ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Технологии информационные

МЕТОДЫ ЗАЩИТЫ

Методология оценки защиты информационных технологий

СТ РК ИСО/МЭК 18045-2009

ISO/IEC 18045:2008 (E) Information technology. Security techniques. Methodology for IT security evaluation (IDT)

II - том

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 РАЗРАБОТАН И ВНЕСЕН РГП «Казахстанский институт стандартизации и сертификации» и Техническим комитетом по стандартизации 34 «Информационные технологии» АО «Национальные информационные технологии»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Председателя Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан от 17ноября 2009г. № 563-од

3 Настоящий стандарт идентичен международному стандарту ISO/IEC 18045:2008 (e) Information technology. Security techniques. Methodology for IT security evaluation (Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий).

Международный стандарт разработан Объединенным Техническим комитетом ИСО/МЭК ОТК 1, Информационная технология, Подкомитет ПК 27, Методы и средства обеспечения безопасности ИТ.

Перевод с английского языка (en)

Степень соответствия – идентичная (IDT)

4 В настоящем стандарте реализованы нормы и положения Закона Республики Казахстан «О техническом регулировании», Соглашения Всемирной торговой организации по техническим барьерам в торговле (ТБТ)

5 СРОК ПЕРВОЙ ПРОВЕРКИ **2014 год**
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ **5 лет**

6 ВВЕДЕН ВПЕРВЫЕ

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Нормативные документы по стандартизации», а текст изменений и поправок – в ежемесячно издаваемых информационных указателях «Государственные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Государственные стандарты»

Содержание

II - том

Введение

Целевая аудитория настоящего стандарта - это преимущественно использующие ИСО/МЭК 15408 и эксперты органов по сертификации, подтверждающие действия оценщиков; заявители на проведение оценки, разработчики, авторы ПЗ/ЗБ и другие стороны, заинтересованные в безопасности ИТ, являющиеся вторичной аудиторией.

Список, связанных с методологией действий, которые могут быть обработаны индивидуальными системами, можно найти в Приложении А.

13 Вид деятельности AVA Оценка уязвимостей

13.1 Введение

Оценка уязвимостей позволяет сделать заключение о существовании и пригодности для использования в предопределенной среде недостатков или слабых мест в ОО. Это заключение основывается на анализе свидетельств оценки и общедоступных источников информации, выполненных оценщиком, и поддерживается тестированием на проникновение, выполненным оценщиком.

13.2 Анализ уязвимостей (AVA_VAN)

13.2.1 Оценка подвида деятельности (AVA_VAN.1)

13.2.1.1 Цели

Цель данного подвида деятельности – сделать заключение, имеет ли ОО, находящийся в своей предопределенной среде, явные уязвимости, пригодные для использования

13.2.1.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) руководства;

в) ОО, пригодный для тестирования;

г) общедоступная информация выявление потенциальных уязвимостей.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа по подтверждению соответствия).

13.2.1.3 Замечания по применению

Оценщик должен продумать выполнение дополнительных тестов потенциальных уязвимостей выявленных во время выполнения других действий по оценке.

Использование термина руководство в этом подвиде деятельности относиться к действующему руководству и предварительному руководству.

Уязвимости могут быть или не быть идентифицированы в общедоступных источниках информации, и могут требовать или не требовать навыка для их использования. Эти два аспекта являются связанными, но различными. Не следует предполагать, что уязвимость может быть легко использована просто потому, что она идентифицирована в общедоступных источниках.

13.2.1.4 Операция AVA_VAN.1.1E

ОО должен быть пригоден для тестирования.

13.2.1.4.1 Операция AVA_VAN.1-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена возможностями УК подвид деятельности (ALC_CMC) и идентифицирована во вводной части ЗБ.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ.

Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. В ЗБ могут быть и другие предположения, которые не касаются среды тестирования. Например, предположение относительно допусков пользователей может не касаться среды тестирования, однако, предположение относительно единой точки подключения к сети, как правило, касается среды тестирования.

При использовании, каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика

13.2.1.4.2 Операция AVA_VAN.1-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности (AGD_PRE.1) позволит считать выполненной данную операцию, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данная операция могла бы удовлетворить операцию AGD_PRE.1-3.

13.2.1.5 Действие AVA_VAN.1.2E

13.2.1.5.1 Операция AVA_VAN.1-3

Оценщик должен исследовать источники общедоступной информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик должен исследовать источники общедоступной информации, чтобы обеспечить идентификацию возможных потенциальных уязвимостей в ОО. Существует много источников общедоступной информации, которые должны быть исследованы такие как списки почтовой рассылки, форумы по безопасности во всемирной паутине которые описывают известные уязвимости в специфических технологиях.

Оценщик не должен ограничивать свои исследования общедоступной информации вышеуказанными источниками, а должен исследовать любую другую важную доступную информацию

Наряду с анализом предоставленных свидетельств оценщик будет использовать информацию в общедоступных источниках для последующих поисков. Когда оценщик определить интересующую область, оценщик должен исследовать общедоступную информацию, которая относится к интересующей области.

