеримы и устанавливать объективные требования оценки, такие, что соответствие или несоответствие им ОО может быть определено и последовательно продемонстрировано.

ASE_SRE.1.6C Сформулированные в явном виде требования безопасности ИТ должны быть четко и недвусмысленно выражены.

ASE_SRE.1.7C **Логическое обоснование требований безопасности должно демонстрировать, что требования доверия применимы и пригодны для поддержки каждого из сформулированных в явном виде функциональных требований безопасности ОО.**

Элементы действий оценщика

ASE_SRE.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ASE_SRE.1.2E **Оценщик должен определить, что все зависимости сформулированных в явном виде требований безопасности ИТ были идентифицированы.**

5.8 Краткая спецификация ОО (ASE_TSS)

Цели

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

Замечания по применению

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

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

В компоненте ASE_TSS.1 использованы несколько значений термина "appropriate" ("соответствующий", "необходимый") для указания, что данные элементы допускают выбор в определенных случаях. Какой выбор является приемлемым, зависит от контекста ЗБ. Подробная информация по этим аспектам содержится в приложении В к части 1 ОК.

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

Зависимости

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

Элементы действий разработчика

ASE_TSS.1.1D **Разработчик должен представить краткую спецификацию ОО как часть ЗБ.**

ASE_TSS.1.2D **Разработчик должен представить логическое обоснование краткой спецификации ОО.**

Элементы содержания и представления свидетельств

ASE_TSS.1.1C **Краткая спецификация ОО должна содержать описание функций безопасности ИТ и мер доверия к ОО.**

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

ASE_TSS.1.3C **Функции безопасности ИТ должны быть определены в неформальном стиле на уровне детализации, необходимом для понимания их назначения.**

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

ASE_TSS.1.5C **Логическое обоснование краткой спецификации ОО должно демонстрировать, что функции безопасности ИТ пригодны для удовлетворения функциональных требований безопасности ОО.**

ASE_TSS.1.6C **Логическое обоснование краткой спецификации ОО должно демонстрировать, что сочетание специфицированных функций безопасности ИТ в совокупности способно удовлетворить функциональные требования безопасности ОО.**

ASE_TSS.1.7C **Краткая спецификация ОО должна сопоставить меры и требования доверия так, чтобы можно было отметить, какие меры способствуют удовлетворению каких требований.**

ASE_TSS.1.8C **Логическое обоснование краткой спецификации ОО должно демонстрировать, что меры доверия удовлетворяют все требования доверия к ОО.**

ASE_TSS.1.9C **Краткая спецификация ОО должна идентифицировать все функции безопасности ИТ, которые реализованы вероятностным или перестановочным механизмом соответственно.**

ASE_TSS.1.10C **Краткая спецификация ОО должна установить для каждой функции безопасности ИТ, для которой это необходимо, требование стойкости**

функции либо по специальной метрике, либо как базовую, среднюю или высокую СФБ.

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 ОО является полной, логически последовательной и внутренне непротиворечивой.**

6 Оценочные уровни доверия

Оценочные уровни доверия (ОУД) образуют возрастающую шкалу, которая позволяет соотнести получаемый уровень доверия со стоимостью и возможностью достижения этой степени доверия. В части 3 ОК идентифицированы разделенные понятия доверия к ОО по завершению оценки и поддержки этого доверия в процессе эксплуатации ОО.

Важно обратить внимание, что не все семейства и компоненты из части 3 ОК включены в оценочные уровни доверия. Это не означает, что они не обеспечивают значимое и полезное доверие. Напротив, ожидается, что эти семейства и их компоненты будут рассматриваться для усиления ОУД в тех ПЗ и ЗБ, для которых они полезны.

6.1 Краткий обзор оценочных уровней доверия (ОУД)

В таблице 6.1 представлено сводное описание ОУД. Графы таблицы представляют иерархически упорядоченный набор ОУД, а строки – семейства доверия. Каждый номер в образованной ими матрице идентифицирует конкретный компонент доверия, применяемый в данном случае.

Как показано в следующем подразделе, в части 3 ОК определены семь иерархически упорядоченных оценочных уровней доверия для ранжирования доверия к ОО. Каждый последующий ОУД представляет более высокое доверие, чем любой из предыдущих. Увеличение доверия от предыдущего ОУД к последующему достигается *заменой* какого-либо компонента доверия иерархичным компонентом из того же семейства доверия (т.е. увеличением строгости, области и/или глубины оценки) и *добавлением* компонентов из других семейств доверия (т.е. добавлением новых требований).

ОУД состоят из определенной комбинации компонентов доверия, как описано в разделе 2. Точнее, каждый ОУД включает в себя не более одного компонента каждого семейства доверия, а все зависимости каждого компонента доверия учтены.

Хотя в части 3 ОК определены именно ОУД, можно представлять другие комбинации компонентов доверия. Специально введенное понятие "усиление" ("augmentation") допускает добавление (из семейств доверия, до этого не включенных в ОУД) или замену компонентов доверия в ОУД (другими, иерархичными компонентами из того же самого семейства доверия). Из конструкций установления доверия, определенных в ОК, только ОУД могут быть усилены. Понятие "ОУД за исключением какого-либо составляющего его компонента доверия" не признано в ОК как допустимое утверждение. Вводящий усиление обязан строго обосновать полезность и дополнительную ценность добавленного к ОУД компонента доверия. ОУД может быть также расширен требованиями доверия, сформулированными в явном виде.

Таблица 6.1 – Обзор оценочных уровней доверия

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

6.2 Детализация оценочных уровней доверия

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

6.2.1 Оценочный уровень доверия 1 (ОУД1) – предусматривающий функциональное тестирование

Цели

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

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

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

Компоненты доверия

ОУД1 (см. таблицу 6.2) предоставляет базовый уровень доверия посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов и руководств.

Анализ поддержан независимым тестированием ФБО.

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

Таблица 6.2 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 1

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

6.2.2 Оценочный уровень доверия 2 (ОУД2) – предусматривающий структурное тестирование

Цели

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

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

Компоненты доверия

ОУД2 (см. таблицу **6.3**) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов, руководств и **проекта ОО верхнего уровня**.

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

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

Этот ОУД представляет значимое увеличение доверия по сравнению с ОУД1, требуя тестирование и анализ уязвимостей разработчиком, а также независимое тестирование, основанное на более детализированных спецификациях ОО.

Таблица 6.3 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 2

Класс доверия	Компоненты доверия
Управление конфигурацией	**ACM_CAP.2 Элементы конфигурации**
Поставка и эксплуатация	**ADO_DEL.1 Процедуры поставки**
	ADO_IGS.1 Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1 Неформальная функциональная спецификация
	ADV_HLD.1 Описательный проект верхнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия
Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
Тестирование	**ATE_COV.1 Свидетельство покрытия**
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
Оценка уязвимостей	**AVA_SOF.1 Оценка стойкости функции безопасности ОО**
	AVA_VLA.1 Анализ уязвимостей разработчиком

6.2.3 Оценочный уровень доверия 3 (ОУД3) – предусматривающий методическое тестирование и проверку

Цели

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

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

Компоненты доверия

ОУД3 (см. таблицу **6.4**) обеспечивает доверие путем анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, спецификации интерфейсов, руководств и проекта ОО верхнего уровня.

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

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

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

Таблица 6.4 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 3

Класс доверия	Компоненты доверия
Управление конфигурацией	**ACM_CAP.3 Средства контроля авторизации**
	ACM_SCP.1 Охват УК объекта оценки
Поставка и эксплуатация	ADO_DEL.1 Процедуры поставки
	ADO_IGS.1 Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1 Неформальная функциональная спецификация
	ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия
Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
Поддержка жизненного цикла	**ALC_DVS.1 Идентификация мер безопасности**
Тестирование	**ATE_COV.2 Анализ покрытия**
	ATE_DPT.1 Тестирование: проект верхнего уровня
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
Оценка уязвимостей	**AVA_MSU.1 Экспертиза руководств**
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.1 Анализ уязвимостей разработчиком

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

Цели

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

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

Компоненты доверия

ОУД4 (см. таблицу **6.5**) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, **полной** спецификации интерфейсов, руководств, проекта ОО верхнего уровня **и нижнего уровня**, **а также подмножества реализации**. **Доверие дополнительно достигается применением неформальной модели политики безопасности ОО**.

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

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

Этот ОУД представляет значимое увеличение доверия по сравнению с ОУД3, требуя более детальное описание проекта, подмножество реализации и улучшенные механизмы и/или процедуры, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки или поставки.

Таблица 6.5 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 4

Класс доверия	Компоненты доверия
Управление конфигурацией	**ACM_AUT.1 Частичная автоматизация УК**
	ACM_CAP.4 Поддержка генерации, процедуры приемки
	ACM_SCP.2 Охват УК отслеживания проблем
Поставка и эксплуатация	**ADO_DEL.2 Обнаружение модификации**
	ADO_IGS.1 Процедуры установки, генерации и запуска
Разработка	**ADV_FSP.2 Полностью определенные внешние интерфейсы**
	ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня
	ADV_IMP.1 Подмножество реализации ФБО
	ADV_LLD.1 Описательный проект нижнего уровня
	ADV_RCR.1 Неформальная демонстрация соответствия
	ADV_SPM.1 Неформальная модель политики безопасности ОО
Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
Поддержка жизненного цикла	ALC_DVS.1 Идентификация мер безопасности
	ALC_LCD.1 Модель жизненного цикла, определенная разработчиком
	ALC_TAT.1 Полностью определенные инструментальные средства разработки
Тестирование	ATE_COV.2 Анализ покрытия
	ATE_DPT.1 Тестирование: проект верхнего уровня
	ATE_FUN.1 Функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
Оценка уязвимостей	**AVA_MSU.2 Подтверждение правильности анализа**
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.2 Независимый анализ уязвимостей

6.2.5 Оценочный уровень доверия 5 (ОУД5) – предусматривающий полуформальное проектирование и тестирование

Цели

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

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

Компоненты доверия

ОУД5 (см. таблицу **6.6**) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего уровня и нижнего уровня, а также **всей** реализации. Доверие дополнительно достигается применением **формальной** модели политики безопасности ОО **и полуформального представления функциональной спецификации и проекта верхнего уровня, а также полуформальной демонстрации соответствия между ними. Кроме этого, требуется модульное проектирование ОО.**

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

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

Этот ОУД представляет значимое увеличение доверия по сравнению с ОУД4, требуя полуформальное описание проекта, полную реализацию, более структурированную (и, следовательно, лучше анализируемую) архитектуру, анализ скрытых каналов и улучшенные механизмы и/или процедуры, что дает уверенность в том, что в ОО не будут внесены искажения во время разработки.

Таблица 6.6 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 5

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

6.2.6 Оценочный уровень доверия 6 (ОУД6) – предусматривающий полуформальную верификацию проекта и тестирование

Цели

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

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

Компоненты доверия

ОУД6 (см. таблицу **6.7**) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего уровня и нижнего уровня, а также **структурированного представления** реализации. Доверие дополнительно достигается применением формальной модели политики безопасности ОО и полуформального представления функциональной спецификации, проекта верхнего уровня **и проекта нижнего уровня**, а также полуформальной демонстрации соответствия между ними. Кроме этого, требуется модульное **и иерархическое (по уровням)** проектирование ОО.

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

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

Этот ОУД представляет значимое увеличение доверия по сравнению с ОУД5, требуя всесторонний анализ, структурированное представление реализации, более стройную структуру (например, с разбиением на уровни), всесторонний независимый анализ уязвимостей, систематическую идентификацию скрытых каналов, улучшенное управление конфигурацией и улучшенный контроль среды разработки.

Таблица 6.7 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 6

Класс доверия	Компоненты доверия
Управление конфигурацией	**ACM_AUT.2 Полная автоматизация УК**
	ACM_CAP.5 Расширенная поддержка
	ACM_SCP.3 Охват УК инструментальных средств разработки
Поставка и эксплуатация	ADO_DEL.2 Обнаружение модификации
	ADO_IGS.1 Процедуры установки, генерации и запуска
Разработка	**ADV_FSP.3 Полуформальная функциональная спецификация**
	ADV_HLD.4 Пояснения в полуформальном проекте верхнего уровня
	ADV_IMP.3 Структурированная реализация ФБО
	ADV_INT.2 Уменьшение сложности
	ADV_LLD.2 Полуформальный проект нижнего уровня
	ADV_RCR.2 Полуформальная демонстрация соответствия
	ADV_SPM.3 Формальная модель политики безопасности ОО
Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
Поддержка жизненного цикла	**ALC_DVS.2 Достаточность мер безопасности**
	ALC_LCD.2 Стандартизованная модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей объекта оценки стандартам реализации
Тестирование	**ATE_COV.3 Строгий анализ покрытия**
	ATE_DPT.2 Тестирование: проект нижнего уровня
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.2 Выборочное независимое тестирование
Оценка уязвимостей	**AVA_CCA.2 Систематический анализ скрытых каналов**
	AVA_MSU.3 Анализ и тестирование опасных состояний
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.4 Высокостойкий

6.2.7 Оценочный уровень доверия 7 (ОУД7) – предусматривающий формальную верификацию проекта и тестирование

Цели

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

Компоненты доверия

ОУД7 (см. таблицу **6.8**) обеспечивает доверие посредством анализа функций безопасности с использованием для понимания режима безопасности функциональной спецификации, полной спецификации интерфейсов, руководств, проекта ОО верхнего уровня и нижнего уровня, а также структурированного представления реализации. Доверие дополнительно достигается применением формальной модели политики безопасности ОО, **формального представления функциональной спецификации и проекта верхнего уровня**, полуформального представления проекта нижнего уровня, а также **формальной (где это требуется) и** полуформальной демонстрации соответствия между ними. Кроме этого, требуется модульное, иерархическое (по уровням) **и простое** проектирование ОО.

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

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

Этот ОУД представляет значимое увеличение доверия по сравнению с ОУД6, требуя всесторонний анализ, использующий формальные представления и формальное соответствие, а также всестороннее тестирование.

Таблица 6.8 – ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ 7

Класс доверия	Компоненты доверия
Управление конфигурацией	ACM_AUT.2 Полная автоматизация УК
	ACM_CAP.5 Расширенная поддержка
	ACM_SCP.3 Охват УК инструментальных средств разработки
Поставка и эксплуатация	**ADO_DEL.3 Предотвращение модификации**
	ADO_IGS.1 Процедуры установки, генерации и запуска
Разработка	**ADV_FSP.4 Формальная функциональная спецификация**
	ADV_HLD.5 Формальный проект верхнего уровня
	ADV_IMP.3 Структурированная реализация ФБО
	ADV_INT.3 Минимизация сложности
	ADV_LLD.2 Полуформальный проект нижнего уровня
	ADV_RCR.3 Формальная демонстрация соответствия
	ADV_SPM.3 Формальная модель политики безопасности ОО
Руководства	AGD_ADM.1 Руководство администратора
	AGD_USR.1 Руководство пользователя
Поддержка жизненного цикла	ALC_DVS.2 Достаточность мер безопасности
	ALC_LCD.3 Измеримая модель жизненного цикла
	ALC_TAT.3 Соответствие всех частей объекта оценки стандартам реализации
Тестирование	ATE_COV.3 Строгий анализ покрытия
	ATE_DPT.3 Тестирование на уровне реализации
	ATE_FUN.2 Упорядоченное функциональное тестирование
	ATE_IND.3 Полное независимое тестирование
Оценка уязвимостей	AVA_CCA.2 Систематический анализ скрытых каналов
	AVA_MSU.3 Анализ и тестирование опасных состояний
	AVA_SOF.1 Оценка стойкости функции безопасности ОО
	AVA_VLA.4 Высокостойкий

7 Классы, семейства и компоненты доверия

Разделы 8–14 содержат детализированные требования, представленные во всех компонентах доверия, сгруппированных в классы и семейства в алфавитном (по-латински) порядке.

8 Класс ACM. Управление конфигурацией

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

На рисунке 8.1 показаны семейства этого класса и иерархия компонентов в семействах.

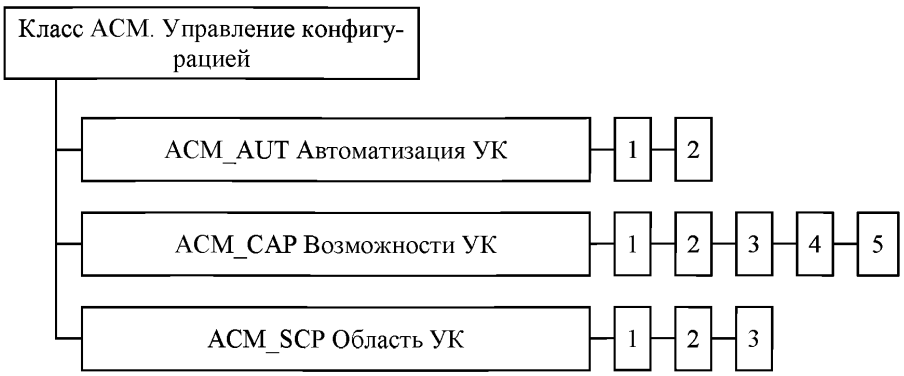


Рисунок 8.1 – Декомпозиция класса "Управление конфигурацией"

8.1 Автоматизация УК (ACM_AUT)

Цели

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

Ранжирование компонентов

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

Замечания по применению

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

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

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

ACM_AUT.1 Частичная автоматизация УК

Цели

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

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ACM_AUT.1.1D Разработчик должен использовать систему УК.

ACM_AUT.1.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

ACM_AUT.1.1C Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО производятся только санкционированные изменения.

ACM_AUT.1.2C Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

ACM_AUT.1.3C План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

ACM_AUT.1.4C План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

Элементы действий оценщика

ACM_AUT.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_AUT.2 Полная автоматизация УК

Цели

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

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

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ACM_AUT.2.1D Разработчик должен использовать систему УК.

ACM_AUT.2.2D Разработчик должен представить план УК.

Элементы содержания и представления свидетельств

ACM_AUT.2.1C Система УК должна предоставить автоматизированные средства, с использованием которых в представлении реализации ОО **и во всех остальных элементах конфигурации** производятся только санкционированные изменения.

ACM_AUT.2.2C Система УК должна предоставить автоматизированные средства для поддержки генерации ОО.

ACM_AUT.2.3C План УК должен содержать описание автоматизированных инструментальных средств, используемых в системе УК.

ACM_AUT.2.4C План УК должен содержать описание, как автоматизированные инструментальные средства используются в системе УК.

ACM_AUT.2.5C Система УК должна предоставить автоматизированные средства для выявления различий между ОО и предшествующей версией.

ACM_AUT.2.6C Система УК должна предоставить автоматизированные средства для определения всех других элементов конфигурации, на которые воздействует модификация данного элемента конфигурации.

Элементы действий оценщика

ACM_AUT.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

8.2 Возможности УК (ACM_CAP)

Цели

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

Цели этого семейства состоят в следующем:

а) обеспечение корректности и полноты ОО к моменту представления его потребителю;

б) обеспечение, чтобы никакие элементы конфигурации не были пропущены в процессе оценки;

в) предотвращение несанкционированной модификации, добавления или удаления элементов конфигурации ОО.

Ранжирование компонентов

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

Замечания по применению

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

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

ACM_CAP.2.6C содержит требование, чтобы система УК уникально идентифицировала все элементы конфигурации. Также требуется, чтобы модификация элемента конфигурации приводила к назначению нового уникального идентификатора.

ACM_CAP.3.8C содержит требование, что свидетельство должно демонстрировать функционирование системы УК в соответствии с планом УК. Примерами такого свидетельства являются как документация типа образов экрана или журнала аудита для системы УК, так и подробная демонстрация системы УК разработчиком. Оценщик является ответственным за заключение, что это свидетельство является достаточным для показа, что система УК функционирует в соответствии с планом УК.

ACM_CAP.3.9C содержит требование, чтобы было представлено свидетельство, показывающее, что все элементы конфигурации поддерживаются системой УК. Так как элементом конфигурации считается элемент, включенный в список конфигурации, это требование устанавливает, что все элементы списка конфигурации поддерживаются системой УК.

ACM_CAP.4.11C содержит требование, чтобы система УК поддерживала генерацию ОО. Для этого требуется, чтобы система УК предоставила информационные и/или

электронные средства, содействующие принятию заключения, что при генерации ОО использованы правильные элементы конфигурации.

ACM_CAP.1 Номера версий

Цели

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

Зависимости отсутствуют.

Элементы действий разработчика

ACM_CAP.1.1D **Разработчик должен предоставить маркировку для ОО.**

Элементы содержания и представления свидетельств

ACM_CAP.1.1C **Маркировка ОО должна быть уникальна для каждой версии ОО.**

ACM_CAP.1.2C **ОО должен быть помечен маркировкой.**

Элементы действий оценщика

ACM_CAP.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ACM_CAP.2 Элементы конфигурации

Цели

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

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

Зависимости отсутствуют.

Элементы действий разработчика

ACM_CAP.2.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.2.2D **Разработчик должен использовать систему УК.**

ACM_CAP.2.3D **Разработчик должен представить документацию УК.**

Элементы содержания и представления свидетельств

ACM_CAP.2.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.2.2C ОО должен быть помечен маркировкой.

ACM_CAP.2.3C **Документация УК должна включать в себя список конфигурации.**

ACM_CAP.2.4C **Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.**

ACM_CAP.2.5C **Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.**

ACM_CAP.2.6C **Система УК должна уникально идентифицировать все элементы конфигурации.**

Элементы действий оценщика

ACM_CAP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_CAP.3 Средства контроля авторизации

Цели

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

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

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

Зависимости

ACM_SCP.1 Охват УК объекта оценки

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

ACM_CAP.3.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.3.2D Разработчик должен использовать систему УК.

ACM_CAP.3.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_CAP.3.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.3.2C ОО должен быть помечен маркировкой.

ACM_CAP.3.3C Документация УК должна включать в себя список конфигурации **и план УК**.

ACM_CAP.3.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.3.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.3.6C Система УК должна уникально идентифицировать все элементы конфигурации.

ACM_CAP.3.7C **План УК должен содержать описание, как используется система УК.**

ACM_CAP.3.8C **Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.**

ACM_CAP.3.9C **Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.**

ACM_CAP.3.10C **Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.**

Элементы действий оценщика

ACM_CAP.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_CAP.4 Поддержка генерации, процедуры приемки

Цели

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

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

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

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

Зависимости

ACM_SCP.1 Охват УК объекта оценки

ALC_DVS.1 Идентификация мер безопасности

Элементы действий разработчика

ACM_CAP.4.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.4.2D Разработчик должен использовать систему УК.

ACM_CAP.4.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_CAP.4.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.4.2C ОО должен быть помечен маркировкой.

ACM_CAP.4.3C Документация УК должна включать в себя список конфигурации, план УК **и план приемки**.

ACM_CAP.4.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.4.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.4.6C Система УК должна уникально идентифицировать все элементы конфигурации.

ACM_CAP.4.7C План УК должен содержать описание, как используется система УК.

ACM_CAP.4.8C Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

ACM_CAP.4.9C Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

ACM_CAP.4.10C Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

ACM_CAP.4.11C **Система УК должна поддерживать генерацию ОО.**

ACM_CAP.4.12C **План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.**

Элементы действий оценщика

ACM_CAP.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_CAP.5 Расширенная поддержка

Цели

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

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

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

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

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

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

Зависимости

ACM_SCP.1 Охват УК объекта оценки

ALC_DVS.2 Достаточность мер безопасности

Элементы действий разработчика

ACM_CAP.5.1D Разработчик должен предоставить маркировку для ОО.

ACM_CAP.5.2D Разработчик должен использовать систему УК.

ACM_CAP.5.3D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_CAP.5.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.5.2C ОО должен быть помечен маркировкой.

ACM_CAP.5.3C Документация УК должна включать в себя список конфигурации, план УК, план приемки **и процедуры компоновки.**

ACM_CAP.5.4C Список конфигурации должен содержать описание элементов конфигурации, входящих в ОО.

ACM_CAP.5.5C Документация УК должна содержать описание метода, используемого для уникальной идентификации элементов конфигурации.

ACM_CAP.5.6C Система УК должна уникально идентифицировать все элементы конфигурации.

ACM_CAP.5.7C План УК должен содержать описание, как используется система УК.

ACM_CAP.5.8C Свидетельство должно демонстрировать, что система УК действует в соответствии с планом УК.

ACM_CAP.5.9C Документация УК должна содержать свидетельство, что система УК действительно сопровождала и продолжает эффективно сопровождать все элементы конфигурации.

ACM_CAP.5.10C Система УК должна предусмотреть такие меры, при которых в элементах конфигурации могут быть сделаны только санкционированные изменения.

ACM_CAP.5.11C Система УК должна поддерживать генерацию ОО.

ACM_CAP.5.12C План приемки должен содержать описание процедур, используемых для приемки модифицированного или вновь созданного элемента конфигурации как части ОО.

ACM_CAP.5.13C **Процедуры компоновки должны описать, как систему УК применяют в процессе изготовления ОО.**

ACM_CAP.5.14C Система УК должна содержать требование, чтобы лицо, ответственное за включение элемента конфигурации под УК, не являлось его разработчиком.

ACM_CAP.5.15C Система УК должна четко идентифицировать элементы конфигурации, которые составляют ФБО.

ACM_CAP.5.16C Система УК должна поддерживать аудит всех модификаций ОО с регистрацией, как минимум, инициатора, даты и времени модификации в журнале аудита.

ACM_CAP.5.17C Система УК должна быть способна идентифицировать оригиналы всех материалов, используемые для генерации ОО.

ACM_CAP.5.18C Документация УК должна демонстрировать, что использование системы УК совместно с мерами безопасности разработки сделает возможными только санкционированные изменения в ОО.

ACM_CAP.5.19C Документация УК должна демонстрировать, что использование процедур компоновки обеспечивает выполнение генерации ОО правильно и санкционированным способом.

ACM_CAP.5.20C Документация УК должна демонстрировать, что система УК достаточна для обеспечения того , чтобы лицо, ответственное за включение элемента конфигурации под УК, не было его разработчиком.

ACM_CAP.5.21C Документация УК должна содержать строгое обоснование, что процедуры приемки обеспечивают адекватный и удобный просмотр изменений всех элементов конфигурации.

Элементы действий оценщика

ACM_CAP.5.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

8.3 Область УК (ACM_SCP)

Цели

Цель этого семейства – обеспечить, чтобы все необходимые элементы конфигурации ОО отслеживались системой УК. Это способствует обеспечению защиты целостности элементов конфигурации с использованием возможностей системы УК.

Компонентами семейства может обеспечиваться отслеживание:

а) представления реализации ОО;

б) всей необходимой документации, включая сообщения о проблемах, возникающих во время разработки и эксплуатации;

в) опций конфигурации (например, ключей компилятора);

г) инструментальных средств разработки.

Ранжирование компонентов

Компоненты семейства ранжированы на основе того, что из перечисленного ниже отслеживается системой УК: представление реализации ОО, проектная документация, тестовая документация, документация пользователя, документация администратора, документация УК, недостатки безопасности, инструментальные средства разработки.

Замечания по применению

ACM_SCP.1.1C содержит требование, чтобы системой УК отслеживалось представление реализации ОО. Представление реализации ОО включает в себя все аппаратные, программные и программно-аппаратные средства, которые составляют ОО по существу. В случае, когда ОО состоит только из программных средств, представление реализации может состоять исключительно из исходного и объектного кода.

ACM_SCP.1.1C содержит также требование, чтобы системой УК отслеживалась документация УК. Документация включает в себя план УК, а также информацию относительно актуальных версий любых инструментальных средств, которые входят в состав системы УК.

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

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

ACM_SCP.1 Охват УК объекта оценки

Цели

Система УК может контролировать изменения только тех элементов, которые были включены под УК. Включение под УК представления реализации ОО, проектной и тестовой документации, документации администратора и пользователя и документации УК обеспечивает доверие, что они могут быть модифицированы только под контролем в соответствии с полномочиями.

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ACM_SCP.1.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_SCP.1.1C Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора и документацию УК.

ACM_SCP.1.2C **Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.**

Элементы действий оценщика

ACM_SCP.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ACM_SCP.2 Охват УК отслеживания проблем

Цели

Система УК может контролировать изменения только тех элементов, которые были включены под УК. Включение под УК представления реализации ОО, проектной и тестовой документации, документации администратора и пользователя и документации УК обеспечивает доверие, что они могут быть модифицированы только под контролем в соответствии с полномочиями.

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

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ACM_SCP.2.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_SCP.2.1C Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК **и недостатки безопасности**.

ACM_SCP.2.2C Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

Элементы действий оценщика

ACM_SCP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ACM_SCP.3 Охват УК инструментальных средств разработки

Цели

Система УК может контролировать изменения только тех элементов, которые были включены под УК. Включение под УК представления реализации ОО, проектной и тестовой документации, документации администратора и пользователя и документации УК обеспечивает доверие к тому, что они могут быть модифицированы только под контролем в соответствии с полномочиями.

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

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

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ACM_SCP.3.1D Разработчик должен представить документацию УК.

Элементы содержания и представления свидетельств

ACM_SCP.3.1C Документация УК должна показать, что система УК, как минимум, отслеживает: представление реализации ОО, проектную документацию, тестовую документацию, документацию пользователя, документацию администратора, документацию УК, недостатки безопасности **и инструментальные средства разработки и связанную с ними информацию.**

ACM_SCP.3.2C Документация УК должна содержать описание, как элементы конфигурации отслеживаются системой УК.

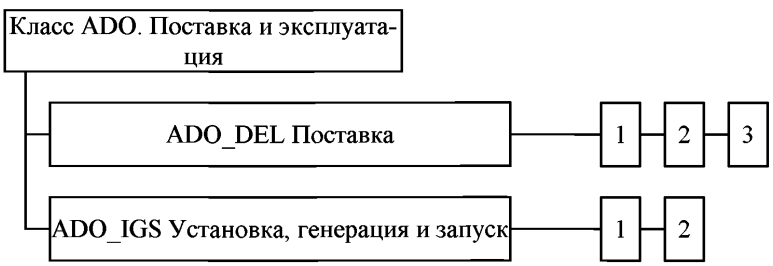
Элементы действий оценщика

ACM_SCP.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

9 Класс ADO. Поставка и эксплуатация

Класс "Поставка и эксплуатация" содержит требования правильной поставки, установки, генерации и запуска ОО.

На рисунке 9.1 показаны семейства этого класса и иерархия компонентов в семей-



ствах.

Рисунок 9.1 – Декомпозиция класса " Поставка и эксплуатация "

9.1 Поставка (ADO_DEL)

Цели

Требования для поставки предусматривают такие средства и процедуры контроля и распространения системы, которые обеспечивают доверие к тому, что потребитель получит именно тот ОО, который отправитель намеревался отослать, без каких-либо модификаций. Правильно выполненная поставка предполагает необходимость точного соответствия полученной версии оригиналу ОО, исключая, таким образом, как любое вмешательство в актуальную версию, так и подмену ее фальсифицированной версией.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе повышения требований к разработчику, позволяющих обнаружить и предотвратить модификации ОО во время его поставки.

ADO_DEL.1 Процедуры поставки

Зависимости отсутствуют.

Элементы действий разработчика

ADO_DEL.1.1D **Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.**

ADO_DEL.1.2.D **Разработчик должен использовать процедуры поставки.**

Элементы содержания и представления свидетельств

ADO_DEL.1.1C **Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.**

Элементы действий оценщика

ADO_DEL.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADO_DEL.2 Обнаружение модификации

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ADO_DEL.2.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.2.2 Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.2.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий к местам использования.

ADO_DEL.2.2C **Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают обнаружение модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.**

ADO_DEL.2.3C **Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.**

Элементы действий оценщика

ADO_DEL.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_DEL.3 Предотвращение модификации

Зависимости

ACM_CAP.3 Средства контроля авторизации

Элементы действий разработчика

ADO_DEL.3.1D Разработчик должен задокументировать процедуры поставки ОО или его частей пользователю.

ADO_DEL.3.2D Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ADO_DEL.3.1C Документация поставки должна содержать описание всех процедур, необходимых для поддержки безопасности при распространении версий ОО к местам использования.

ADO_DEL.3.2C Документация поставки должна содержать описание, как различные процедуры и технические меры обеспечивают **предотвращение** модификаций или любого расхождения между оригиналом разработчика и версией, полученной в месте использования.

ADO_DEL.3.3C Документация поставки должна содержать описание, как различные процедуры позволяют обнаружить попытку подмены от имени разработчика, даже в тех случаях, когда разработчик ничего не отсылал к месту использования.

Элементы действий оценщика

ADO_DEL.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

9.2 Установка, генерация и запуск (ADO_IGS)

Цели

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

Ранжирование компонентов

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

Замечания по применению

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

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

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

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

ADO_IGS.1 Процедуры установки, генерации и запуска

Зависимости

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

ADO_IGS.1.1D **Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.**

Элементы содержания и представления свидетельств

ADO_IGS.1.1C **Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.**

Элементы действий оценщика

ADO_IGS.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADO_IGS.1.2E **Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.**

ADO_IGS.2 Журнал регистрации генерации

Зависимости

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

ADO_IGS.2.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.2.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

ADO_IGS.2.2C **Документация должна содержать описание процедур, позволяющих таким образом создать журнал регистрации, содержащий применявшиеся опции генерации ОО, чтобы можно было точно определить, как и когда ОО был сгенерирован.**

Элементы действий оценщика

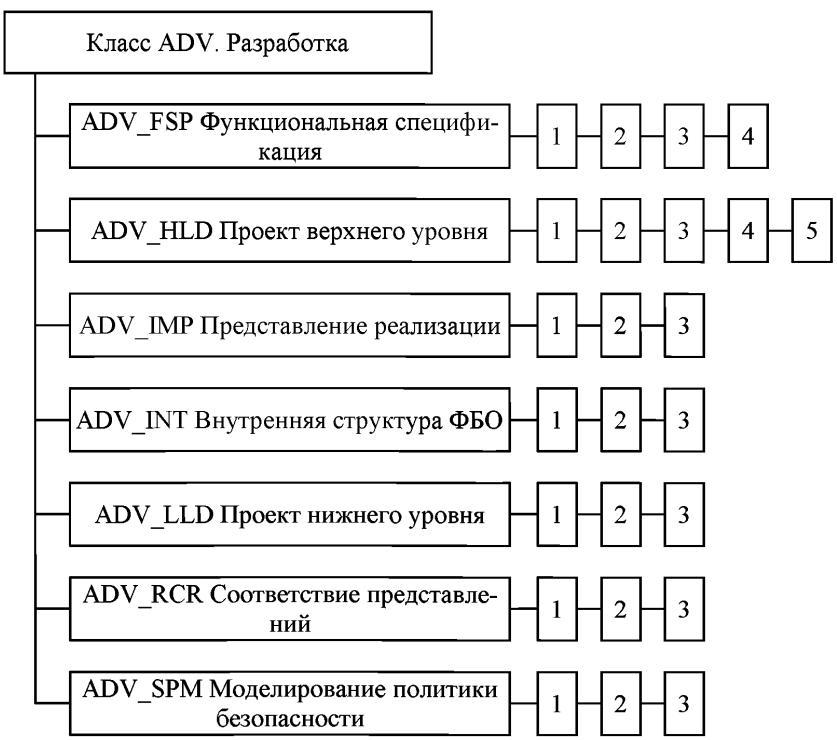
ADO_IGS.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.2.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

10 Класс ADV. Разработка

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

На рисунке 10.1 показаны семейства этого класса и иерархия компонентов в семей-



ствах.

Рисунок 10.1 – Декомпозиция класса "Разработка"

Парадигма, очевидная для этих семейств, – функциональная спецификация ФБО, разбиение ФБО на подсистемы, разбиение подсистем на модули, показ реализации модулей и демонстрация соответствия между всеми декомпозициями, которая представляется

как свидетельство. Требования для различных представлений ФБО разнесены по разным семействам, однако разработчику ПЗ/ЗБ дается возможность определить, какое именно подмножество представлений ФБО требуется.

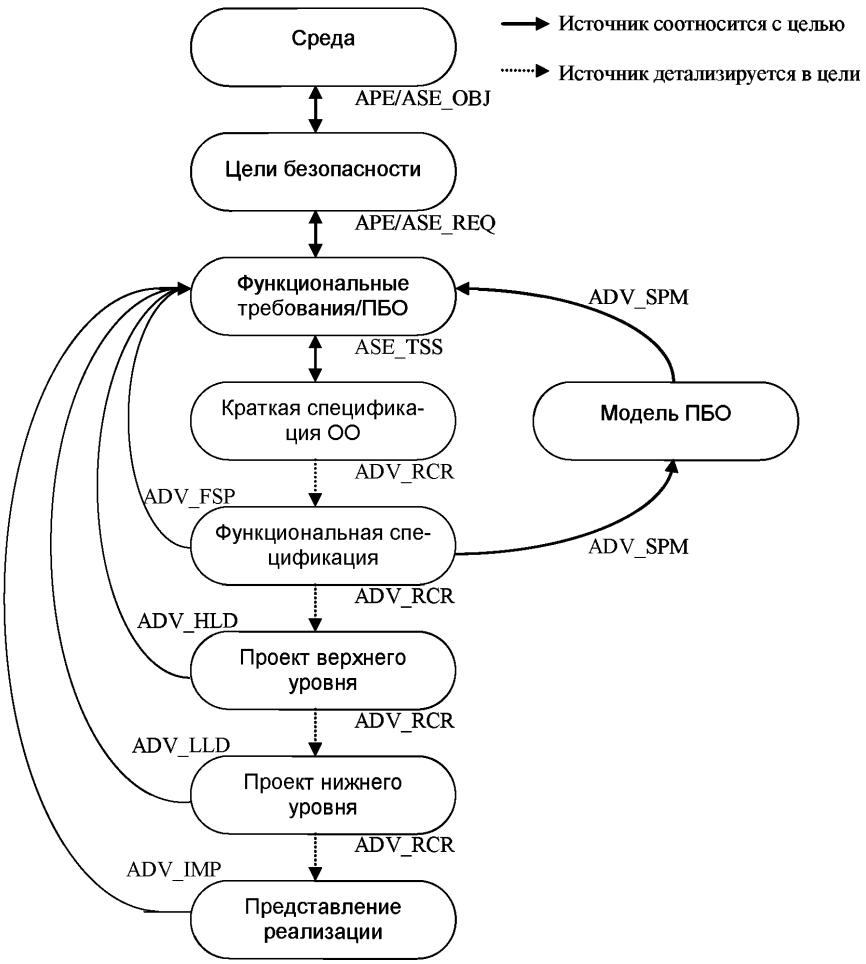


Рисунок 10.2 – Связи между представлениями ОО и требованиями

На рисунке 10.2 показаны связи между различными представлениями ФБО, целями и требованиями, с которыми они связаны. Классы APE и ASE определяют требования соответствия между функциональными требованиями и целями безопасности, а также между целями безопасности и ожидаемой средой ОО. Класс ASE также определяет требования к соответствию между целями безопасности, функциональными требованиями и краткой спецификацией ОО.

Требования для всех других соответствий, показанных на рисунке 10.2, определены в классе ADV. Семейство ADV_SPM определяет требования соответствия между ПБО и

моделью ПБО, а также между моделью ПБО и функциональной спецификацией. Семейство ADV_RCR определяет требования соответствия между всеми имеющимися представлениями ФБО — от краткой спецификации ОО до представления реализации. Наконец, каждое семейство доверия, относящееся к конкретному представлению ФБО (т.е. ADV_FSP, ADV_HLD, ADV_LLD и ADV_IMP), определяет требования, устанавливающие связь между представлением ФБО и функциональными требованиями, сочетание которых помогает убедиться в том, что функциональные требования безопасности ОО были учтены. Анализ прослеживания будет выполняться всегда, начиная с самого высокого уровня представления ФБО, включая каждое из имеющихся представлений ФБО. ОК реализуют это требование прослеживания, используя зависимости от семейства ADV_RCR. Семейство ADV_INT не представлено на рисунке 10.2, поскольку оно связано с внутренней структурой ФБО и имеет лишь косвенное отношение к процессу уточнения представлений ФБО.

Замечания по применению

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

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

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

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

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

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

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

Существенное доверие может быть достигнуто через обеспечение прослеживания ФБО до каждого из его представлений и соответствия модели ПБО функциональной спецификации. Семейство ADV_RCR содержит требования к отображению соответствия между различными представлениями ФБО, а семейство ADV_SPM – между моделью ПБО и функциональной спецификацией. Соответствие может принять форму либо неформальной или полуформальной демонстрации, либо формального доказательства.

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

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

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

Элементы ADV_RCR.*.1C содержат требование, чтобы разработчик представил свидетельство для каждой смежной пары представлений ФБО, что все относящиеся к безопасности функциональные возможности более абстрактного представления ФБО уточнены в менее абстрактном представлении ФБО. Каждый из элементов ADV_FSP.*.2E, ADV_HLD.*.2E, ADV_LLD.*.2E и ADV_IMP.*.2E содержит требование, чтобы оценщик сделал заключение о том, что ФБО, представляемые этим семейством требований – точное

и полное отображение функциональных требований безопасности ОО. Чтобы сделать заключение, что представление ФБО является точным и полным отображением функциональных требований безопасности ОО, предполагается, что оценщик использует свидетельство, предоставленное разработчиком в ADV_RCR.*.1C, как основание для этого заключения. Устанавливая соответствие между функциональными требованиями безопасности ОО и каждым из цепочки последовательных представлений ФБО, этот пошаговый процесс предоставит, в конечном счете, более высокое доверие соответствию наименее абстрактного представления ФБО функциональным требованиям безопасности ОО, что и является конечной целью этого класса. Если оценщик не устанавливает соответствие функциональным требованиям безопасности ОО для промежуточных представлений ФБО, то попытка сделать заключение о соответствии наименее абстрактного представления ФБО функциональным требованиям безопасности ОО может представлять собой слишком большой шаг для точного выполнения. И, наконец, в зависимости от требуемой совокупности представлений ФБО, вполне возможно, что проект нижнего уровня, проект верхнего уровня или даже функциональная спецификация может являться наименее абстрактным имеющимся представлением ФБО.

10.1 Функциональная спецификация (ADV_FSP)

Цели

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

Ранжирование компонентов

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

Замечания по применению

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

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

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

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

ADV_FSP.1 Неформальная функциональная спецификация

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_FSP.1.1D **Разработчик должен представить функциональную спецификацию.**

Элементы содержания и представления свидетельств

ADV_FSP.1.1C **Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.**

ADV_FSP.1.2C **Функциональная спецификация должна быть внутренне непротиворечивой.**

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

ADV_FSP.1.4C **Функциональная спецификация должна полностью представить ФБО.**

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 – точное и полное отображение функциональных требований безопасности ОО.**

ADV_FSP.2 Полностью определенные внешние интерфейсы

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_FSP.2.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.2.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.2.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.2.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.2.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.2.5C **Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.**

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 – точное и полное отображение функциональных требований безопасности ОО.

ADV_FSP.3 Полуформальная функциональная спецификация

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_FSP.3.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.3.1C Функциональная спецификация должна содержать **полуформальное** описание ФБО и их внешних интерфейсов, **поддержанное, где это необходимо, неформальным пояснительным текстом**.

ADV_FSP.3.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.3.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.3.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.3.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

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 – точное и полное отображение функциональных требований безопасности ОО.

ADV_FSP.4 Формальная функциональная спецификация

Зависимости

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_FSP.4.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.4.1C Функциональная спецификация должна содержать **формальное** описание ФБО и их внешних интерфейсов, поддержанное, где это необходимо, неформальным пояснительным текстом.

ADV_FSP.4.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.4.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.4.4C Функциональная спецификация должна полностью представить ФБО.

ADV_FSP.4.5C Функциональная спецификация должна включать в себя логическое обоснование, что ФБО полностью представлены.

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 – точное и полное отображение функциональных требований безопасности ОО.

10.2 Проект верхнего уровня (ADV_HLD)

Цели

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

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

Ранжирование компонентов

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

Замечания по применению

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

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

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

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

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

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

ADV_HLD.1 Описательный проект верхнего уровня

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_HLD.1.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.1.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.1.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.1.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.1.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.1.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.1.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.1.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

Элементы действий оценщика

ADV_HLD.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.1.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_HLD.2.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.2.1C Представление проекта верхнего уровня должно быть неформальным.

ADV_HLD.2.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.2.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.2.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.2.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.2.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.2.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.2.8C **Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.**

ADV_HLD.2.9C **Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.**

Элементы действий оценщика

ADV_HLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.2.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.3 Полуформальный проект верхнего уровня

Зависимости

ADV_FSP.3 Полуформальная функциональная спецификация

ADV_RCR.2 Полуформальная демонстрация соответствия

Элементы действий разработчика

ADV_HLD.3.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.3.1C Представление проекта верхнего уровня должно быть **полуформальным**.

ADV_HLD.3.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.3.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.3.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.3.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.3.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.3.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.3.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая **полную** детализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.3.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_HLD.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.3.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.4 Пояснения в полуформальном проекте верхнего уровня

Зависимости

ADV_FSP.3 Полуформальная функциональная спецификация

ADV_RCR.2 Полуформальная демонстрация соответствия

Элементы действий разработчика

ADV_HLD.4.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.4.1C Представление проекта верхнего уровня должно быть полуформальным.

ADV_HLD.4.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.4.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.4.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.4.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.4.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.4.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.4.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.4.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

ADV_HLD.4.10C **Проект верхнего уровня должен содержать строгое обоснование, что идентифицированный способ выполнения разделения, в том числе любых механизмов защиты, достаточен для обеспечения четкого и эффективного отделения функций, осуществляющих ПБО, от функций, не участвующих в осуществлении ПБО.**

ADV_HLD.4.11C **Проект верхнего уровня должен содержать строгое обоснование, что механизмы ФБО достаточны для реализации функций безопасности, идентифицированных в проекте верхнего уровня.**

Элементы действий оценщика

ADV_HLD.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.4.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_HLD.5 Формальный проект верхнего уровня

Зависимости

ADV_FSP.4 Формальная функциональная спецификация

ADV_RCR.3 Формальная демонстрация соответствия

Элементы действий разработчика

ADV_HLD.5.1D Разработчик должен представить проект верхнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_HLD.5.1C Представление проекта верхнего уровня должно быть **формальным**.

ADV_HLD.5.2C Проект верхнего уровня должен быть внутренне непротиворечивым.

ADV_HLD.5.3C Проект верхнего уровня должен содержать описание структуры ФБО в терминах подсистем.

ADV_HLD.5.4C Проект верхнего уровня должен содержать описание функциональных возможностей безопасности, предоставленных каждой подсистемой ФБО.

ADV_HLD.5.5C Проект верхнего уровня должен идентифицировать все базовые аппаратные, программно-аппаратные и/или программные средства, требуемые для реализации ФБО, с представлением функций, обеспечиваемых поддержкой механизмов защиты, реализуемых этими средствами.

ADV_HLD.5.6C Проект верхнего уровня должен идентифицировать все интерфейсы для подсистем ФБО.

ADV_HLD.5.7C Проект верхнего уровня должен идентифицировать, какие из интерфейсов подсистем ФБО являются видимыми извне.

ADV_HLD.5.8C Проект верхнего уровня должен содержать описание назначения и методов использования всех интерфейсов подсистем ФБО, обеспечивая полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

ADV_HLD.5.9C Проект верхнего уровня должен содержать описание разделения ОО на подсистемы, осуществляющие ПБО, и прочие.

ADV_HLD.5.10C Проект верхнего уровня должен содержать строгое обоснование, что идентифицированный способ выполнения разделения, в том числе любых механизмов защиты, достаточен для обеспечения четкого и эффективного отделения функций, осуществляющих ПБО, от функций, не участвующих в осуществлении ПБО.

ADV_HLD.5.11C Проект верхнего уровня должен содержать строгое обоснование, что механизмы ФБО достаточны для реализации функций безопасности, идентифицированных в проекте верхнего уровня.

Элементы действий оценщика

ADV_HLD.5.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_HLD.5.2E Оценщик должен сделать независимое заключение, что проект верхнего уровня – точное и полное отображение функциональных требований безопасности ОО.

10.3 Представление реализации (ADV_IMP)

Цели

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

Ранжирование компонентов

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

Замечания по применению

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

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

ADV_IMP.1 Подмножество реализации ФБО

Замечания по применению

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

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

Зависимости

ADV_LLD.1 Описательный проект нижнего уровня

ADV_RCR.1 Неформальная демонстрация соответствия

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ADV_IMP.1.1D **Разработчик должен обеспечить представление реализации для выбранного подмножества ФБО.**

Элементы содержания и представления свидетельств

ADV_IMP.1.1C **Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.**

ADV_IMP.1.2C **Представление реализации должно быть внутренне непротиворечивым.**

Элементы действий оценщика

ADV_IMP.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADV_IMP.1.2E **Оценщик должен сделать независимое заключение, что наименее абстрактное представление ФБО – точное и полное отображение функциональных требований безопасности ОО.**

ADV_IMP.2 Реализация ФБО

Замечания по применению

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

Зависимости

ADV_LLD.1 Описательный проект нижнего уровня

ADV_RCR.1 Неформальная демонстрация соответствия

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ADV_IMP.2.1D Разработчик должен обеспечить представление реализации для **всех** ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.2.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.2.2C Представление реализации должно быть внутренне непротиворечивым.

ADV_IMP.2.3C **Представление реализации должно включать в себя описание взаимосвязей между всеми частями реализации.**

Элементы действий оценщика

ADV_IMP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_IMP.2.2E Оценщик должен сделать независимое заключение, что **представление реализации** – точное и полное отображение функциональных требований безопасности ОО.

ADV_IMP.3 Структурированная реализация ФБО

Замечания по применению

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

Зависимости

ADV_INT.1 Модульность

ADV_LLD.1 Описательный проект нижнего уровня

ADV_RCR.1 Неформальная демонстрация соответствия

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Элементы действий разработчика

ADV_IMP.3.1D Разработчик должен обеспечить представление реализации для всех ФБО.

Элементы содержания и представления свидетельств

ADV_IMP.3.1C Представление реализации должно однозначно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дальнейших проектных решений.

ADV_IMP.3.2C Представление реализации должно быть внутренне непротиворечивым.

ADV_IMP.3.3C Представление реализации должно включать в себя описание взаимосвязей между всеми частями реализации.

ADV_IMP.3.4C **Представление реализации должно быть структурировано в малые и понятные разделы.**

Элементы действий оценщика

ADV_IMP.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_IMP.3.2E Оценщик должен сделать независимое заключение, что представление реализации – точное и полное отображение функциональных требований безопасности ОО.

10.4 Внутренняя структура ФБО (ADV_INT)

Цели

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

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

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

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

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

Ранжирование компонентов

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

Замечания по применению

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

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

ADV_INT.2.6C обращается к концепции монитора обращений, требуя минимизацию сложности тех частей ФБО, которые осуществляют политики управления доступом

и/или управления информационными потоками, идентифицированные в ПБО. ADV_INT.3.6C развивает далее концепцию монитора обращений, требуя минимизацию сложности всех ФБО.

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

ADV_INT.1 Модульность

Зависимости

ADV_IMP.1 Подмножество реализации ФБО

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_INT.1.1D **Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.**

ADV_INT.1.2D **Разработчик должен представить описание архитектуры.**

Элементы содержания и представления свидетельств

ADV_INT.1.1C **Описание архитектуры должно идентифицировать модули ФБО.**

ADV_INT.1.2C **Описание архитектуры должно содержать изложение назначения, интерфейсов, параметров и результатов применения каждого модуля ФБО.**

ADV_INT.1.3C **Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.**

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 сделать независимое заключение, что и проект нижнего уровня, и представление реализации согласуются с описанием архитектуры.**

ADV_INT.2 Уменьшение сложности

Замечания по применению

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

Зависимости

ADV_IMP.1 Подмножество реализации ФБО

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_INT.2.1D Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.

ADV_INT.2.2D Разработчик должен представить описание архитектуры.

ADV_INT.2.3D **Разработчик должен проектировать и структурировать ФБО по уровням с минимизацией взаимных связей между уровнями проекта.**

ADV_INT.2.4D **Разработчик должен проектировать и структурировать ФБО способом, минимизирующим сложность тех частей ФБО, которые осуществляют какие-либо политики управления доступом и/или информационными потоками.**

Элементы содержания и представления свидетельств

ADV_INT.2.1C Описание архитектуры должно идентифицировать модули ФБО **и специфицировать, какие части ФБО осуществляют политики управления доступом и/или информационными потоками**.

ADV_INT.2.2C Описание архитектуры должно содержать изложение назначения, интерфейсов, параметров и результатов применения каждого модуля ФБО.

ADV_INT.2.3C Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.

ADV_INT.2.4C **Описание архитектуры должно показать ее разбиение на уровни.**

ADV_INT.2.5C **Описание архитектуры должно показать, что взаимные связи были минимизированы, и содержать строгое обоснование оставшихся связей.**

ADV_INT.2.6C **Описание архитектуры должно содержать изложение, каким образом части ФБО, которые осуществляют любые политики управления доступом и/или информационными потоками, структурированы для минимизации сложности.**

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

ADV_INT.3 Минимизация сложности

Замечания по применению

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

Зависимости

ADV_IMP.2 Реализация ФБО

ADV_LLD.1 Описательный проект нижнего уровня

Элементы действий разработчика

ADV_INT.3.1D Разработчик должен проектировать и структурировать ФБО в модульном виде, избегая необязательных связей между модулями проекта.

ADV_INT.3.2D Разработчик должен представить описание архитектуры.

ADV_INT.3.3D Разработчик должен проектировать и структурировать ФБО по уровням с минимизацией взаимных связей между уровнями проекта.

ADV_INT.3.4D Разработчик должен проектировать и структурировать ФБО способом, минимизирующим сложность **ФБО в целом**.

ADV_INT.3.5D **Разработчик должен проектировать и структурировать части ФБО, которые осуществляют какие-либо политики управления доступом и/или информационными потоками так, чтобы они были достаточно простыми для анализа.**

ADV_INT.3.6D **Разработчик должен обеспечить, чтобы функции, цели которых не имеют отношения к безопасности, были устранены из модулей ФБО.**

Элементы содержания и представления свидетельств

ADV_INT.3.1C Описание архитектуры должно идентифицировать модули ФБО и специфицировать, какие части ФБО осуществляют политики управления доступом и/или управления информационными потоками.

ADV_INT.3.2C Описание архитектуры должно содержать изложение назначения, интерфейса, параметров и результатов применения каждого модуля ФБО.

ADV_INT.3.3C Описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия.

ADV_INT.3.4C Описание архитектуры должно показать ее разбиение на уровни.

ADV_INT.3.5C Описание архитектуры должно показать, что взаимные связи были минимизированы, и содержать строгое обоснование оставшихся связей.

ADV_INT.3.6C Описание архитектуры должно содержать изложение, каким образом **все ФБО** структурированы для минимизации сложности.

ADV_INT.3.7C **Описание архитектуры должно содержать строгое обоснование включения в ФБО каждого модуля, не участвующего в осуществлении ПБО.**

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

ADV_INT.3.3E **Оценщик должен подтвердить, что части ФБО, которые осуществляют какие-либо политики управления доступом и/или информационными потоками, достаточно просты для анализа.**

10.5 Проект нижнего уровня (ADV_LLD)

Цели

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

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

Ранжирование компонентов

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

Замечания по применению

Выражение "модуль, осуществляющий ПБО" относится к любому модулю, направленному на осуществление ПБО.

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

Элементы ADV_LLD.*.6C содержат требование, чтобы проект нижнего уровня описал, как обеспечивается каждая из функций, осуществляющих ПБО. Смысл этого требования состоит в том, чтобы проект нижнего уровня содержал описание того, как планируется реализовать каждый модуль, исходя из перспективы проекта.

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

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

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

ADV_LLD.1 Описательный проект нижнего уровня

Зависимости

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_LLD.1.1D **Разработчик должен представить проект нижнего уровня ФБО.**

Элементы содержания и представления свидетельств

ADV_LLD.1.1C **Представление проекта нижнего уровня должно быть неформальным.**

ADV_LLD.1.2C **Проект нижнего уровня должен быть внутренне непротиворечивым.**

ADV_LLD.1.3C **Проект нижнего уровня должен содержать описание ФБО в терминах модулей.**

ADV_LLD.1.4C **Проект нижнего уровня должен содержать описание назначения каждого модуля.**

ADV_LLD.1.5C **Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.**

ADV_LLD.1.6C **Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.**

ADV_LLD.1.7C **Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.**

ADV_LLD.1.8C **Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.**

ADV_LLD.1.9C **Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя, при необходимости, детализацию результатов, нештатных ситуаций и сообщений об ошибках.**

ADV_LLD.1.10C **Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.**

Элементы действий оценщика

ADV_LLD.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADV_LLD.1.2E **Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.**

ADV_LLD.2 Полуформальный проект нижнего уровня

Зависимости

ADV_HLD.3 Полуформальный проект верхнего уровня

ADV_RCR.2 Полуформальная демонстрация соответствия

Элементы действий разработчика

ADV_LLD.2.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.2.1C Представление проекта нижнего уровня должно быть **полуформальным**.

ADV_LLD.2.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.2.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.2.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.2.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.2.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.2.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.2.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.2.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя **полную** де-

тализацию **всех** результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.2.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_LLD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_LLD.2.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

ADV_LLD.3 Формальный проект нижнего уровня

Зависимости

ADV_HLD.5 Формальный проект верхнего уровня

ADV_RCR.3 Формальная демонстрация соответствия

Элементы действий разработчика

ADV_LLD.3.1D Разработчик должен представить проект нижнего уровня ФБО.

Элементы содержания и представления свидетельств

ADV_LLD.3.1C Представление проекта нижнего уровня должно быть **формальным**.

ADV_LLD.3.2C Проект нижнего уровня должен быть внутренне непротиворечивым.

ADV_LLD.3.3C Проект нижнего уровня должен содержать описание ФБО в терминах модулей.

ADV_LLD.3.4C Проект нижнего уровня должен содержать описание назначения каждого модуля.

ADV_LLD.3.5C Проект нижнего уровня должен определить взаимосвязи между модулями в терминах предоставляемых функциональных возможностей безопасности и зависимостей от других модулей.

ADV_LLD.3.6C Проект нижнего уровня должен содержать описание, как предоставляется каждая из функций, осуществляющих ПБО.

ADV_LLD.3.7C Проект нижнего уровня должен идентифицировать все интерфейсы модулей ФБО.

ADV_LLD.3.8C Проект нижнего уровня должен идентифицировать, какие из интерфейсов модулей ФБО являются видимыми извне.

ADV_LLD.3.9C Проект нижнего уровня должен содержать описание назначения и методов использования всех интерфейсов модулей ФБО, предоставляя полную детализацию всех результатов, нештатных ситуаций и сообщений об ошибках.

ADV_LLD.3.10C Проект нижнего уровня должен содержать описание разделения ОО на модули, осуществляющие ПБО, и прочие.

Элементы действий оценщика

ADV_LLD.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_LLD.3.2E Оценщик должен сделать независимое заключение, что проект нижнего уровня – точное и полное отображение функциональных требований безопасности ОО.

10.6 Соответствие представлений (ADV_RCR)

Цели

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

Ранжирование компонентов

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

Замечания по применению

Необходимо, чтобы разработчик продемонстрировал оценщику, что наиболее детализированное или наименее абстрактное имеющееся представление ФБО – точное, непротиворечивое и полное отображение функций, выраженных как функциональные требования в ЗБ. Это выполняют путем показа соответствия между смежными представлениями на соразмерном уровне строгости.

Семейство ADV_RCR не связано с требованиями соответствия ПБО или модели ПБО. В этом семействе, как показано на рисунке 10.2, рассмотрено соответствие между различными представлениями ФБО (т.е. краткой спецификацией ОО, функциональной спецификацией, проектом верхнего уровня, проектом нижнего уровня и представлением реализации).

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

более абстрактного представления ФБО были уточнены в менее абстрактном представлении ФБО.

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

ADV_RCR.1 Неформальная демонстрация соответствия

Зависимости отсутствуют.

Элементы действий разработчика

ADV_RCR.1.1D **Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.**

Элементы содержания и представления свидетельств

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

Элементы действий оценщика

ADV_RCR.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADV_RCR.2 Полуформальная демонстрация соответствия

Зависимости отсутствуют.

Элементы действий разработчика

ADV_RCR.2.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.2.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

ADV_RCR.2.2C **Для каждой смежной пары имеющихся представлений ФБО, где части обоих представлений специфицированы, по меньшей мере, полуформально, демонстрация соответствия между этими частями представлений должна быть полуформальной.**

Элементы действий оценщика

ADV_RCR.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_RCR.3 Формальная демонстрация соответствия

Замечания по применению

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

Зависимости отсутствуют.

Элементы действий разработчика

ADV_RCR.3.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

ADV_RCR.3.2D **Для тех из соответствующих частей представлений, которые специфицированы формально, разработчик должен доказать это соответствие.**

Элементы содержания и представления свидетельств

ADV_RCR.3.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен **доказать или** демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности, правильно и полностью уточнены в менее абстрактном представлении ФБО.

ADV_RCR.3.2C Для каждой смежной пары имеющихся представлений ФБО, где части **одного** представления **специфицированы полуформально**, **а другого** – по меньшей мере, полуформально, демонстрация соответствия между этими частями представлений должна быть полуформальной.

ADV_RCR.3.3C **Для каждой смежной пары имеющихся представлений ФБО, где части обоих представлений специфицированы формально, доказательство соответствия между этими частями представлений должно быть формальным.**

Элементы действий оценщика

ADV_RCR.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_RCR.3.2E **Оценщик должен сделать независимое заключение о правильности доказательств соответствия, избирательно верифицируя формальный анализ.**

10.7 Моделирование политики безопасности (ADV_SPM)

Цели

Цель этого семейства – повысить доверие, что функции безопасности в функциональной спецификации осуществляют политики ПБО. Это выполняется посредством разработки модели политики безопасности, которая основана на подмножестве политик ПБО, и установления соответствия между функциональной спецификацией, моделью политики безопасности и этим подмножеством политик ПБО.

Ранжирование компонентов

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

Замечания по применению

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

В каждом из компонентов этого семейства присутствует требование описания в модели ПБО правил и характеристик применяемых политик ПБО и обеспечения, чтобы модель ПБО была адекватна соответствующим политикам ПБО. "Правила" и "характеристики" модели ПБО предназначены для обеспечения гибкости в выборе типа модели (например, переход из одного состояния в другое, невмешательство), которая может быть разработана. Например, правила могут быть представлены как "свойства" (например, простое свойство безопасности, при которой уровень доступа субъекта выше уровня доступа к объекту или равен ему), а характеристики могут быть представлены такими определениями, как "начальное состояние", "безопасное состояние", "субъекты" и "объекты".

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

ADV_SPM.1 Неформальная модель политики безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_SPM.1.1D **Разработчик должен представить модель ПБО.**

ADV_SPM.1.2D **Разработчик должен демонстрировать соответствие между функциональной спецификацией и моделью ПБО.**

Элементы содержания и представления свидетельств

ADV_SPM.1.1C **Модель ПБО должна быть неформальной.**

ADV_SPM.1.2C **Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.**

ADV_SPM.1.3C **Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.**

ADV_SPM.1.4C **Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.**

Элементы действий оценщика

ADV_SPM.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ADV_SPM.2 Полуформальная модель политики безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_SPM.2.1D Разработчик должен представить модель ПБО.

ADV_SPM.2.2D Разработчик должен демонстрировать соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.2.1C Модель ПБО должна быть **полуформальной.**

ADV_SPM.2.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.2.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.2.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

ADV_SPM.2.5C **Там, где функциональная спецификация, по меньшей мере, полуформальна, демонстрация соответствия между моделью ПБО и функциональной спецификацией должна быть полуформальной.**

Элементы действий оценщика

ADV_SPM.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_SPM.3 Формальная модель политики безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_SPM.3.1D Разработчик должен представить модель ПБО.

ADV_SPM.3.2D Разработчик должен демонстрировать **или доказать, где это требуется**, соответствие между функциональной спецификацией и моделью ПБО.

Элементы содержания и представления свидетельств

ADV_SPM.3.1C Модель ПБО должна быть **формальной.**

ADV_SPM.3.2C Модель ПБО должна содержать описание правил и характеристик всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.3.3C Модель ПБО должна включать в себя логическое обоснование, которое демонстрирует, что она согласована и полна относительно всех политик ПБО, которые могут быть смоделированы.

ADV_SPM.3.4C Демонстрация соответствия между моделью ПБО и функциональной спецификацией должна показать, что все функции безопасности в функциональной спецификации являются непротиворечивыми и полными относительно модели ПБО.

ADV_SPM.3.5C Там, где функциональная спецификация **полуформальна**, демонстрация соответствия между моделью ПБО и функциональной спецификацией должна быть полуформальной.

ADV_SPM.3.6C **Там, где функциональная спецификация формальна, доказательство соответствия между моделью ПБО и функциональной спецификацией должно быть формальным.**

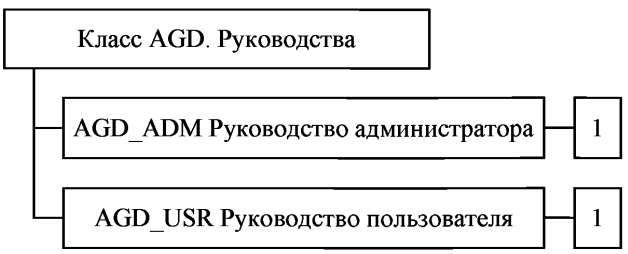
Элементы действий оценщика

ADV_SPM.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

11 Класс AGD. Руководства

Класс "Руководства" предоставляет требования к содержанию "Руководства администратора" и "Руководства пользователя". Для безопасного администрирования и использования ОО необходимо описать все аспекты, относящиеся к безопасному применению ОО.

На рисунке 11.1 показаны семейства этого класса и иерархия компонентов в семей-



ствах.

Рисунок 11.1 – Декомпозиция класса "Руководства"

11.1 Руководство администратора (AGD_ADM)

Цели

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

Ранжирование компонентов

Это семейство содержит только один компонент.

Замечания по применению

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

Понятие безопасных значений, как оно используется в AGD_ADM.1.5C, уместно при управлении администратором параметрами безопасности. В руководстве необходимо представить безопасные и опасные устанавливаемые значения для таких параметров. Это понятие связано с применением компонента FMT_MSA.2 из части 2 ОК.

AGD_ADM.1 Руководство администратора

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

AGD_ADM.1.1D **Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.**

Элементы содержания и представления свидетельств

AGD_ADM.1.1C **Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.**

AGD_ADM.1.2C **Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.**

AGD_ADM.1.3C **Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.**

AGD_ADM.1.4C **Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.**

AGD_ADM.1.5C **Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.**

AGD_ADM.1.6C **Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.**

AGD_ADM.1.7C **Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.**

AGD_ADM.1.8C **Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.**

Элементы действий оценщика

AGD_ADM.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

11.2 Руководство пользователя (AGD_USR)

Цели

Руководство пользователя относится к материалам, предназначенным для применения пользователями ОО, не связанными с администрированием, и другими лицами (например, программистами), использующими внешние интерфейсы ОО. Руководство описывает доступные пользователям функции безопасности, входящие в состав ФБО, и содержит инструкции и предписания, включая предупреждения, по их безопасному использованию.

Руководство пользователя предоставляет основание для предположений об использовании ОО и обеспечивает уверенность в том, что лояльные пользователи, поставщики приложений и прочие лица, использующие внешние интерфейсы ОО, поймут, как безопасно эксплуатировать ОО, и будут использовать его в соответствии с предназначением.

Ранжирование компонентов

Это семейство содержит только один компонент.

Замечания по применению

Требования AGD_USR.1.3C и AGD_USR.1.5C касаются того аспекта, что в руководстве пользователя приемлемо отражены все упомянутые в ПЗ/ЗБ предупреждения пользователям ОО, относящиеся к среде безопасности и целям безопасности ОО.

Во многих случаях может оказаться целесообразным, чтобы руководство было представлено раздельными документами: один для пользователей, а другой для прикладных программистов и/или проектировщиков аппаратных средств, использующих программные или аппаратные интерфейсы.

AGD_USR.1 Руководство пользователя

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

AGD_USR.1.1D **Разработчик должен представить руководство пользователя.**

Элементы содержания и представления свидетельств

AGD_USR.1.1C **Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.**

AGD_USR.1.2C **Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.**

AGD_USR.1.3C **Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.**

AGD_USR.1.4C **Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.**

AGD_USR.1.5C **Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.**

AGD_USR.1.6C **Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.**

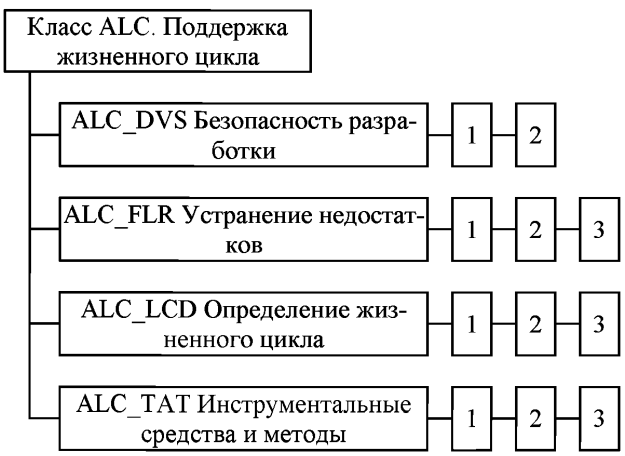
Элементы действий оценщика

AGD_USR.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

12 Класс ALC. Поддержка жизненного цикла

Поддержка жизненного цикла является аспектом установления дисциплины и контроля в процессе уточнения ОО во время его разработки и сопровождения. Уверенность в соответствии ОО требованиям безопасности к ОО больше, если анализ безопасности и формирование свидетельств выполняют на регулярной основе как неотъемлемую часть деятельности при разработке и сопровождении.

На рисунке 12.1 показаны семейства этого класса и иерархия компонентов в семей-



ствах.

Рисунок 12.1 – Декомпозиция класса "Поддержка жизненного цикла"

12.1 Безопасность разработки (ALC_DVS)

Цели

Безопасность разработки связана с физическими, процедурными, относящимися к персоналу и другими мерами безопасности, которые могут применяться в среде разработки для защиты ОО. Она включает в себя физическую безопасность места разработки и любые процедуры, связанные с отбором персонала разработчиков.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе того, требуется ли строгое обоснование достаточности мер безопасности.

Замечания по применению

Семейство ALC_DVS связано с мерами по устранению или уменьшению угроз, существующих в месте разработки. Напротив, угрозы, противостоять которым предполагается по месту эксплуатации ОО, обычно учитывают в разделе "Среда безопасности" ПЗ или ЗБ.

Оценщику следует сделать заключение, необходимо ли ему посетить место разработки для подтверждения выполнения требований этого семейства.

Известно, что конфиденциальность не всегда может включаться в задачи защиты ОО в среде его разработки. Использование слова "необходимый" ("necessary") предусматривает возможность выбора соответствующих мер защиты.

ALC_DVS.1 Идентификация мер безопасности

Зависимости отсутствуют.

Элементы действий разработчика

ALC_DVS.1.1D **Разработчик должен иметь документацию по безопасности разработки.**

Элементы содержания и представления свидетельств

ALC_DVS.1.1C **Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.**

ALC_DVS.1.2C **Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.**

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 применение мер безопасности.**

ALC_DVS.2 Достаточность мер безопасности

Зависимости отсутствуют.

Элементы действий разработчика

ALC_DVS.2.1D Разработчик должен иметь документацию по безопасности разработки.

Элементы содержания и представления свидетельств

ALC_DVS.2.1C Документация по безопасности разработки должна содержать описание всех физических, процедурных, относящихся к персоналу и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

ALC_DVS.2.2C Документация по безопасности разработки должна предоставить свидетельство, что необходимые меры безопасности соблюдаются во время разработки и сопровождения ОО.

ALC_DVS.2.3C **Свидетельство должно содержать строгое обоснование, что меры безопасности обеспечивают необходимый уровень защиты 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 применение мер безопасности.

12.2 Устранение недостатков (ALC_FLR)

Цели

Семейство ALC_FLR содержит требование, чтобы обнаруженные недостатки безопасности были отслежены и исправлены разработчиком. Хотя при оценке ОО не может быть сделано заключение о его соответствии процедурам устранения недостатков в будущем, можно оценить политики и процедуры, которые предусмотрены разработчиком для отслеживания и исправления недостатков, а также распространения информации о недостатках и их исправлении.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе расширения области применения процедур устранения недостатков и повышения строгости политик устранения недостатков.

Замечания по применению

Это семейство обеспечивает доверие к сопровождению и поддержке ОО в будущем, требуя от разработчика ОО отслеживать и исправлять недостатки в ОО. Кроме того, имеются требования по распространению сведений об исправлениях недостатков. Однако это семейство не налагает требований, выходящих за рамки текущей оценки.

В процедурах устранения недостатков следует описать методы реагирования на недостатки всех типов, которым необходимо противостоять. Некоторые недостатки не могут быть исправлены немедленно. Не исключено, что недостаток вообще не может быть исправлен, и необходимо применить другие (например, процедурные) меры. Представленную документацию следует распространить на процедуры по обеспечению исправлений в местах эксплуатации, а также для предоставления информации о недостатках, для которых исправление отложено (и что делать в этой ситуации) или невозможно.

ALC_FLR.1 Базовое устранение недостатков

Зависимости отсутствуют.

Элементы действий разработчика

ALC_FLR.1.1D **Разработчик должен задокументировать процедуры устранения недостатков.**

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 каждой редакции ОО.**

ALC_FLR.1.2C **Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.**

ALC_FLR.1.3C **Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.**

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.**

ALC_FLR.2 Процедуры сообщений о недостатках

Зависимости отсутствуют.

Элементы действий разработчика

ALC_FLR.2.1D Разработчик должен задокументировать процедуры устранения недостатков.

ALC_FLR.2.2D **Разработчик должен установить процедуру приема и отработки сообщений пользователей о недостатках безопасности и запросов на их исправление.**

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 каждой редакции ОО.

ALC_FLR.2.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.2.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

ALC_FLR.2.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО ин-

формации о недостатках, материалов исправлений и руководства по внесению исправлений.

ALC_FLR.2.5C **Процедуры обработки недостатков безопасности, ставших известными, должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а исправления изданы.**

ALC_FLR.2.6C **Процедуры обработки недостатков безопасности, ставших известными, должны предоставить такие меры безопасности, чтобы любые исправления этих недостатков не приводили к появлению новых.**

Элементы действий оценщика

ALC_FLR.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_FLR.3 Систематическое устранение недостатков

Зависимости отсутствуют.

Элементы действий разработчика

ALC_FLR.3.1D Разработчик должен задокументировать процедуры устранения недостатков.

ALC_FLR.3.2D Разработчик должен установить процедуру приема и отработки сообщений пользователей о недостатках безопасности и запросов на исправление этих недостатков.

ALC_FLR.3.3D **Разработчик должен указать один или несколько адресов для сообщений и запросов пользователей о проблемах безопасности, касающихся 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 выпуске ОО.

ALC_FLR.3.2C Процедуры устранения недостатков должны содержать требование представления описания природы и проявлений каждого недостатка безопасности, а также статуса завершения исправления этого недостатка.

ALC_FLR.3.3C Процедуры устранения недостатков должны содержать требование, чтобы действия по исправлению были идентифицированы для каждого недостатка безопасности.

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 обработки недостатков безопасности, ставших известными, должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а исправления изданы.

ALC_FLR.3.6C Процедуры обработки недостатков безопасности, ставших известными, должны предоставить такие меры безопасности, чтобы любые исправления этих недостатков не приводили к появлению новых.

ALC_FLR.3.7C **Процедуры устранения недостатков должны включать процедуру автоматического распространения сообщений о недостатках безопасности и их исправлении зарегистрированным пользователям, которым эти недостатки могут причинить ущерб.**

Элементы действий оценщика

ALC_FLR.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

12.3 Определение жизненного цикла (ALC_LCD)

Цели

Плохо управляемые разработка и сопровождение ОО могут приводить к неправильной реализации ОО (или к ОО, который отвечает не всем требованиям безопасности). Это, в свою очередь, приводит к нарушениям безопасности. Поэтому важно, чтобы в жизненном цикле ОО была как можно раньше установлена модель разработки и сопровождения ОО.

Использование модели разработки и сопровождения ОО не гарантирует, что ОО не будет содержать недостатки и будет отвечать всем функциональным требованиям безопасности. Может оказаться, что выбранная модель будет недостаточной или неадекватной, и поэтому выигрыш в качестве ОО не будет заметен. Использование модели жизненного цикла, которая одобрена некоторой группой экспертов (например, специалистами-теоретиками, органами стандартизации), повышает вероятность, что модель разработки и сопровождения будет содействовать достижению требуемого качества ОО.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе повышения требований к стандартизации и измеримости модели жизненного цикла, а также к согласованности с этой моделью.

Замечания по применению

Модель жизненного цикла объединяет процедуры, инструментальные средства и методы, используемые для разработки и сопровождения ОО. Аспекты процесса, которые могут быть охвачены такой моделью, включают в себя методы проектирования, процедуры просмотра, средства управления проектом, процедуры контроля изменений, 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 развитие.

Оценка аспектов сопровождения ОО повышает доверие к ОО за счет анализа информации о жизненном цикле ОО, представленной во время оценки до начала сопровождения.

Стандартизованная модель жизненного цикла — модель, которая была одобрена некоторой группой экспертов (например, специалистами-теоретиками, органами стандартизации).

Измеримая модель жизненного цикла — модель с количественными параметрами и/или метриками, используемыми для измерения характеристик разработки ОО (например, метрикой сложности исходного текста).

Модель жизненного цикла обеспечивает необходимый контроль за разработкой и сопровождением ОО, если разработчик может предоставить информацию, которая показала бы, что модель приемлемым образом минимизирует риск нарушений безопасности в ОО. При определении модели для части жизненного цикла после поставки ОО может быть полезна информация о предполагаемой среде ОО и целях безопасности ОО, приведенная в ЗБ.

ALC_LCD.1 Определение модели жизненного цикла разработчиком

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 за 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.**

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 ОО.

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.**

Элементы содержания и представления свидетельств

ALC_LCD.2.1C Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.

ALC_LCD.2.2C Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

ALC_LCD.2.3C **Документация по определению жизненного цикла должна объяснить выбор модели.**

ALC_LCD.2.4C **Документация по определению жизненного цикла должна объяснить, как модель используется при разработке и сопровождении ОО.**

ALC_LCD.2.5C **Документация по определению жизненного цикла должна демонстрировать согласованность со стандартизованной моделью жизненного цикла.**

Элементы действий оценщика

ALC_LCD.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_LCD.3 Измеримая модель жизненного цикла

Зависимости отсутствуют.

Элементы действий разработчика

ALC_LCD.3.1D Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.

ALC_LCD.3.2D Разработчик должен представить документацию по определению жизненного цикла.

ALC_LCD.3.3D Разработчик должен использовать стандартизованную **и измеримую** модель жизненного цикла для разработки и сопровождения ОО.

ALC_LCD.3.4D **Разработчик должен количественно оценить процесс разработки ОО, используя стандартизованную и измеримую модель жизненного цикла.**

Элементы содержания и представления свидетельств

ALC_LCD.3.1C Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО, **включая детализацию ее количественных параметров и/или метрик, используемых для оценки соответствия процесса разработки ОО принятой модели**.

ALC_LCD.3.2C Модель жизненного цикла должна обеспечить необходимый контроль за разработкой и сопровождением ОО.

ALC_LCD.3.3C Документация по определению жизненного цикла должна объяснить выбор модели.

ALC_LCD.3.4C Документация по определению жизненного цикла должна объяснить, как модель используется при разработке и сопровождении ОО.

ALC_LCD.3.5C Документация по определению жизненного цикла должна демонстрировать согласованность со стандартизованной **и измеримой** моделью жизненного цикла.

ALC_LCD.3.6C **Документация по жизненному циклу должна представить результаты количественной оценки процесса разработки ОО с использованием стандартизованной и измеримой модели жизненного цикла.**

Элементы действий оценщика

ALC_LCD.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

12.4 Инструментальные средства и методы (ALC_TAT)

Семейство ALC_TAT связано с выбором инструментальных средств, используемых для разработки, анализа и реализации ОО. Семейство содержит требования по предотвращению использования плохо определенных, несогласованных или неподходящих инструментальных средств разработки ОО. Это относится, в частности, к языкам программирования, документации, стандартам реализации и некоторым частям ОО, например вспомогательным динамическим библиотекам.

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.

Замечания по применению

Полностью определенными называют инструментальные средства разработки, которые применимы без необходимости подробных дополнительных пояснений. Например, принято считать полностью определенными языки программирования и системы автоматизации проектирования (САПР), которые основаны на стандартах, изданных органами стандартизации.

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.

Требование в ALC_TAT.1.2C применяют, главным образом, к языкам программирования для обеспечения однозначности всех операторов исходного текста.

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 инструментальные средства разработки ОО.**

ALC_TAT.1.2D **Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.**

Элементы содержания и представления свидетельств

ALC_TAT.1.1C **Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.**

ALC_TAT.1.2C **Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.**

ALC_TAT.1.3C **Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.**

Элементы действий оценщика

ALC_TAT.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ALC_TAT.2 Соответствие стандартам реализации

Зависимости

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ALC_TAT.2.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.2.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

ALC_TAT.2.3D **Разработчик должен привести описание применявшихся стандартов реализации.**

Элементы содержания и представления свидетельств

ALC_TAT.2.1C Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC_TAT.2.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.2.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

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, что стандарты реализации применялись.**

ALC_TAT.3 Соответствие всех частей ОО стандартам реализации

Зависимости

ADV_IMP.1 Подмножество реализации ФБО

Элементы действий разработчика

ALC_TAT.3.1D Разработчик должен идентифицировать инструментальные средства разработки ОО.

ALC_TAT.3.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, зависящие от реализации.

ALC_TAT.3.3D Разработчик должен привести описание стандартов реализации **для всех частей ОО**.

Элементы содержания и представления свидетельств

ALC_TAT.3.1C Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.

ALC_TAT.3.2C Документация инструментальных средств разработки должна однозначно определить значения всех конструкций языка, используемых в реализации.

ALC_TAT.3.3C Документация инструментальных средств разработки должна однозначно определить значения всех опций, зависящих от реализации.

Элементы действий оценщика

ALC_TAT.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_TAT.3.2E Оценщик должен подтвердить, что стандарты реализации применялись.

13 Класс ATE. Тестирование

Класс "Тестирование" включает в себя четыре семейства: "Покрытие" (ATE_COV), "Глубина" (ATE_DPT), "Функциональное тестирование" (ATE_FUN) и "Независимое тестирование" (например, функциональное тестирование, выполняемое оценщиками, ATE_IND). Тестирование помогает установить, что функциональные требования безопасности ОО выполнены. Тестирование обеспечивает доверие к тому, что ОО удовлетворяет, по меньшей мере, функциональным требованиям безопасности ОО, хотя оно и не может установить, что ОО не обладает большими возможностями, чем определено спецификациями. Тестирование также может быть направлено на внутреннюю структуру ФБО, например тестирование подсистем и модулей на соответствие их спецификациям.

Аспекты покрытия и глубины отделены от функционального тестирования для повышения гибкости при применении компонентов семейств. Тем не менее, требования этих трех семейств предназначены для совместного применения.

Компоненты семейства "Независимое тестирование" имеют зависимости от компонентов других семейств, позволяющие получить необходимую информацию для поддержки требований, но при этом относятся в первую очередь к независимым действиям оценщика.

Основное внимание в этом классе уделено подтверждению того, что ФБО выполняются согласно их спецификациям. Для этого применяют и позитивное тестирование, основанное на функциональных требованиях, и негативное тестирование, чтобы проверить отсутствие нежелательных режимов выполнения. Этот класс не распространяется на тестирование проникновения, которое направлено на поиск уязвимостей, дающих пользователю возможность нарушить политику безопасности. Тестирование проникновения базируется на анализе ОО, направленном специально на идентификацию уязвимостей в проекте и реализации ФБО, и рассматривается отдельно как аспект оценки уязвимостей в классе AVA.

На рисунке 13.1 показаны семейства этого класса и иерархия компонентов в семействах.

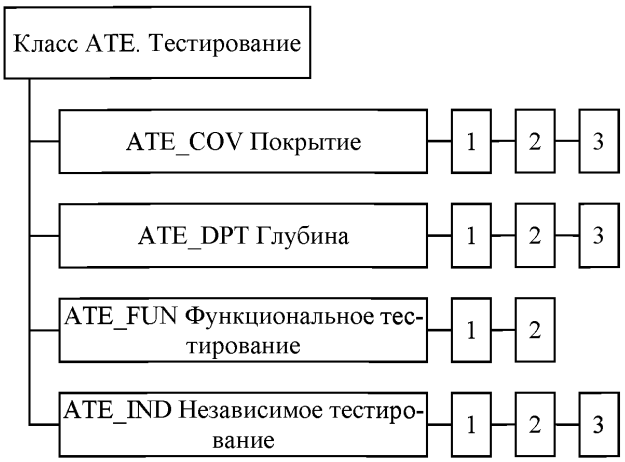


Рисунок 13.1 – Декомпозиция класса "Тестирование"

13.1 Покрытие (ATE_COV)

Цели

Семейство ATE_COV направлено на аспекты тестирования, которые имеют отношение к полноте охвата (покрытия) тестами. Таким образом, семейство связано с объемом тестирования ФБО, а также с выяснением, является ли тестирование достаточно всесторонним, чтобы демонстрировать выполнение ФБО в соответствии со спецификациями.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе повышения строгости тестирования интерфейсов и анализа достаточности тестов для демонстрации, что ФБО выполняются в соответствии с их функциональной спецификацией.

ATE_COV.1 Свидетельство покрытия

Цели

Цель этого компонента состоит в том, чтобы установить, что ФБО были проверены на соответствие их функциональной спецификации. Это предполагается достичь путем экспертизы свидетельства о соответствии, представленного разработчиком.

Замечания по применению

Несмотря на то, что цель тестирования состоит в полном покрытии ФБО, для верификации этого утверждения не требуется обеспечить ничего, помимо неформального сопоставления тестов с функциональной спецификацией и собственно данных тестирования.

В этом компоненте от разработчика требуется показать, насколько идентифицированные тесты соответствуют описанию ФБО в функциональной спецификации. Это может быть достигнуто представлением соответствия (возможно, с использованием таблицы). Эта информация требуется для содействия оценщику в планировании программы тестирования при оценке. На этом уровне нет требований полного покрытия разработчиком каждого ас-

пекта ФБО, поэтому необходимо, чтобы оценщик принял во внимание возможные пробелы в этой области.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ATE_FUN.1 Функциональное тестирование

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 показать соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

Элементы действий оценщика

ATE_COV.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_COV.2 Анализ покрытия

Цели

Цель этого компонента состоит в том, чтобы установить, что ФБО были проверены на соответствие их функциональной спецификации систематическим методом. Это предполагается достичь путем экспертизы анализа соответствия, представленного разработчиком.

Замечания по применению

От разработчика требуется демонстрировать, что идентифицированные тесты включают в себя проверку всех функций безопасности, представленных в функциональной спецификации. При анализе следует не только показать соответствие между тестами и функциями безопасности, но также предоставить оценщику достаточную информацию для вынесения независимого заключения о том, насколько функции были проверены. Эта информация может быть использована при планировании дополнительных тестов оценщика. Хотя на этом уровне разработчик должен продемонстрировать, что каждая из функций в функциональной спецификации была проверена, исчерпывающее тестирование каждой функции не обязательно.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_COV.2.1D Разработчик должен представить **анализ** покрытия тестами.

Элементы содержания и представления свидетельств

ATE_COV.2.1C **Анализ** покрытия тестами должен **демонстрировать** соответствие между тестами, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_COV.2.2C **Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.**

Элементы действий оценщика

ATE_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_COV.3 Строгий анализ покрытия

Цели

Цель этого компонента состоит в том, чтобы установить, что ФБО были проверены систематическим и исчерпывающим образом на соответствие их функциональной спецификации. Это предполагается достичь путем экспертизы анализа соответствия, представленного разработчиком.

Замечания по применению

От разработчика требуется предоставить убедительные аргументы, что идентифицированные тесты покрывают все функции безопасности, а тестирование каждой функции безопасности является полным. Оценщику останется мало возможностей для разработки дополнительных функциональных тестов интерфейсов ФБО, основанных на функциональной спецификации, поскольку они будут исчерпывающе проверены. Тем не менее, оценщику следует стремиться разработать такие тесты.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ATE_FUN.1 Функциональное тестирование

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, идентифицированными в тестовой документации, и описанием ФБО в функциональной спецификации.

ATE_COV.3.2C Анализ покрытия тестами должен демонстрировать полное соответствие между описанием ФБО в функциональной спецификации и тестами, идентифицированными в тестовой документации.

ATE_COV.3.3C **Анализ покрытия тестами должен убедительно демонстрировать, что все внешние интерфейсы ФБО, идентифицированные в функциональной спецификации, полностью проверены.**

Элементы действий оценщика

ATE_COV.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

13.2 Глубина (ATE_DPT)

Цели

Компоненты семейства ATE_DPT имеют отношение к уровню детализации тестирования ФБО. Тестирование функций безопасности основано на детализации информации, полученной из анализа представлений.

Целью является противостоять риску пропуска ошибки при разработке ОО. Дополнительно компоненты этого семейства позволяют с большей вероятностью обнаружить любой внесенный злонамеренный код, особенно потому, что тестирование в большей степени касается внутренней структуры ФБО.

Тестирование конкретных внутренних интерфейсов может обеспечивать доверие не только к тому, что ФБО внешне соответствуют желательному режиму безопасности, но также к тому, что этот режим является следствием корректного функционирования внутренних механизмов.

Ранжирование компонентов

Компоненты в этом семействе ранжированы на основе увеличения степени детализации, обеспеченной в представлениях ФБО, от проекта верхнего уровня до представления реализации. Это ранжирование отражает представления ФБО, рассмотренные в классе ADV.

Замечания по применению

Конкретный объем, а также типы документации и свидетельств будут определяться, в основном, выбранным компонентом из ATE_FUN.

Тестирование на уровне функциональной спецификации рассмотрено в ATE_COV.

В данном семействе принят принцип, чтобы уровень тестирования соответствовал искомому уровню доверия. Там, где применяют более высокие по иерархии компоненты, от результатов тестирования потребуется демонстрация того, что реализация ФБО не противоречит проекту ФБО. Например, в проекте верхнего уровня следует описать каждую из подсистем, а также интерфейсы для взаимодействия этих подсистем с достаточной детализацией. В свидетельстве тестирования необходимо показать, что были проверены внутренние интерфейсы для взаимодействия подсистем. Это может быть достигнуто либо тестированием через внешние интерфейсы ФБО, либо автономной проверкой интерфейсов подсистем, возможно с использованием средств и среды автономного тестирования. В случаях, когда некоторые аспекты внутреннего интерфейса не могут быть проверены через внешние интерфейсы, следует либо иметь строгое обоснование, что эти аспекты проверять необязательно, либо проверить этот внутренний интерфейс непосредственно. В последнем случае необходимо, чтобы проект верхнего уровня был достаточно детализирован для облегчения прямого тестирования. Иерархичные компоненты в этом семействе нацелены на проверку правильности использования внутренних интерфейсов, которые становятся видимыми, поскольку проект становится менее абстрактным. Когда применяют эти компо-

ненты, сложнее предоставить адекватное свидетельство глубины тестирования, используя только внешние интерфейсы ФБО, поэтому, как правило, необходимо тестирование на уровне модулей.

ATE_DPT.1 Тестирование: проект верхнего уровня

Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутренних действий ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие, что подсистемы ФБО были правильно реализованы.

Замечания по применению

Разработчик, как ожидается, опишет тестирование проекта верхнего уровня ФБО в терминах "подсистем". Термин "подсистема" используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

Зависимости

ADV_HLD.1 Описательный проект верхнего уровня

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_DPT.1.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.1.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня.

Элементы действий оценщика

ATE_DPT.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.2 Тестирование: проект нижнего уровня

Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутренних действий ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие, что подсистемы ФБО были правильно реализованы.

Модули ФБО обеспечивают описание внутренних действий ФБО. Тестирование на уровне модулей для демонстрации наличия любых недостатков обеспечивает доверие, что модули ФБО были правильно реализованы.

Замечания по применению

Разработчик, как ожидается, опишет тестирование проекта верхнего уровня ФБО в терминах "подсистем". Термин "подсистема" используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

Разработчик, как ожидается, опишет тестирование проекта нижнего уровня ФБО в терминах "модулей". Термин "модуль" используют, чтобы отразить декомпозицию каждой из "подсистем" ФБО на относительно малое число частей.

Зависимости

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_LLD.1 Описательный проект нижнего уровня

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_DPT.2.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.2.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня **и проектом нижнего уровня.**

Элементы действий оценщика

ATE_DPT.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_DPT.3 Тестирование на уровне реализации

Цели

Подсистемы ФБО обеспечивают высокоуровневое описание внутренних действий ФБО. Тестирование на уровне подсистем для демонстрации наличия любых недостатков обеспечивает доверие, что подсистемы ФБО были правильно реализованы.

Модули ФБО обеспечивают описание внутренних действий ФБО. Тестирование на уровне модулей для демонстрации наличия любых недостатков обеспечивает доверие, что модули ФБО были правильно реализованы.

Представление реализации ФБО обеспечивает детализированное описание внутренних действий ФБО. Тестирование на уровне реализации для демонстрации наличия любых недостатков обеспечивает доверие, что реализация ФБО была выполнена правильно.

Замечания по применению

Разработчик, как ожидается, опишет тестирование проекта верхнего уровня ФБО в терминах "подсистем". Термин "подсистема" используют, чтобы отразить декомпозицию ФБО на относительно малое число частей.

Разработчик, как ожидается, опишет тестирование проекта нижнего уровня ФБО в терминах "модулей". Термин "модули" используют, чтобы отразить декомпозицию каждой из "подсистем" ФБО на относительно малое число частей.

Представление реализации используют непосредственно для генерации реализации ФБО (например, исходный текст, который затем компилируют).

Зависимости

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_IMP.2 Реализация ФБО

ADV_LLD.1 Описательный проект нижнего уровня

ATE_FUN.1 Функциональное тестирование

Элементы действий разработчика

ATE_DPT.3.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

ATE_DPT.3.1C Анализ глубины должен показать достаточность тестов, идентифицированных в тестовой документации, для демонстрации, что ФБО выполняются в соответствии с проектом верхнего уровня, проектом нижнего уровня **и представлением реализации.**

Элементы действий оценщика

ATE_DPT.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

13.3 Функциональное тестирование (ATE_FUN)

Цели

Функциональное тестирование, выполняемое разработчиком, устанавливает, что ФБО проявляют свойства, необходимые для удовлетворения функциональных требований ПЗ/ЗБ. Такое функциональное тестирование обеспечивает доверие к тому, что ОО, по меньшей мере, удовлетворяет функциональным требованиям безопасности ОО, хотя и не может установить, что ОО не обладает большими возможностями, чем определено спецификациями. Семейство ATE_FUN сосредоточено на типе и объеме необходимой документации или требуемых инструментальных средств поддержки, а также на том, что будет демонстрировать тестирование, проведенное разработчиком. Функциональное тестирование не ограничено позитивным подтверждением предоставления требуемых функций безопасности, но может также включать в себя негативное тестирование (часто основанное на инверсии функциональных требований) для проверки отсутствия нежелательных режимов функционирования.

Это семейство способствует обеспечению доверия, что вероятность наличия незамеченных недостатков относительно мала.

Семейства ATE_COV, ATE_DPT и ATE_FUN используют совместно для определения свидетельства тестирования, представляемого разработчиком. Независимое функциональное тестирование, выполняемое оценщиком, рассмотрено в ATE_IND.

Ранжирование компонентов

Это семейство содержит два компонента. Иерархичный компонент содержит требование, чтобы была проанализирована зависимость от порядка выполнения процедур тестирования.

Замечания по применению

Как ожидается, процедуры выполнения тестов будут обеспечены инструкциями по использованию тестовых программ и комплектов тестов, включая среду и условия тестирования, параметры и значения тестовых данных. Следует также, чтобы процедуры тестирования показывали, как результаты тестирования получаются из входных данных тестирования.

Это семейство определяет требования для представления всех планов, процедур и результатов тестирования. В соответствии с этим объем информации, которую необходимо представить, будет меняться в зависимости от использования ATE_COV и ATE_DPT.

Зависимость от порядка выполнения актуальна, когда успешное выполнение конкретного теста зависит от существования конкретного состояния. Например, можно потребовать, чтобы тест А выполнялся непосредственно перед тестом Б, так как состояние, следующее из успешного выполнения теста А, – предпосылка для успешного выполнения теста Б. Таким образом, неудача теста Б может быть связана с проблемой зависимости от порядка выполнения. В приведенном примере тест Б может закончиться неудачно, потому что тест В (а не А) был выполнен непосредственно перед ним, или же неудача теста Б связана с неудачей теста А.

ATE_FUN.1 Функциональное тестирование

Цели

Цель разработчика – демонстрировать, что все функции безопасности выполняются в соответствии со спецификациями. От разработчика требуется выполнить тестирование и представить тестовую документацию.

Зависимости отсутствуют.

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 и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.**

ATE_FUN.1.2C **Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.**

ATE_FUN.1.3C **Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.**

ATE_FUN.1.4C **Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.**

ATE_FUN.1.5C **Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.**

Элементы действий оценщика

ATE_FUN.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

ATE_FUN.2 Упорядоченное функциональное тестирование

Цели

Цель разработчика – демонстрировать, что все функции безопасности выполняются в соответствии со спецификациями. От разработчика требуется выполнить тестирование и представить тестовую документацию.

Дополнительная цель данного компонента – обеспечение структурирования тестирования таким образом, чтобы избежать циклической зависимости при подтверждении правильности проверяемых частей ФБО.

Замечания по применению

Хотя процедуры тестирования могут устанавливать предопределенные начальные условия тестирования на основе упорядочения тестов, они могут не иметь логического обоснования упорядочения. Анализ упорядочения тестов – важный фактор в определении адекватности тестирования, так как имеется возможность наличия ошибок, скрытых порядком выполнения тестов.

Зависимости отсутствуют.

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 и описаний процедур тестирования, а также ожидаемых и фактических результатов тестирования.

ATE_FUN.2.2C Планы тестирования должны идентифицировать проверяемые функции безопасности и содержать изложение целей тестирования.

ATE_FUN.2.3C Описания процедур тестирования должны идентифицировать тесты, которые необходимо выполнить, и включать в себя сценарии для тестирования каждой функции безопасности. Эти сценарии должны учитывать любое влияние последовательности выполнения тестов на результаты других тестов.

ATE_FUN.2.4C Ожидаемые результаты тестирования должны показать прогнозируемые выходные данные успешного выполнения тестов.

ATE_FUN.2.5C Результаты выполнения тестов разработчиком должны демонстрировать, что каждая проверенная функция безопасности выполнялась в соответствии со спецификациями.

ATE_FUN.2.6C **Тестовая документация должна включать в себя анализ зависимостей от порядка выполнения процедуры тестирования.**

Элементы действий оценщика

ATE_FUN.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

13.4 Независимое тестирование (ATE_IND)

Цели

Главная цель – демонстрировать, что функции безопасности выполняются в соответствии со спецификациями.

Дополнительная цель – противостоять риску неправильной оценки разработчиком выходных данных тестов в результате неправильной реализации спецификаций или пропуска кода, который не согласуется со спецификациями.

Ранжирование компонентов

Ранжирование основано на объеме тестовой документации и поддержки тестирования, а также на объеме тестирования оценщиком.

Замечания по применению

Тестирование, рассматриваемое в этом семействе, может проводиться с привлечением, помимо оценщика, других квалифицированных исполнителей (например, независимой лаборатории, организации конечных потребителей). При этом тестирование требует понимания ОО с учетом выполнения других действий по установлению доверия к ОО, а оценщик по-прежнему отвечает за обеспечение удовлетворения требований данного семейства.

Это семейство имеет отношение к степени выполнения независимого функционального тестирования ФБО. Независимое функциональное тестирование может приобретать форму полного или частичного повторения функциональных тестов, выполненных разработчиком. Оно может также проводиться в дополнение к функциональным тестам, выполненным разработчиком, как для увеличения области покрытия или глубины тестов, так и для проверки очевидных, известных из общедоступных источников слабых мест безопасности, которые могут иметься в ОО. Эти действия дополняют друг друга, и для каждого ОО необходимо планировать приемлемое их сочетание с учетом применимости и области покрытия результатов тестов, а также функциональной сложности ФБО. Следует разработать план тестирования, согласующийся с уровнем других действий по установлению доверия к ОО, который, когда требуется более высокое доверие, включает в себя повторение большей выборки тестов и большего объема независимых позитивных и негативных функциональных тестов, выполняемых оценщиком.

Повторение выборки тестов, выполненных разработчиком, предназначено для обеспечения подтверждения, что разработчик выполнил свою запланированную программу

тестирования ФБО и правильно зафиксировал результаты. На объем установленной выборки будут влиять детализация и качество результатов функционального тестирования разработчиком. Необходимо также, чтобы оценщик рассмотрел возможность разработки дополнительных тестов и соотношение результатов, которые могут быть получены по этим двум направлениям. Повторение всех тестов, выполненных разработчиком, может быть возможно и желательно в некоторых случаях, но весьма затруднено и менее продуктивно в других. Поэтому самый высокий по иерархии компонент этого семейства следует использовать осторожно. При формировании выборки рассматривается весь диапазон применения результатов тестирования, включая обеспечение выполнения требований семейств ATE_COV и ATE_DPT.

Необходимо также принять во внимание, что при оценке могут использоваться разные конфигурации ОО. Оценщику придется проанализировать применимость предоставленных результатов и в соответствии с этим планировать свое собственное тестирование.

Независимое функциональное тестирование отличается от тестирования проникновения, основанного на целенаправленном и систематическом поиске уязвимостей в проекте и/или реализации. Тестирование проникновения рассмотрено в семействе AVA_VLA.

Пригодность ОО для тестирования основана на доступности ОО и поддержке документацией и информацией, необходимой для выполнения тестов (включая любое тестовое программное обеспечение или инструментальные средства тестирования). Необходимость в такой поддержке отражена в зависимостях от других семейств доверия.

Кроме того, пригодность ОО для тестирования может основываться на других соображениях. Например, версия ОО, представленная разработчиком, может быть не окончательной.

Ссылки на подмножество ФБО предназначены для того, чтобы позволить оценщику проектировать приемлемую совокупность тестов, которая согласована с целями проводимой оценки.

ATE_IND.1 Независимое тестирование на соответствие

Цели

Целью является демонстрация выполнения функций безопасности в соответствии со спецификациями.

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 разработчиком, принимается без проверки. От оценщика требуется разработать и выполнить тесты с целью подтверждения, что функциональные требования безопасности ОО удовлетворены. При этом подходе предполагается убедиться в правильном функционировании через репрезентативное тестирование, а не через выполнение всех возможных тестов. Объем тестирования, планируемый для этой цели, является методологической проблемой, и его необходимо рассматривать в контексте конкретного ОО и в сопоставлении с другими действиями оценки.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

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 необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2 Выборочное независимое тестирование

Цели

Целью является демонстрация выполнения функций безопасности в соответствии со спецификациями. Тестирование, проводимое оценщиком, включает в себя отбор и повторение тестов, выполненных разработчиком.

Замечания по применению

Разработчику следует обеспечить оценщика материалами, необходимыми для эффективного воспроизведения тестов, выполненных разработчиком. Сюда могут быть включены такие материалы, как машиночитаемая тестовая документация, тест-программы и т.д.

Этот компонент содержит требование, чтобы оценщику были доступны результаты тестирования разработчиком для дополнения программы тестирования. Оценщик повторит выборку из тестов, выполненных разработчиком, чтобы получить уверенность в полученных результатах. Получив такую уверенность, оценщик расширит тестирование, выполненное разработчиком, проводя дополнительные испытания ОО способом, отличающимся от примененного разработчиком. Основываясь на подтверждении достоверности результатов тестов, выполненных разработчиком, оценщик способен убедиться, что ОО функционирует правильно в более широком диапазоне условий, чем это было бы возможно для разработчика, ограниченного уровнем его ресурсов. Убедившись в том, что разработчик протестировал ОО, оценщик будет также иметь больше свободы для концентрации тестирования в тех направлениях, где экспертиза документации или специальные знания вызвали определенную настороженность.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

ATE_FUN.1 Функциональное тестирование

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 протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.2.3E **Оценщик должен выполнить выборку тестов из тестовой документации, чтобы верифицировать результаты тестирования, полученные разработчиком.**

ATE_IND.3 Полное независимое тестирование

Цели

Целью является демонстрация выполнения функций безопасности в соответствии со спецификациями. Тестирование, проводимое оценщиком, включает в себя повторное выполнение всех тестов, выполненных разработчиком.

Замечания по применению

Разработчику следует обеспечить оценщика материалами, необходимыми для эффективного воспроизведения тестов, выполненных разработчиком. Сюда могут быть включены такие материалы, как машиночитаемая тестовая документация, тест-программы и т.д.

В этом компоненте требуется, чтобы оценщик повторил все тесты, выполненные разработчиком, как часть программы тестирования. Как и в предыдущем компоненте, оценщик проведет дополнительные испытания, стремясь проверить ОО способом, отличным от использованного разработчиком. В случае, когда тестирование разработчиком было исчерпывающим, для этого могут оставаться небольшие возможности.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

ATE_FUN.1 Функциональное тестирование

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.

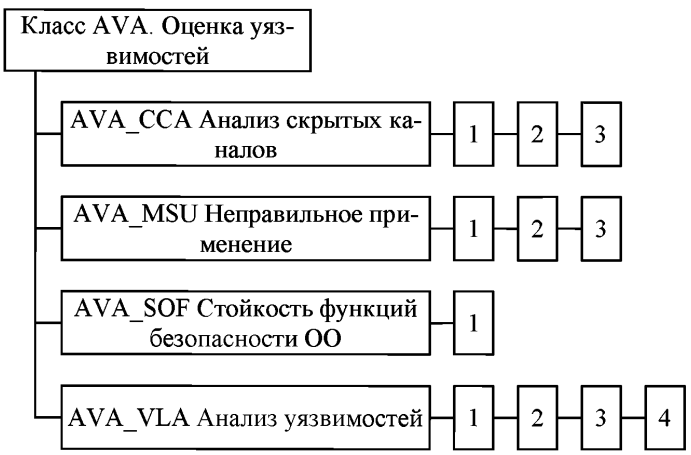
ATE_IND.3.2E Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

ATE_IND.3.3E Оценщик должен выполнить **все** тесты из тестовой документации, чтобы верифицировать результаты тестирования разработчиком.

14 Класс AVA. Оценка уязвимостей

Класс AVA связан с наличием пригодных для использования скрытых каналов и с возможностью неправильного применения или конфигурирования ОО, а также с возможностью преодоления вероятностных или перестановочных механизмов безопасности и использованием уязвимостей, вносимых при разработке или эксплуатации ОО.

На рисунке 14.1 показаны семейства этого класса и иерархия компонентов в семей-



ствах.

Рисунок 14.1 – Декомпозиция класса "Оценка уязвимостей"

14.1 Анализ скрытых каналов (AVA_CCA)

Цели

Анализ скрытых каналов выполняют с целью сделать заключение о существовании и потенциальной пропускной способности непредусмотренных каналов передачи сигналов (т.е. неразрешенных информационных потоков), которые могут быть использованы.

Требования доверия связаны с угрозой существования непредусмотренных и пригодных для использования путей передачи сигналов, которые могут быть применены для нарушения ПФБ.

Ранжирование компонентов

Компоненты ранжированы по повышению строгости анализа скрытых каналов.

Замечания по применению

Оценка пропускной способности канала основана на технических расчетах, а также на фактических результатах выполнения тестов.

Примеры предположений, на которых основан анализ скрытых каналов, могут включать в себя быстродействие процессора, системную или сетевую конфигурацию, размер памяти, размер кэш-памяти.

Выборочное подтверждение правильности анализа скрытых каналов путем тестирования дает оценщику возможность верифицировать любые аспекты анализа (такие, как идентификация, оценка пропускной способности, удаление, мониторинг, сценарии применения). Это не требует демонстрации всех результатов анализа скрытых каналов.

Если в ЗБ не содержатся никакие ПФБ управления информационными потоками, это семейство требований доверия не применяют, поскольку оно относится только к ПФБ управления информационными потоками.

AVA_CCA.1 Анализ скрытых каналов

Цели

Целью является идентифицировать скрытые каналы, которые можно найти путем неформального поиска скрытых каналов.

Зависимости

ADV_FSP.2 Полностью определенные внешние интерфейсы

ADV_IMP.2 Реализация ФБО

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_CCA.1.1D **Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.**

AVA_CCA.1.2D **Разработчик должен представить документацию анализа скрытых каналов.**

Элементы содержания и представления свидетельств

AVA_CCA.1.1C **Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.**

AVA_CCA.1.2C **Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.**

AVA_CCA.1.3C **Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.**

AVA_CCA.1.4C **Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.**

AVA_CCA.1.5C **Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.**

Элементы действий оценщика

AVA_CCA.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AVA_CCA.1.2E **Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО удовлетворяет функциональным требованиям.**

AVA_CCA.1.3E **Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.**

AVA_CCA.2 Систематический анализ скрытых каналов

Цели

Целью является идентифицировать скрытые каналы, которые можно найти путем систематического поиска скрытых каналов.

Замечания по применению

Для систематического анализа скрытых каналов требуется, чтобы разработчик идентифицировал скрытые каналы структурированным и повторяемым образом, в противоположность идентификации скрытых каналов частным методом, применимым для конкретной ситуации.

Зависимости

ADV_FSP.2 Полностью определенные внешние интерфейсы

ADV_IMP.2 Реализация ФБО

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_CCA.2.1D Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

AVA_CCA.2.2D Разработчик должен представить документацию анализа скрытых каналов.

Элементы содержания и представления свидетельств

AVA_CCA.2.1C Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.

AVA_CCA.2.2C Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA.2.3C Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.

AVA_CCA.2.4C Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.

AVA_CCA.2.5C Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.

AVA_CCA.2.6C **Документация анализа должна содержать свидетельство, что метод, использованный для идентификации скрытых каналов, является систематическим.**

Элементы действий оценщика

AVA_CCA.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_CCA.2.2E Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО удовлетворяет функциональным требованиям.

AVA_CCA.2.3E Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.

AVA_CCA.3 Исчерпывающий анализ скрытых каналов

Цели

Целью является идентифицировать скрытые каналы, которые можно найти путем исчерпывающего поиска скрытых каналов.

Замечания по применению

Для исчерпывающего анализа скрытых каналов требуется представление дополнительного свидетельства, что план идентификации скрытых каналов достаточен для утверждения, что были испробованы все возможные пути исследования скрытых каналов.

Зависимости

ADV_FSP.2 Полностью определенные внешние интерфейсы

ADV_IMP.2 Реализация ФБО

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_CCA.3.1D Разработчик должен провести поиск скрытых каналов для каждой политики управления информационными потоками.

AVA_CCA.3.2D Разработчик должен представить документацию анализа скрытых каналов.

Элементы содержания и представления свидетельств

AVA_CCA.3.1C Документация анализа должна идентифицировать скрытые каналы и содержать оценку их пропускной способности.

AVA_CCA.3.2C Документация анализа должна содержать описание процедур, используемых для вынесения заключения о существовании скрытых каналов, и информацию, необходимую для анализа скрытых каналов.

AVA_CCA.3.3C Документация анализа должна содержать описание всех предположений, сделанных в процессе анализа скрытых каналов.

AVA_CCA.3.4C Документация анализа должна содержать описание метода, используемого для оценки пропускной способности канала для случая наиболее опасного варианта сценария.

AVA_CCA.3.5C Документация анализа должна содержать описание наиболее опасного варианта сценария использования каждого идентифицированного скрытого канала.

AVA_CCA.3.6C Документация анализа должна содержать свидетельство, что метод, использованный для идентификации скрытых каналов, является **исчерпывающим**.

Элементы действий оценщика

AVA_CCA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_CCA.3.2E Оценщик должен подтвердить, что результаты анализа скрытых каналов показывают, что ОО удовлетворяет функциональным требованиям.

AVA_CCA.3.3E Оценщик должен выборочно подтвердить правильность результатов анализа скрытых каналов, применяя тестирование.

14.2 Неправильное применение (AVA_MSU)

Цели

Семейство AVA_MSU позволяет установить, может ли ОО быть конфигурирован или использован опасным образом так, чтобы администратор или пользователь ОО считал бы его безопасным.

Целями являются:

а) минимизация вероятности конфигурирования или установки ОО опасным образом, исключающим возможность обнаружения пользователем или администратором;

б) минимизация риска ошибок, обусловленных человеческим фактором или иными причинами, в операциях, которые могут блокировать, отключить или помешать активизировать функции безопасности, приводя к необнаруженному опасному состоянию.

Ранжирование компонентов

Компоненты ранжированы по возрастанию числа свидетельств, представляемых разработчиком, и повышению строгости анализа.

Замечания по применению

Противоречивое, вводящее в заблуждение, неполное или необоснованное руководство может убедить пользователя в безопасности ОО при ее отсутствии, что может привести к уязвимостям.

Примером противоречия является наличие двух инструкций руководства, которые подразумевают различные выходные результаты при одних и тех же входных данных.

Примером введения в заблуждение является такая формулировка инструкции руководства, которую можно трактовать неоднозначно, причем одна из трактовок может привести к опасному состоянию.

Примером неполноты является список существенных физических требований безопасности, в котором опущен важный пункт, что приведет к игнорированию соответствующего требования администратором, считающим список полным.

Примером необоснованности является рекомендация следовать процедуре, приводящей к чрезмерной административной нагрузке.

Требуется руководящая документация по выявлению опасных состояний. Она может быть включена в руководства пользователя и администратора или же представляться отдельно. При отдельном представлении оценщику следует подтвердить, что данная документация поставлена вместе с ОО.

AVA_MSU.1 Экспертиза руководств

Цели

Целью является обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться.

Зависимости

ADO_IGS.1 Процедуры установки, генерации и запуска

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_MSU.1.1D Разработчик должен представить руководства по применению ОО.

Элементы содержания и представления свидетельств

AVA_MSU.1.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.1.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.1.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.1.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль над процедурами, физическими мерами и персоналом).

Элементы действий оценщика

AVA_MSU.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AVA_MSU.1.2E **Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.**

AVA_MSU.1.3E **Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.**

AVA_MSU.2 Подтверждение правильности анализа

Цели

Целью является обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться. В этом компоненте требуется анализ разработчиком руководств для повышения доверия, что цель достигнута.

Зависимости

ADO_IGS.1 Процедуры установки, генерации и запуска

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_MSU.2.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.2.2D **Разработчик должен задокументировать анализ руководств.**

Элементы содержания и представления свидетельств

AVA_MSU.2.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.2.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.2.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.2.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.2.5C **Документация анализа должна демонстрировать, что руководства полны.**

Элементы действий оценщика

AVA_MSU.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки **и выборочно другие процедуры** для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.2.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.2.4E **Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.**

AVA_MSU.3 Анализ и тестирование опасных состояний

Цели

Целью является обеспечить отсутствие в руководствах вводящих в заблуждение, необоснованных и противоречивых указаний и предусмотреть безопасные процедуры для всех режимов функционирования. Опасные состояния должны легко выявляться. В этом компоненте требуется анализ разработчиком руководств для повышения доверия, что цель достигнута, и этот анализ проверяется и подтверждается оценщиком путем тестирования.

Замечания по применению

В этом компоненте от оценщика требуется выполнить тестирование, что при переходе ОО в опасное состояние оно может быть легко выявлено. Это тестирование может рассматриваться как специфический аспект тестирования проникновения.

Зависимости

ADO_IGS.1 Процедуры установки, генерации и запуска

ADV_FSP.1 Неформальная функциональная спецификация

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_MSU.3.1D Разработчик должен представить руководства по применению ОО.

AVA_MSU.3.2D Разработчик должен задокументировать анализ руководств.

Элементы содержания и представления свидетельств

AVA_MSU.3.1C Руководства должны идентифицировать все возможные режимы эксплуатации ОО (включая действия после сбоя или ошибки в работе), их последствия и значение для обеспечения безопасной эксплуатации.

AVA_MSU.3.2C Руководства должны быть полны, понятны, непротиворечивы и обоснованы.

AVA_MSU.3.3C Руководства должны содержать список всех предположений относительно среды эксплуатации.

AVA_MSU.3.4C Руководства должны содержать список всех требований к внешним мерам безопасности (включая внешний контроль за процедурами, физическими мерами и персоналом).

AVA_MSU.3.5C Документация анализа должна демонстрировать, что руководства полны.

Элементы действий оценщика

AVA_MSU.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_MSU.3.2E Оценщик должен повторить все процедуры конфигурирования и установки и выборочно другие процедуры для подтверждения, что ОО можно безопасно конфигурировать и использовать, применяя только представленные руководства.

AVA_MSU.3.3E Оценщик должен сделать независимое заключение, что использование руководств позволяет выявить все опасные состояния.

AVA_MSU.3.4E Оценщик должен подтвердить, что документация анализа показывает обеспечение руководствами безопасного функционирования во всех режимах эксплуатации ОО.

AVA_MSU.3.5E **Оценщик должен выполнить независимое тестирование, чтобы сделать заключение, будут ли администратор или пользователь способны установить, руководствуясь документацией, что ОО конфигурирован или используется опасным образом.**

14.3 Стойкость функций безопасности ОО (AVA_SOF)

Цели

Даже если функцию безопасности ОО нельзя обойти, отключить или исказить, в некоторых случаях все же существует возможность ее преодоления из-за уязвимости в концепции реализующих ее базовых механизмов безопасности. Для этих функций квалификация режима безопасности может быть проведена с использованием результатов количественного или статистического анализа режима безопасности указанных механизмов, а также усилий, требуемых для их преодоления. Квалификацию осуществляют в виде утверждения о стойкости функции безопасности ОО.

Ранжирование компонентов

В этом семействе имеется только один компонент.

Замечания по применению

Функции безопасности реализуются механизмами безопасности. Например, механизм пароля может использоваться при реализации функций идентификации и аутентификации.

Оценку стойкости функции безопасности ОО выполняют на уровне механизма безопасности, но ее результаты позволяют определить способность соответствующей функции безопасности противостоять идентифицированным угрозам.

При анализе стойкости функции безопасности ОО следует рассматривать, по меньшей мере, содержание всех поставляемых материалов ОО, включая ЗБ, с учетом намеченного оценочного уровня доверия.

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_HLD.1 Описательный проект верхнего уровня

Элементы действий разработчика

AVA_SOF.1.1D **Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.**

Элементы содержания и представления свидетельств

AVA_SOF.1.1C **Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.**

AVA_SOF.1.2C **Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.**

Элементы действий оценщика

AVA_SOF.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AVA_SOF.1.2E **Оценщик должен подтвердить, что утверждения относительно стойкости корректны.**

14.4 Анализ уязвимостей (AVA_VLA)

Цели

Анализ уязвимостей позволяет сделать заключение, могут ли уязвимости, идентифицированные в процессе оценки ОО и его ожидаемого применения или другими методами (например, из гипотезы о недостатках), быть использованы пользователями для нарушения ПБО.

При анализе уязвимостей рассматривают угрозы, что пользователь будет в состоянии обнаружить недостатки, позволяющие получить несанкционированный доступ к ре-

сурсам (например, данным), препятствовать выполнению ФБО и искажать их или же ограничивать санкционированные возможности других пользователей.

Ранжирование компонентов

Ранжирование основано на повышении строгости анализа уязвимостей разработчиком и оценщиком.

Замечания по применению

Разработчик выполняет анализ уязвимостей, чтобы установить присутствие уязвимостей безопасности; при этом следует рассматривать, по меньшей мере, содержание всех поставляемых материалов ОО, включая ЗБ, с учетом намеченного оценочного уровня доверия. От разработчика требуется задокументировать местоположение идентифицированных уязвимостей, чтобы позволить оценщику использовать эту информацию, если ее признают полезной, для поддержки независимого анализа уязвимостей оценщиком.

Анализ, проводимый разработчиком, предназначен для подтверждения невозможности использования идентифицированных уязвимостей безопасности в предполагаемой среде ОО и стойкости ОО к явным нападениям проникновения.

Под явными уязвимостями понимают те, которые открыты для использования, требующего минимума понимания ОО, умений, технического опыта и ресурсов. Они могут быть подсказаны описанием интерфейса ФБО. К явным уязвимостям относятся известные из общедоступных источников (и разработчику следует детально знать их) или полученные от органа оценки.

Систематический поиск уязвимостей предусматривает, чтобы разработчик идентифицировал эти уязвимости структурированным и повторяемым образом, в противоположность идентификации их частными методами. Следует, чтобы свидетельство того, что поиск уязвимостей был систематическим, включало в себя идентификацию всей документации ОО, на которой был основан поиск недостатков.

Независимый анализ уязвимостей не ограничивается уязвимостями, идентифицированными разработчиком. Основная цель анализа, проводимого оценщиком, – сделать заключение, что ОО является стойким к нападениям проникновения со стороны нарушителя, обладающего низким (для AVA_VLA.2), умеренным (для AVA_VLA.3) или высоким (для AVA_VLA.4) потенциалом нападения. Для выполнения этой цели оценщик сначала проверяет возможности использования всех идентифицированных уязвимостей. Это осуществляется посредством тестирования проникновения. Оценщику следует принять на себя роль нарушителя с одним из указанным выше потенциалов нападения при попытке проникновения в ОО. Любое использование уязвимостей таким нарушителем оценщику следует рассматривать как "явное нападение проникновения" (в отношении элементов AVA_VLA.*.2C) в контексте компонентов AVA_VLA.2–4.

AVA_VLA.1 Анализ уязвимостей разработчиком

Цели

Разработчик выполняет анализ уязвимостей, чтобы установить присутствие явных уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Замечания по применению

Оценщику следует предусмотреть дополнительные тесты для уязвимостей, выявленных при выполнении других частей оценки и потенциально пригодных для использования.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_HLD.1 Описательный проект верхнего уровня

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_VLA.1.1D **Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску явных путей, которыми пользователь может нарушить ПБО.**

AVA_VLA.1.2D **Разработчик должен задокументировать местоположение явных уязвимостей.**

Элементы содержания и представления свидетельств

AVA_VLA.1.1C **Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.**

Элементы действий оценщика

AVA_VLA.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AVA_VLA.1.2E **Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета явных уязвимостей.**

AVA_VLA.2 Независимый анализ уязвимостей

Цели

Разработчик выполняет анализ уязвимостей, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, чтобы сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими низким потенциалом нападения.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_IMP.1 Подмножество реализации ФБО

ADV_LLD.1 Описательный проект нижнего уровня

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_VLA.2.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску **путей**, которыми пользователь может нарушить ПБО.

AVA_VLA.2.2D Разработчик должен задокументировать местоположение **идентифицированных** уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.2.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.2.2C **Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.**

Элементы действий оценщика

AVA_VLA.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.2.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета **идентифицированных** уязвимостей.

AVA_VLA.2.3E **Оценщик должен выполнить независимый анализ уязвимостей.**

AVA_VLA.2.4E **Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.**

AVA_VLA.2.5E **Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим низким потенциалом нападения.**

AVA_VLA.3 Умеренно стойкий

Цели

Разработчик выполняет анализ уязвимостей, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, чтобы сделать независимое заключение,

что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими умеренным потенциалом нападения.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_IMP.1 Подмножество реализации ФБО

ADV_LLD.1 Описательный проект нижнего уровня

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.3.3C **Свидетельство должно показать, что поиск уязвимостей является систематическим.**

Элементы действий оценщика

AVA_VLA.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.3.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

AVA_VLA.3.3E Оценщик должен выполнить независимый анализ уязвимостей.

AVA_VLA.3.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

AVA_VLA.3.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **умеренным** потенциалом нападения.

AVA_VLA.4 Высокостойкий

Цели

Разработчик выполняет анализ уязвимостей, чтобы установить присутствие уязвимостей безопасности и подтвердить, что они не могут быть использованы в предполагаемой среде ОО.

Оценщик выполняет независимое тестирование проникновения, поддержанное собственным независимым анализом уязвимостей, чтобы сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителями, обладающими высоким потенциалом нападения.

Зависимости

ADV_FSP.1 Неформальная функциональная спецификация

ADV_HLD.2 Детализация вопросов безопасности в проекте верхнего уровня

ADV_IMP.1 Подмножество реализации ФБО

ADV_LLD.1 Описательный проект нижнего уровня

AGD_ADM.1 Руководство администратора

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AVA_VLA.4.1D Разработчик должен выполнить и задокументировать анализ поставляемых материалов ОО по поиску путей, которыми пользователь может нарушить ПБО.

AVA_VLA.4.2D Разработчик должен задокументировать местоположение идентифицированных уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.4.1C Документация должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.4.2C Документация должна содержать строгое обоснование, что ОО с идентифицированными уязвимостями является стойким к явным нападениям проникновения.

AVA_VLA.4.3C Свидетельство должно показать, что поиск уязвимостей является систематическим.

AVA_VLA.4.4C **Документация анализа должна содержать строгое обоснование, что анализ полностью учитывает все поставляемые материалы ОО.**

Элементы действий оценщика

AVA_VLA.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VLA.4.2E Оценщик должен провести тестирование проникновения, основанное на анализе уязвимостей, выполненном разработчиком, для обеспечения учета идентифицированных уязвимостей.

AVA_VLA.4.3E Оценщик должен выполнить независимый анализ уязвимостей.

AVA_VLA.4.4E Оценщик должен выполнить независимое тестирование проникновения, основанное на независимом анализе уязвимостей, и сделать независимое заключение о возможности использования дополнительно идентифицированных уязвимостей в предполагаемой среде.

AVA_VLA.4.5E Оценщик должен сделать независимое заключение, что ОО является стойким к нападениям проникновения, выполняемым нарушителем, обладающим **высоким** потенциалом нападения.

15 Парадигма поддержки доверия

15.1 Введение

В этом разделе представлена парадигма поддержки доверия, которой посвящен класс "Поддержка доверия" (АМА). Здесь также приведена полезная информация, помогающая понять один из возможных подходов к применению требований класса АМА.

Поддержка доверия – понятие, применение которого предполагается после того, как ОО уже оценен и сертифицирован по критериям из разделов 4-5 и 8-14. Поддержка требований доверия направлена на получение уверенности в том, что ОО будет по-прежнему отвечать своему заданию по безопасности после изменений в ОО или его среде. К таким изменениям относятся: обнаружение новых угроз или уязвимостей, изменения в требованиях пользователя, исправление ошибок, обнаруженных в сертифицированном ОО, а также другие обновления функциональных возможностей ОО.

Одним из способов вынесения заключения о поддержке доверие является переоценка ОО. Термин "переоценка" здесь означает оценку новой версии ОО, учитывающую все относящиеся к безопасности изменения, произведенные в сертифицированной ранее версии ОО, при которой повторно используют результаты предыдущей оценки, оставшиеся актуальными. Однако во многих случаях вряд ли будет практично выполнять переоценку каждой новой версии ОО для дальнейшей поддержки доверия.

Поэтому главная цель класса АМА – определить совокупность требований, которые могут применяться, чтобы убедиться в поддержке установленного доверия к ОО, не требуя во всех случаях формальной переоценки новых версий ОО. Класс АМА не исключает полностью необходимость переоценки. В некоторых случаях изменения могут быть настолько значительными, что для дальнейшей поддержки доверия переоценка обязательна. Таким образом, требования этого класса имеют дополнительную цель по обеспечению, при необходимости, экономически оправданной переоценки ОО.

Следует отметить, что вполне возможна переоценка каждой новой версии ОО по критериям из разделов 4-5 и 8-14 вообще без учета требований класса АМА. Однако класс АМА включает в себя требования, которые могут быть использованы для поддержки любой такой переоценки.

Действия разработчика и оценщика по поддержке предполагается выполнять после того, как ОО был оценен и сертифицирован, хотя, как описано ниже, некоторые требования могут применяться и на стадии оценки. Примеры использования терминов в описании парадигмы:

а) *сертифицированная версия* ОО – версия, которая была оценена и сертифицирована;

б) *текущая версия* ОО – версия, которая в некотором смысле отличается от сертифицированной версии; это может быть, например:

- новый выпуск ОО,
- сертифицированная версия с обновлениями, внесенными для исправления вновь обнаруженных ошибок,

– та же самая базовая версия ОО, но на другой аппаратной или программной платформе.

Роли разработчика и оценщика в этом классе такие же, как и описанные в части 1 ОК. Однако совершенно необязательно, чтобы оценщик, упоминаемый в требованиях этого класса, ранее принимал участие в оценке сертифицированной версии ОО.

Чтобы сделать возможным продолжение поддержки доверия к ОО без обязательной формальной переоценки, требования этого класса накладывают на разработчика обязанность представить свидетельство, показывающее, что ОО по-прежнему удовлетворяет своему заданию по безопасности (например, свидетельство тестирования разработчиком).

15.2 Цикл поддержки доверия

Этот подраздел описывает один из возможных подходов к использованию семейств и компонентов поддержки доверия с целью проиллюстрировать использование рассматриваемых понятий. В качестве примера приведен "цикл поддержки доверия", разделенный на три следующие фазы:

а) *приемка ОО для поддержки* – начало цикла, когда планы и процедуры разработчика по поддержке доверия в течение цикла устанавливает разработчик, и затем их правильность независимо подтверждает оценщик;

б) *мониторинг* – разработчик предоставляет в одной или нескольких контрольных точках цикла свидетельство, что доверие к ОО поддерживается в соответствии с установленными планами и процедурами; это свидетельство поддержки доверия затем независимо проверяет оценщик;

в) *переоценка* – окончание цикла, когда обновленная версия ОО представляется на рассмотрение для переоценки, основанной на изменениях, которым подверглась сертифицированная версия ОО.

Семейства класса АМА связаны, прежде всего, с двумя первыми фазами, обеспечивая поддержку для третьей. Эти фазы введены здесь только для того, чтобы понятнее описать применение требований поддержки доверия. Не ставится цель сделать строго обязательной схему поддержки доверия, которая формально включает в себя эти три фазы.

Цикл поддержки доверия проиллюстрирован на рисунке 15.1.

В рассматриваемом примере можно переходить к фазе мониторинга ОО только после успешного завершения фазы приемки (т.е. когда планы и процедуры разработчика по поддержке доверия уже приняты). Если разработчик вносит изменения в эти планы или процедуры в фазе мониторинга, необходимо вернуться к фазе приемки ОО, чтобы учесть произведенные изменения.

В фазе мониторинга разработчик выполняет планы и процедуры поддержки доверия, проводя анализ влияния на безопасность изменений, которым подвергается ОО (анализ влияния на безопасность). В определенных контрольных точках этой фазы оценщик независимо проверяет (посредством аудита) деятельность разработчика. От разработчика требуется четкое выполнение планов и процедур поддержки и анализа влияния на безопасность.

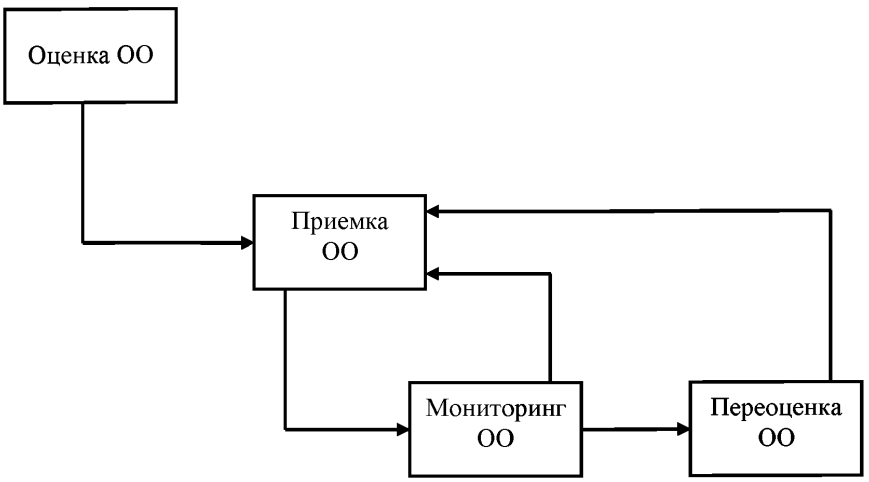


Рисунок 15.1 – Пример цикла поддержки доверия

Поэтому при нахождении ОО в фазе мониторинга появляется возможность убедиться, что доверие к ОО поддерживается для новых версий ОО, выпущенных разработчиком.

ОО, который подвергается изменениям, не может пребывать в фазе мониторинга постоянно: в какой-то момент времени переоценка ОО становится необходимой. Время принятия решения о необходимости переоценки зависит от накопления изменений в ОО, а также от особо значительных изменений. Например, большое количество малых изменений может повлиять на доверие к ОО как одно значительное изменение. План разработчика по поддержке доверия определяет предел для изменений в ОО, которые могут быть внесены в фазе мониторинга (см. 15.3.1).

Подобным образом невозможно "повысить рейтинг" ОО (т.е. повысить его уровень доверия) в фазе мониторинга. Это может быть достигнуто только посредством новой оценки ОО (использующей, по возможности, результаты предыдущего оценивания).

Статус поддержки доверия к ОО должен быть пересмотрен, если будет обнаружено, что процедуры поддержки доверия не выполняются, в результате чего утрачивается доверие к ОО. В некоторых случаях от разработчика может потребоваться представление ОО для переоценки, после которой начнется новый цикл поддержки доверия.

15.2.1 Приемка ОО

В рассматриваемом примере фаза приемки ОО в цикле поддержки доверия может быть далее уточнена путем использования семейств "План поддержки доверия" и "Отчет о категорировании компонентов ОО" из класса АМА.

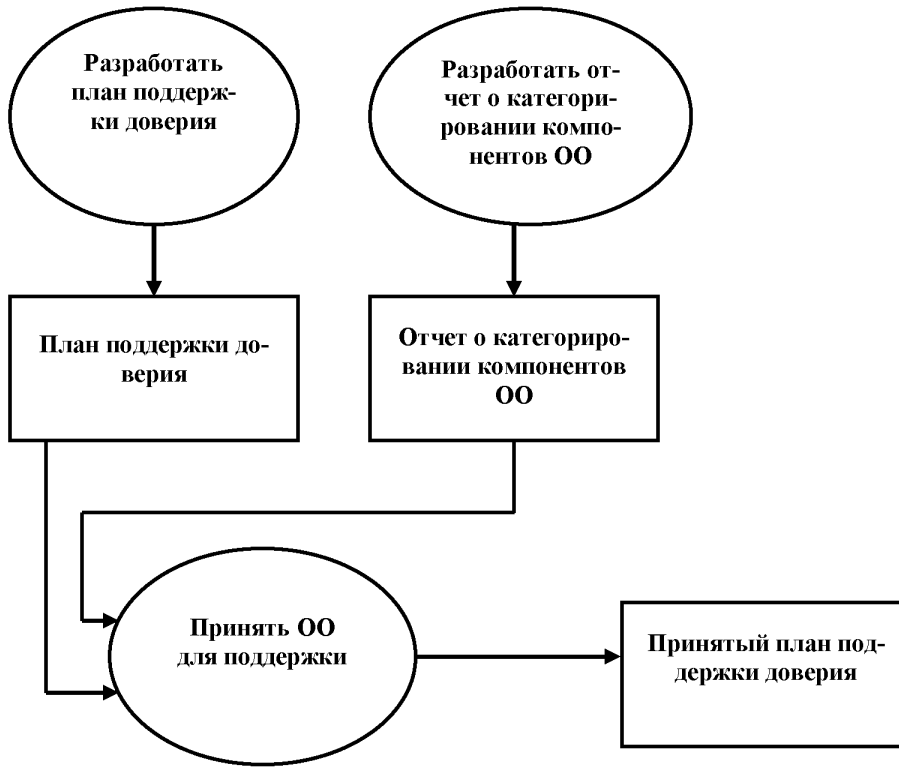


Рисунок 15.2 – Пример подхода к приемке ОО

15.2.2 Мониторинг ОО

Фаза мониторинга ОО в цикле поддержки доверия будет уточнена ниже с использованием семейств "Свидетельство поддержки доверия" и "Анализ влияния на безопасность" класса AMA.

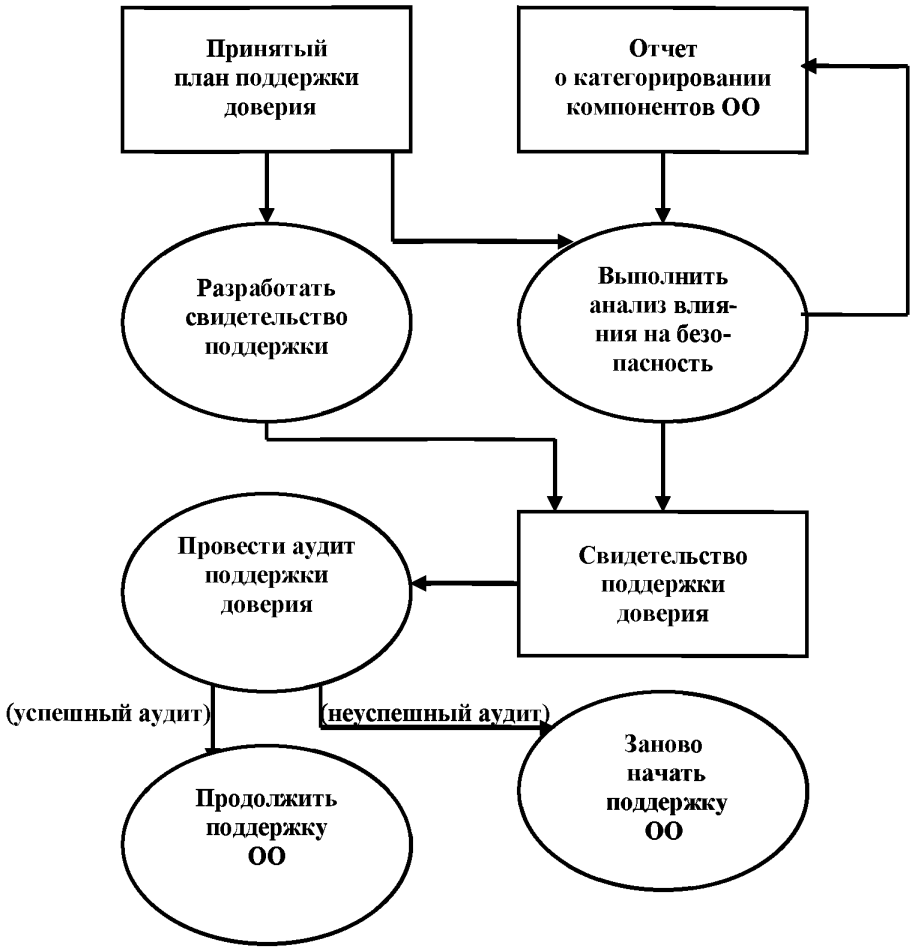


Рисунок 15.3 – Пример подхода к мониторингу ОО

15.2.3 Переоценка

Третья фаза рассматриваемого примера цикла поддержки – переоценка, когда оценщик использует анализ влияния изменений и свидетельство поддержки доверия, чтобы заново выполнить экспертизу частей ОО, применяя компоненты доверия, соответствующие намеченному уровню доверия.

Переход к переоценке предусмотрен в плане поддержки доверия; он же может выполняться вследствие непредвиденных значительных изменений в ОО или его среде, после которых дальнейшая поддержка доверия окажется неприемлемой.

15.3 Класс и семейства поддержки доверия

Для осуществления концепции поддержки доверия был разработан класс AMA, включающий в себя четыре семейства, приведенные в таблице 15.1.

Таблица 15.1 – Представление семейств поддержки доверия

Класс доверия	Семейство доверия	Краткое имя
АМА – Поддержка доверия	План поддержки доверия	AMA_AMP
	Отчет о категорировании компонентов ОО	AMA_CAT
	Свидетельство поддержки доверия	AMA_EVD
	Анализ влияния на безопасность	AMA_SIA

15.3.1 План поддержки доверия

План поддержки доверия (ПД) определяет основную линию поведения при поддержке доверия в зависимости от результатов оценки и проведения категорирования компонентов ОО.

План ПД определяет процедуры, выполняемые разработчиком по мере изменений в ОО или его среде для обеспечения поддержки доверия, которое было установлено в сертифицированном ОО. План ПД распространяется на один цикл поддержки доверия.

План ПД определяет пределы изменений, которые могут быть сделаны в ОО без необходимости переоценки. Конкретный применяемый подход зависим от схемы, но следующие типы изменений, вероятно, обязательно приведут к переоценке, находясь, тем не менее, за пределами плана ПД:

а) значительное изменение задания по безопасности (т.е. значительные изменения среды безопасности, целей безопасности, функциональных требований безопасности или *любое* повышение требований доверия);

б) значительное изменение внешних интерфейсов ФБО, отнесенных к категории обеспечивающих осуществление ПБО;

в) значительное изменение подсистем ФБО, отнесенных к категории обеспечивающих осуществление ПБО (для случаев, когда требования доверия включают в себя ADV_HLD.1 или иерархичные компоненты).

Следует отметить, что на подход к изменениям, вносимым во время поддержки, могут повлиять любые функции, предусмотренные в ОО для поддержки автоматизированной проверки безопасности оцененной конфигурации. Такие функции могут предотвращать неприемлемые или наносящие ущерб изменения при внесении их в эксплуатируемый ОО.

Более подробная спецификация правил находится вне рамок ОК, в частности, из-за того, что смысл выражения *значительное* изменение будет зависеть от типа оцененного ОО и содержания задания по безопасности.

В плане ПД требуется определить или сослаться на процедуры, которые будут использоваться для обеспечения поддержки доверия к ОО на протяжении данного цикла поддержки. Идентифицированы четыре типа процедур, которые рекомендуется применять:

г) по управлению конфигурацией, которые контролируют и регистрируют изменения в ОО для поддержки анализа влияния на безопасность, проводимого разработчиком, а также в сопроводительной документации (включая собственно план ПД);

д) по поддержке "свидетельства доверия" (т.е. поддержке задокументированного свидетельства, предписанного соответствующими требованиями доверия), ключевой аспект которых – функциональное тестирование ФБО и, в частности, политика регрессивного тестирования разработчиком;

е) регламентирующие анализ влияния на безопасность изменений, воздействующих на ОО (включая изменения в среде ОО типа новых угроз или методов нападения, которые могут нуждаться в идентификации и отслеживании), а также поддержку отчета о категорировании компонентов ОО по мере внесения изменений;

ж) по устранению недостатков, включая отслеживание и исправление выявленных недостатков безопасности (как предусматривает ALC_FLR.1).

План ПД, как ожидается, останется действующим до завершения цикла поддержки доверия (т.е. завершения запланированной переоценки), после которого потребуется новый план. План ПД, как ожидается, будет признан недействительным, если разработчик не придерживается этого плана или вносит изменения в ОО, находящиеся вне рамок этого плана, или вынужден внести подобные изменения в ОО, чтобы он оставался эффективным в пределах своей среды. Обновленный план ПД следует заново представить на рассмотрение и принять прежде, чем ОО войдет в новую фазу мониторинга.

План ПД предусматривает, чтобы разработчик определил аналитика безопасности от разработчика, ответственного за постоянный контроль процесса поддержки доверия. Эту роль могут выполнять и несколько человек. Требуется, чтобы аналитик хорошо знал ОО, результаты оценки и примененные требования доверия, что является необходимым условием для успешной работы. Требования не определяют, как достигается этот уровень знаний и опыта; однако, вероятно, предполагаемый аналитик должен пройти обучение в какой-либо форме, чтобы устранить все пробелы в своих знаниях и навыках. Необходимо, чтобы аналитик имел достаточные полномочия внутри организации разработчика для выполнения требований плана ПД и связанных с ним процедур.

15.3.2 Отчет о категорировании компонентов ОО

Назначение отчета о категорировании компонентов ОО состоит в том, чтобы дополнить план ПД категорированием компонентов ОО (например, подсистем ФБО) по их отношению к безопасности. Это категорирование занимает центральное место как в анализе влияния на безопасность, проводимом разработчиком, так и при последующей переоценке ОО.

Проверка отчета о категорировании компонентов ОО происходит в фазе приемки, причем оценщик проверяет только версию отчета для сертифицированной версии ОО. Хотя процедуры поддержки доверия, идентифицированные в плане ПД, требуют от разработчика обновления отчета о категорировании компонентов ОО по мере внесения изменений в ОО, от оценщика не требуется делать заново обзор документа; в то же время, любые такие обновления, вероятно, будут внимательно проверяться в фазе мониторинга.

Отчет о категорировании компонентов ОО распространяется на все представления ФБО на поддерживаемом уровне доверия. Отчет о категорировании компонентов ОО также идентифицирует:

а) любые аппаратные, программно-аппаратные и программные компоненты, которые являются внешними по отношению к ОО (например, аппаратные или программные платформы) и удовлетворяют требованиям безопасности ИТ, определенным в ЗБ;

б) любые инструментальные средства разработки, модификация которых будет влиять на требуемое доверие к тому, что ОО удовлетворяет своему ЗБ.

Отчет о категорировании компонентов ОО также содержит описание подхода, используемого для категорирования компонентов ОО. Как минимум, компоненты ОО требуется разделить на осуществляющие и не осуществляющие ПБО. Описание схемы категорирования предназначено, чтобы дать возможность аналитику безопасности от разработчика выбрать категорию, к которой следует отнести каждый новый компонент ОО, а также, когда потребуется, изменить категорию существующего компонента ОО после изменений в ОО или его ЗБ.

Начальное категорирование компонентов ОО будет основано на свидетельстве, представленном разработчиком для поддержки оценки ОО и независимо подтвержденном оценщиком. Хотя за поддержку документа отвечает аналитик безопасности от разработчика, начальное его содержание может быть основано на результатах оценки ОО.

Представляется полезным включать в ЗБ компонент AMA_CAT.1, где имеется требование поддержки доверия в последующих версиях ОО. Оно применяется независимо от того, достигается ли поддержка доверия использованием требований этого класса или же периодической переоценкой ОО.

15.3.3 Свидетельство поддержки доверия

Необходимо убедиться в том, что доверие к ОО поддерживается разработчиком в соответствии с планом ПД. Это достигается путем подготовки свидетельства, которое демонстрирует поддержку доверия к ОО и независимо проверяется оценщиком. Эта проверка, называемая "аудит поддержки доверия" (аудит ПД), будет, как правило, применяться периодически в фазе мониторинга цикла поддержки доверия к ОО.

Аудит ПД проводят в соответствии с графиком, определенным в плане ПД. Действия разработчика и оценщика, требуемые в AMA_EVD.1, будут выполняться один или несколько раз в фазе мониторинга цикла поддержки доверия. Оценщику, возможно, необходимо непосредственно ознакомиться с условиями разработки ОО, чтобы выполнить экспертизу требуемого свидетельства, но не исключаются и другие способы проверки.

От разработчика требуется представить свидетельство следования процедурам поддержки доверия, указанным в плане ПД. Оно будет включать в себя:

а) записи управления конфигурацией;

б) документацию, используемую при анализе влияния на безопасность, включая текущую версию отчета о категорировании компонентов ОО и свидетельства для всех примененных требований доверия, такие как улучшения проекта, тестовая документация, новые версии руководств и т.д.;

в) свидетельство отслеживания недостатков безопасности.

Проверка оценщиком анализа влияния на безопасность, проведенного разработчиком, (требуемая AMA_SIA.1, от которого зависит AMA_EVD.1) займет центральное место

в аудите ПД. Аудит ПД будет, в свою очередь, способствовать подтверждению анализа, проведенного разработчиком (и, следовательно, уверенности в качестве анализа), обеспечивая подтверждение правильности утверждения разработчика, что доверие к ОО поддерживается для его текущей версии.

При аудите ПД требуется, чтобы оценщик подтвердил выполнение функционального тестирования текущей версии ОО. Это выделяют в отдельную проверку, потому что тестовая документация обеспечивает убедительное доказательство продолжения выполнения ФБО в соответствии со спецификациями. Оценщик выборочно проверяет тестовую документацию для подтверждения, что тестирование разработчиком показывает правильность выполнения ФБО, а покрытие тестами и глубина тестирования соразмерны поддерживаемому уровню доверия.

15.3.4 Анализ влияния на безопасность

Назначение анализа влияния на безопасность состоит в том, чтобы убедиться в поддержке доверия к ОО посредством проводимого разработчиком анализа влияния на безопасность всех изменений, воздействующих на ОО после его сертификации. Эти требования могут применяться в фазе мониторинга или переоценки.

Анализ влияния на безопасность, проводимый разработчиком, основывается на отчете о категорировании компонентов ОО: изменения в осуществляющих ПБО компонентах ОО могут повлиять на доверие к тому, что ОО продолжает отвечать своему ЗБ после изменений. Поэтому все такие изменения требуют анализа их влияния на безопасность, чтобы показать, что они не нарушают доверия к ОО.

Компоненты этого семейства могут использоваться для поддержки последующего аудита ПД или для переоценки ОО.

Следует, чтобы для аудита ПД краткий обзор оценщиком анализа влияния на безопасность служил бы основой последующих действий аудита, которые, в свою очередь, предоставили бы подтверждение результатов анализа, проведенного разработчиком.

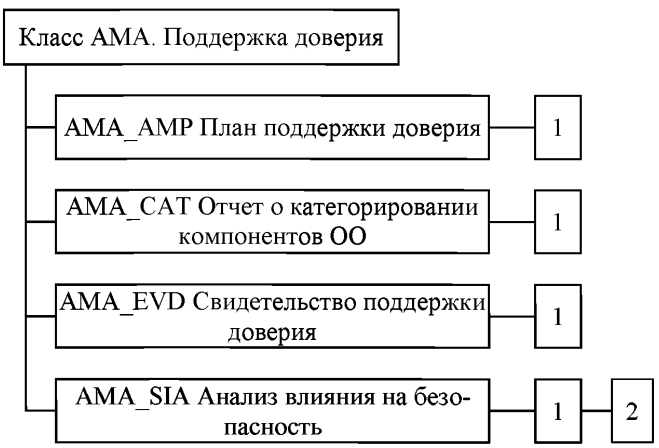
Анализ влияния на безопасность идентифицирует изменения в сертифицированной версии ОО на уровне компонентов ОО, которые или являются новыми, или были модифицированы. Оценщик проверяет точность этой информации либо во время связанного с ними аудита ПД, либо при вызванной ими переоценке ОО.

Следует, чтобы подготовка анализа влияния на безопасность для поддержки переоценки уменьшила трудозатраты оценщика, необходимые для установления требуемого уровня доверия к ОО. Применение AMA_SIA.2, который содержит требование полной экспертизы анализа влияния на безопасность, предоставит, как ожидается, максимальный выигрыш при переоценке. Детализация условий, при которых орган оценки мог бы на практике потребовать использование при переоценке анализа влияния на безопасность, находится за рамками ОК.

16 Класс AMA. Поддержка доверия

Класс AMA содержит требования, предназначенные для применения после того, как ОО был сертифицирован на основе ОК. Эти требования имеют целью сохранить уверенность в том, что ОО продолжит отвечать своему заданию по безопасности после изменений в ОО или его среде. К таким изменениям относятся обнаружение новых угроз или уязвимостей, изменения в требованиях пользователя, а также исправление ошибок, найденных в сертифицированном ОО.

Класс включает в себя четыре семейства с иерархией компонентов в семействах,



показанной на рисунке 16.1:

Рисунок 16.1 – Декомпозиция класса "Поддержка доверия"

16.1 План поддержки доверия (AMA_AMP)

Цели

План поддержки доверия (ПД) идентифицирует процедуры, которые необходимо выполнять разработчику по мере изменений в ОО или его среде для обеспечения поддержки доверия, которое было установлено к сертифицированному ОО. План ПД специфичен для конкретного ОО и зависит от личного опыта и навыков разработчика.

Ранжирование компонентов

Это семейство содержит только один компонент.

Замечания по применению

План ПД распространяется на один цикл поддержки доверия, который представляет собой период от завершения последней выполненной оценки ОО до завершения следующей запланированной переоценки.

Требования AMA_AMP.1.2C и AMA_AMP.1.3C помогают обеспечить четкую идентификацию основания для поддержки доверия в терминах результатов оценки и определения категорирования компонентов ОО. Отчет о категорировании компонентов ОО формируют в соответствии с требованиями семейства AMA_CAT, и он предоставляет основу для анализа влияния на безопасность, выполняемого аналитиком безопасности от разработчика.

Пределы изменений, предусмотренные планом в соответствии с AMA_AMP.1.4C, следует определять в терминах категории компонентов ОО, которые могут подвергнуться изменениям, и уровня представления, на котором могут происходить изменения (со ссылкой, где это необходимо, на отчет о категорировании компонентов ОО).

AMA_AMP.1.5C содержит требование описания *текущих* планов разработчика для любых новых выпусков ОО. Эти планы, естественно, могут изменяться и, следовательно, вызывать обновления в плане ПД. Однако следует отметить, что в данном контексте термин *новый выпуск* не включает в себя, например, второстепенные ("внеплановые") выпуски ОО, обусловленные исправлением незначительных ошибок.

AMA_AMP.1.6C содержит требование определить плановый график аудита ПД (см. семейство AMA_EVD) и намеченную переоценку ОО вместе со строгим обоснованием предложенных графиков. В основу планирования может быть положен определенный период времени (например, ежегодный аудит ПД), или же планирование может быть связано с ожидаемыми новыми выпусками ОО. В графике следует учесть ожидаемые изменения ОО в течение указанного, а также прошедшего между оценкой ОО и составлением плана ПД периодов. В частности, любые изменения, выходящие за рамки плана ПД, могут привести к переоценке.

AMA_AMP.1 План поддержки доверия

Зависимости

ACM_CAP.2 Элементы конфигурации

ALC_FLR.1 Базовое устранение недостатков

AMA_CAT.1 Отчет о категорировании компонентов ОО

Элементы действий разработчика

AMA_AMP.1.1D Разработчик должен представить план ПД.

Элементы содержания и представления свидетельств

AMA_AMP.1.1C План ПД должен содержать или ссылаться на краткое описание ОО, включающее в себя предоставляемые им функциональные возможности безопасности.

AMA_AMP.1.2C План ПД должен идентифицировать сертифицированную версию ОО и ссылаться на результаты оценки.

AMA_AMP.1.3C План ПД должен опираться на отчет о категорировании компонентов ОО для сертифицированной версии ОО.

AMA_AMP.1.4C План ПД должен определить пределы изменений ОО, предусматриваемых планом.

AMA_AMP.1.5C **План ПД должен содержать описание жизненного цикла ОО и идентифицировать текущие планы любых новых выпусков ОО, а также включать в себя краткое описание любых запланированных изменений, которые, как ожидается, будут иметь значительное влияние на безопасность.**

AMA_AMP.1.6C **План ПД должен содержать описание цикла поддержки доверия, устанавливая и строго обосновывая плановый график аудита ПД и намеченную дату следующей переоценки ОО.**

AMA_AMP.1.7C **План ПД должен идентифицировать лицо (а), которое (ые) будет (ут) исполнять роль аналитика безопасности от разработчика для ОО.**

AMA_AMP.1.8C **План ПД должен содержать описание, как роль аналитика безопасности от разработчика обеспечит следование процедурам, которые задокументированы в плане ПД или на которые там имеются ссылки.**

AMA_AMP.1.9C **План ПД должен содержать описание, как роль аналитика безопасности от разработчика обеспечит правильное выполнение всех действий разработчика, связанных с анализом влияния на безопасность изменений, воздействующих на ОО.**

AMA_AMP.1.10C **План ПД должен содержать строгое обоснование, что идентифицированный аналитик безопасности от разработчика хорошо знает задание по безопасности, функциональную спецификацию и (где это необходимо) проект верхнего уровня ОО, а также результаты оценки и все примененные требования доверия для сертифицированной версии ОО.**

AMA_AMP.1.11C **План ПД должен содержать описание или иметь ссылки на процедуры, которые предполагается применять для поддержки доверия к ОО и которые, как минимум, должны включать в себя процедуры управления конфигурацией, поддержки свидетельства доверия, выполнения анализа влияния на безопасность изменений, воздействующих на ОО, и устранения недостатков.**

Элементы действий оценщика

AMA_AMP.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AMA_AMP.1.2E **Оценщик должен подтвердить, что предложенные графики аудита ПД и переоценки ОО приемлемы и согласуются с предполагаемыми изменениями ОО.**

16.2 Отчет о категорировании компонентов ОО (AMA_CAT)

Цели

Назначение отчета о категорировании компонентов ОО состоит в том, чтобы дополнить план ПД обеспечением категорирования компонентов ОО (например, подсистем ФБО) согласно их отношению к безопасности. Категорирование занимает центральное место в

анализе влияния на безопасность, проводимом разработчиком, а также в последующей переоценке ОО.

Ранжирование компонентов

Семейство AMA_CAT содержит только один компонент.

Замечания по применению

Термин "наименее абстрактное из представлений ФБО" в AMA_CAT.1 относится к наименее абстрактному представлению ФБО, которое предоставлено для поддерживаемого уровня доверия. Например, если для ОО поддерживается уровень доверия ОУДЗ, то наименее абстрактное из представлений ФБО – проект верхнего уровня. Следовательно, в этом случае необходимо категорировать следующие компоненты ОО:

а) все внешние интерфейсы ФБО, которые могут быть идентифицированы в функциональной спецификации;

б) все подсистемы ФБО, которые могут быть идентифицированы в проекте верхнего уровня.

В то время как данное семейство содержит требование разделения, по меньшей мере, на две категории, может быть приемлемо (в зависимости от типа ОО) подразделить далее категорию, осуществляющую ПБО, чтобы облегчить анализ влияния на безопасность, проводимый разработчиком. Например, компоненты, осуществляющие ПБО, могли бы быть категорированы на *критичные для безопасности* и на *поддерживающие безопасность*, где:

а) критичные для безопасности компоненты ОО – это те, которые несут *непосредственную* ответственность за осуществление хотя бы одной функции безопасности ИТ, определенной в задании по безопасности;

б) поддерживающие безопасность компоненты ОО – это те, которые не несут *непосредственную* ответственность за осуществление какой-либо функции безопасности ИТ (и поэтому некритичны для безопасности), но на которые, тем не менее, полагаются при поддержке функций безопасности ИТ; эта категория может, в свою очередь, включать в себя компоненты ОО двух различных типов:

   – способствующие выполнению критичных для безопасности компонентов ОО (поэтому для них обязательно правильное функционирование),

   – не способствующие выполнению критичных для безопасности компонентов ОО, но, тем не менее, требующие доверия к тому, что их режим функционирования не является опасным (т.е. не ведет к активизации уязвимостей).

AMA_CAT.1.3C содержит требование идентификации любых инструментальных средств разработки, модификация которых повлияет на доверие к тому, что ОО удовлетворяет своему заданию по безопасности (например, компилятора, используемого для получения объектного кода).

AMA_CAT.1 Отчет о категорировании компонентов ОО

Зависимости

ACM_CAP.2 Элементы конфигурации

Элементы действий разработчика

AMA_CAT.1.1D **Разработчик должен представить отчет о категорировании компонентов ОО для сертифицированной версии ОО.**

Элементы содержания и представления свидетельств

AMA_CAT.1.1C **Отчет о категорировании компонентов ОО должен распределить по категориям каждый компонент ОО, который может быть идентифицирован в каждом представлении ФБО от наиболее до наименее абстрактного, согласно его отношению к безопасности; как минимум, компоненты ОО необходимо разделить на осуществляющие и не осуществляющие ПБО.**

AMA_CAT.1.2C **Отчет о категорировании компонентов ОО должен содержать такое описание используемой схемы категорирования, чтобы можно было определить, как распределять по категориям новые компоненты, включаемые в ОО, а также в каких случаях требуется заново распределять по категориям существующие компоненты ОО вследствие изменений в ОО или в его задании по безопасности.**

AMA_CAT.1.3C **Отчет о категорировании компонентов ОО должен идентифицировать любые инструментальные средства, используемые в среде разработки, модификация которых повлияет на доверие к тому, что ОО удовлетворяет своему заданию по безопасности.**

Элементы действий оценщика

AMA_CAT.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AMA_CAT.1.2E **Оценщик должен подтвердить, что категорирование компонентов и инструментальных средств ОО и используемая схема категорирования приемлемы и согласованы с результатами оценки для сертифицированной версии.**

16.3 Свидетельство поддержки доверия (AMA_EVD)

Цели

Назначение семейства AMA_EVD состоит в том, чтобы убедиться в поддержке разработчиком доверия к ОО в соответствии с планом ПД. Это достигается подготовкой свидетельства, независимо проверяемого оценщиком, которое демонстрирует поддержку доверия к ОО. Указанную проверку, называемую "Аудит ПД", периодически проводят во время действия плана ПД.

Ранжирование компонентов

Семейство содержит только один компонент.

Замечания по применению

Семейство включает в себя некоторые требования к свидетельству, подобные требованиям доверия, определенным в классах ACM, ATE и AVA. В то же время, аудит ПД не

требует проведения оценщиком экспертизы свидетельства в том же самом объеме, как это установлено компонентами перечисленных классов; скорее, здесь достаточно требования, чтобы частичная выборка позволила убедиться в правильности следования процедурам поддержки доверия.

В порядке аудита ПД оценщик проверяет (выборочно) согласованность списка конфигурации и анализа влияния на безопасность с текущей версией ОО для компонентов ОО, которые изменились по сравнению с сертифицированной версией ОО.

AMA_EVD.1.3C содержит требование подготовки свидетельства следования процедурам поддержки доверия из плана ПД. Требование распространяется на все процедуры, упоминаемые в AMA_AMP.1.11C, т.е. необходимо свидетельство применения процедур, относящихся к управлению конфигурацией, поддержке свидетельства доверия, выполнению анализа влияния на безопасность и устранению недостатков.

Свидетельство, требуемое в AMA_EVD.1.4C, содержит список идентифицированных уязвимостей в текущей версии ОО. Это выделено как отдельное требование ввиду важности отсутствия в текущей версии каких-либо недостатков безопасности, которые могли бы быть использованы в среде ОО, с уровнем доверия, полученным при первоначальной оценке. В список в AMA_EVD.1.4C следует включить уязвимости, выявленные в результате:

а) анализа разработчиком, требуемого AVA_VLA.1 или иерархичным компонентом (если он применялся для сертифицированной версии ОО);

б) обнаружения любых других недостатков безопасности, обработанных с использованием процедур их устранения, требуемых ALC_FLR.1 (или ALC_FLR.2) для сертифицированной версии ОО.

AMA_EVD.1.5E содержит требования, чтобы оценщик подтвердил выполнение разработчиком функционального тестирования текущей версии ОО, а также соразмерность покрытия тестами и глубины тестирования с поддерживаемым уровнем доверия. Эту проверку выполняют посредством выборки из тестовой документации для текущей версии ОО.

AMA_EVD.1 Свидетельство процесса поддержки

Зависимости

AMA_AMP.1 План поддержки доверия

AMA_SIA.1 Выборочная проверка анализа влияния на безопасность

Элементы действий разработчика

AMA_EVD.1.1D Аналитик безопасности от разработчика должен представить документацию ПД для текущей версии ОО.

Элементы содержания и представления свидетельств

AMA_EVD.1.1C Документация ПД должна включать в себя список конфигурации и список идентифицированных уязвимостей в ОО.

AMA_EVD.1.2C Список конфигурации должен содержать описание элементов конфигурации, которые составляют текущую версию ОО.

AMA_EVD.1.3C **Документация ПД должна представить свидетельство следования процедурам, которые имеются или на которые есть ссылки в плане ПД.**

AMA_EVD.1.4C **Список идентифицированных уязвимостей в текущей версии ОО должен показать для каждой уязвимости, что она не может быть использована в предполагаемой среде ОО.**

Элементы действий оценщика

AMA_EVD.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AMA_EVD.1.2E **Оценщик должен подтвердить следование процедурам, которые задокументированы или на которые есть ссылки в плане ПД.**

AMA_EVD.1.3E **Оценщик должен подтвердить, что анализ влияния на безопасность для текущей версии ОО согласован со списком конфигурации.**

AMA_EVD.1.4E **Оценщик должен подтвердить, что все изменения, задокументированные при анализе влияния на безопасность для текущей версии ОО, находятся в пределах, установленных планом ПД.**

AMA_EVD.1.5E **Оценщик должен подтвердить, что функциональное тестирование выполнялось на текущей версии ОО соразмерно поддерживаемому уровню доверия.**

16.4 Анализ влияния на безопасность (AMA_SIA)

Цели

Назначение семейства AMA_SIA состоит в том, чтобы убедиться в поддержке доверия к ОО посредством анализа, проводимого разработчиком, по определению влияния на безопасность всех изменений, воздействующих на ОО после его сертификации.

Ранжирование компонентов

Семейство состоит из двух компонентов, ранжированных согласно степени проверки оценщиком правильности анализа влияния на безопасность, проведенного разработчиком.

Замечания по применению

AMA_SIA.1 содержит требование применения выборочного подхода при проверке правильности анализа влияния на безопасность, проведенного разработчиком. AMA_SIA.2 предпочтителен в случаях, когда выборочный подход не рассматривают как достаточный, чтобы убедиться в поддержке доверия к ОО для его текущей версии, но при этом формальную переоценку не считают необходимой.

Оба компонента в этом семействе содержат требование, чтобы анализ влияния на безопасность идентифицировал все новые и модифицированные (по сравнению с сертифицированной версией) компоненты в текущей версии ОО. Точность этой информации проверяют во время связанного с этим аудита ПД (выборочно) или при связанной с этим переоценке ОО, когда список конфигурации проверяют в рамках ACM_CAP.

AMA_SIA.1 Выборочная проверка анализа влияния на безопасность

Зависимости

AMA_CAT.1 Отчет о категорировании компонентов ОО

Элементы действий разработчика

AMA_SIA.1.1D **Аналитик безопасности от разработчика должен представить для текущей версии ОО анализ влияния на безопасность, который учитывает все изменения, воздействующие на ОО, по сравнению с сертифицированной версией.**

Элементы содержания и представления свидетельств

AMA_SIA.1.1C **Анализ влияния на безопасность должен идентифицировать сертифицированный ОО, из которого была получена текущая версия ОО.**

AMA_SIA.1.2C **Анализ влияния на безопасность должен идентифицировать все новые и модифицированные компоненты ОО, которые категорированы как осуществляющие ПБО.**

AMA_SIA.1.3C **Анализ влияния на безопасность должен для каждого изменения, воздействующего на задание по безопасности или представления ФБО, содержать краткое описание изменения и всех последствий, к которым оно приводит на более низких уровнях представления.**

AMA_SIA.1.4C **Анализ влияния на безопасность должен для каждого изменения, воздействующего на задание по безопасности или представления ФБО, идентифицировать все функции безопасности ИТ и компоненты ОО, категорированные как осуществляющие ПБО, на которые влияет данное изменение.**

AMA_SIA.1.5C **Анализ влияния на безопасность должен для каждого изменения, которое приводит к модификации представления реализации ФБО или среды ИТ, идентифицировать свидетельство тестирования, показывающее для требуемого уровня доверия, что ФБО остаются правильно реализованными и после изменения.**

AMA_SIA.1.6C **Анализ влияния на безопасность должен для каждого применяемого требования из классов доверия "Управление конфигурацией" (ACM), "Поддержка жизненного цикла" (ALC), "Поставка и эксплуатация" (ADO) и "Руководства" (AGD) идентифицировать все поставляемые материалы оценки, которые изменились, и содержать краткое описание каждого изменения и его воздействие на доверие к ОО.**

AMA_SIA.1.7C **Анализ влияния на безопасность должен для каждого применяемого требования в классе доверия "Оценка уязвимости" (AVA) идентифицировать, какие поставляемые материалы оценки изменились, а какие нет, и привести доводы для принятого решения, обновлять или нет данный поставляемый материал.**

Элементы действий оценщика

AMA_SIA.1.1E **Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.**

AMA_SIA.1.2E **Оценщик должен выборочно проверить, что при анализе влияния на безопасность изменения задокументированы на приемлемом уровне детализации вместе с соответствующим строгим обоснованием поддержки доверия в текущей версии ОО.**

AMA_SIA.2 Экспертиза анализа влияния на безопасность

Зависимости

AMA_CAT.1 Отчет о категорировании компонентов ОО

Элементы действий разработчика

AMA_SIA.2.1D Аналитик безопасности от разработчика должен представить для текущей версии ОО анализ влияния на безопасность, который учитывает все изменения, воздействующие на ОО, по сравнению с сертифицированной версией.

Элементы содержания и представления свидетельств

AMA_SIA.2.1C Анализ влияния на безопасность должен идентифицировать сертифицированный ОО, из которого была получена текущая версия ОО.

AMA_SIA.2.2C Анализ влияния на безопасность должен идентифицировать все новые и модифицированные компоненты ОО, которые категорированы как осуществляющие ПБО.

AMA_SIA.2.3C Анализ влияния на безопасность должен для каждого изменения, влияющего на задание по безопасности или представления ФБО, содержать краткое описание изменения и всех последствий, к которым оно приводит на более низких уровнях представления.

AMA_SIA.2.4C Анализ влияния на безопасность должен для каждого изменения, влияющего на задание по безопасности или представления ФБО, идентифицировать все функции безопасности ИТ и компоненты ОО, категорированные как осуществляющие ПБО, на которые воздействует данное изменение.

AMA_SIA.2.5C Анализ влияния на безопасность должен для каждого изменения, которое приводит к модификации представления реализации ФБО или среды ИТ, идентифицировать свидетельство тестирования, показывающее для требуемого уровня доверия, что ФБО остаются правильно реализованными и после изменения.

AMA_SIA.2.6C Анализ влияния на безопасность должен для каждого применяемого требования из классов доверия "Управление конфигурацией" (ACM), "Поддержка жизненного цикла" (ALC), "Поставка и эксплуатация" (ADO) и "Руководства" (AGD) идентифицировать все поставляемые материалы оценки, которые изменились, и содержать краткое описание каждого изменения и его воздействие на доверие к ОО.

AMA_SIA.2.7C Анализ влияния на безопасность должен для каждого применяемого требования в классе доверия "Оценка уязвимости" (AVA) идентифицировать, какие поставляемые материалы оценки изменились, а какие нет, и привести доводы для принятого решения, обновлять или нет данный поставляемый материал.

Элементы действий оценщика

AMA_SIA.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AMA_SIA.2.2E Оценщик должен проверить, что при анализе влияния на безопасность **все** изменения задокументированы на приемлемом уровне детализации вместе с соответствующим строгим обоснованием поддержки доверия в текущей версии ОО.

Приложение А
(справочное)
Перекрестные ссылки между компонентами доверия

Зависимости между компонентами, приведенные в разделах 8-14 и 16, являются прямыми зависимостями между компонентами доверия. В таблице А.1 объединены как прямые, так и косвенные зависимости. Косвенные зависимости являются, в конечном счете, результатом последовательного учета всех зависимостей каждого компонента, приведенного в списке зависимостей.

Таблица А.1 – Зависимости между компонентами доверия

Имена компонентов	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
AUT.1-2		**3**	*1*												*1*											
CAP.1-2																										
CAP.3-4			**1**												**1**											
CAP.5			**1**												**2**											
SCP.1-3		**3**													*1*											
DEL.1																										
DEL.2-3		**3**	*1*												*1*											
IGS.1-2						*1*					*1*		**1**													
FSP.1-4											**1**															
HLD.1-2						**1**					**1**															
HLD.3-4						**3**					**2**															
HLD.5						**4**					**3**															
IMP.1-2						*1*	*2*			**1**	**1**							**1**								
IMP.3						*1*	*2*		**1**	**1**	**1**							**1**								
INT.1-2						*1*	*2*	**1**		**1**	*1*							*1*								
INT.3						*1*	*2*	**2**		**1**	*1*							*1*								
LLD.1						*1*	**2**				**1**															
LLD.2						*3*	**3**				**2**															
LLD.3						*4*	**5**				**3**															
RCR.1-3																										
SPM.1-3						**1**					*1*															
ADM.1						**1**					*1*															
USR.1						**1**					*1*															
DVS.1-2																										
FLR.1-3																										
LCD.1-3																										
TAT.1-3						*1*	*2*	**1**		*1*	*1*															
COV.1-3						**1**					*1*										**1**					
DPT.1						*1*	**1**				*1*										**1**					
DPT.2						*1*	**2**			**1**	*1*										**1**					
DPT.3						*1*	**2**	**2**		**1**	*1*							*1*			**1**					

Окончание таблицы А.1

Имена компонентов	AUT	CAP	SCP	DEL	IGS	FSP	HLD	IMP	INT	LLD	RCR	SPM	ADM	USR	DVS	FLR	LCD	TAT	COV	DPT	FUN	IND	CCA	MSU	SOF	VLA
FUN.1-2																										
IND.1						**1**					*1*		**1**	**1**												
IND.2-3						**1**					*1*		**1**	**1**							**1**					
CCA.1-3						**2**	*2*	**2**		*1*	*1*		**1**	**1**				*1*								
MSU.1-3					**1**	**1**					*1*		**1**	**1**												
SOF.1						**1**	**1**				*1*															
VLA.1						**1**	**1**				*1*		**1**	**1**												
VLA.2-4						**1**	**2**	**1**		**1**	*1*		**1**	**1**				*1*								
AMP.1		**2**														**1**										
CAT.1		**2**																								
EVD.1																										
SIA.1-2																										

Примечание – В таблице А.1 в боковике содержатся сокращенные обозначения компонентов (приведены только первые три буквы имени семейства и номер компонента или диапазон номеров компонентов). Каждая заполненная ячейка в таблице указывает на компонент, идентифицированный первыми тремя буквами имени семейства в наименовании графы и номером компонента в ячейке, для которого компонент, указанный в боковике, является зависимым. Полужирным шрифтом выделены прямые зависимости, курсивом – косвенные зависимости. Серый фон выделяет пересечение компонента с самим собой. Зависимости компонентов класса AMA от компонентов доверия включены в таблицу А.1, в то время как внутренние зависимости класса AMA приведены в таблице А.2. От компонентов класса AMA не зависят никакие компоненты других классов, поэтому в таблице А.1 нет граф, представляющих семейства класса AMA.

Таблица А.2 – Внутренние зависимости класса AMA

Имена компонентов класса AMA	AMP	CAT	EVD	SIA
AMP.1		**1**		
CAT.1				
EVD.1	**1**	*1*		**1**
SIA.1-2		**1**		

Приложение Б
(справочное)
Перекрестные ссылки ОУД и компонентов доверия

Взаимосвязь между оценочными уровнями доверия и классами, семействами и компонентами доверия приведена в таблице Б.1.

Таблица Б.1 – Обзор оценочных уровней доверия

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