Доступность информации, легко доступной нарушителю помогает идентифицировать и способствует нападению, существенно действует, увеличивая потенциал нападения данным взломщиком. Доступность информации об уязвимостях и изощренных средствах взлома в Интернете увеличивает вероятность того, что эта информация будет использована в попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска такой информации делают её легко доступной для оценщика и определение противодействия к опубликованным потенциальным уязвимостям и хорошо известным простым атакам может быть достигнута высокоэффективным способом.

Поиск общедоступной информации должен быть сфокусирован на ресурсах, которые занимаются продуктами, к типу которых относится ОО. Экстенсивность такого поиска должна определяться следующими факторами: тип ОО, опыт работы оценщика с ОО такого типа, вероятность потенциальных атак и уровень ADV по имеющимся свидетельствам.

Процесс идентификации повторяющийся, где идентификация одной потенциальной уязвимости может привести к идентификации другой интересующей области, которая требует дальнейшего исследования.

Оценщик должен указать, какие действия были проделаны, чтобы идентифицировать потенциальные уязвимости в общедоступной информации. Однако, при таком методе поиска оценщик, возможно не сможет описать операцию по идентификации потенциальных уязвимостей перед началом исследования, так как метод может быть выявлен в результате полученных во время поиска.

Оценщик укажет исследованные свидетельства по окончании поиска потенциальных уязвимостей.

13.2.1.5.2 Операция AVA_VAN.1-4

Оценщик должен указать в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к ОО в его предопределенной среде.

Возможно, будет установлено что нет необходимости в дальнейшем исследовании потенциальных уязвимостей, если оценщик идентифицирует что меры в предопределенной среде, ни ИТ ни не-Ит среде предотвращают использование уязвимости в предопределенной среде.

Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования. Если оценщик определить, что потенциальная уязвимость непригодна в предопределенной среде, оценщик указывает полностью причины для отказа от исследования потенциальной уязвимости.

В остальных случаях, оценщик указывает потенциальные уязвимости для дальнейших исследований.

Список потенциальных уязвимостей пригодных к ОО в его предопределенной среде, и которые могут быть использованы для выполнения тестов проникновения, должны быть указаны в ТОО оценщиком.

13.2.1.6 Действие AVA_VAN.1.3E

13.2.1.6.1 Операция AVA_VAN.1-5

Оценщик должен разработать тесты проникновения, основанные на независимом поиске потенциальных уязвимостей.

Оценщик должен достаточно подготовиться к тестированию проникновения, чтобы определить восприимчивость ОО в его преопределенной среде к потенциальным уязвимостям, идентифицированным в ходе поиска в источниках общедоступной информации. Любая текущая информация, предоставленная оценщику третьей стороной (например, органом по сертификации) относящаяся к известным потенциальным уязвимостям должна быть исследована оценщиком наряду, с любой потенциальной уязвимостью выявленной в ходе выполнения других действий по оценке.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную

уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

13.2.1.6.2 Операция AVA_VAN.1-6

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на списке потенциальных уязвимостей детализация, которой достаточна, чтобы обеспечить воспроизводимость тестов.

Тестовая документация должна включать:

а) идентификацию тестируемой уязвимости ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения теста проникновения;

в) инструкции по установке всех предварительных начальных условий выполнения теста проникновения;

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого после тестового состояния ОО.

Оценщик готовится к тестированию проникновения, основанным на списке потенциальных уязвимостей идентифицированных в ходе поисков в общедоступных источниках.

Не предполагается определение оценщиком пригодности использования уязвимостей помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы ИФБО или другого ОО, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо иметь;

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости).

г) замена физического тестирования теоретическим анализом особенно существенна, когда результаты первоначально анализа могут быть экстраполированы, чтобы продемонстрировать что повторяющиеся попытки атак, вероятно, будут иметь успех после определенного числа попыток

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

Цель установления данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат

13.2.1.6.3 Операция AVA_VAN.1-7

Оценщик должен провести тестирование проникновения

Оценщик использует документацию для тестов проникновения, разработанную на операции AVA_VAN.1-5 как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может придумать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если выполнялись оценщиком, заносятся в документацию для тестов проникновения. Такие тесты могут потребоваться, чтобы разобраться с непредвиденными результатами или наблюдениями или исследовать потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

13.2.1.6.4 Операция AVA_VAN.1-8

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя, некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общий результат должен быть идентичным. Любые различия следует строго обосновать.

13.2.1.6.5 Операция AVA_VAN.1-9

Оценщик должен привести в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления этой информации состоит в том, чтобы дать краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных операций тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по сертификации получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) Тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) ИФБО подвергшиеся тестированию проникновения. Краткий перечень ИФБО, и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

в) Вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

13.2.1.6.6 Операция AVA_VAN.1-10

Оценщик должен исследовать результаты всего тестирования, чтобы определить является ли ОО, находящийся в своей предопределенной среде, стойким к нарушителю, обладающему низким потенциалом нападения

Если результаты показывают, что ОО, находящийся в своей предопределенной среде, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по данному действию оценщиком делается отрицательное заключение.

Чтобы определить потенциал атаки необходимый для использования конкретной уязвимости и может ли она вследствие этого использоваться в заданной среде должен использоваться Пункт В.4 руководства. Нет

необходимости вычислять потенциал атаки каждый раз, за исключением случаев, когда существуют сомнения, может ли, или нет, уязвимость использована нарушителем, обладающим потенциалом меньший, чем умеренный.

13.2.1.6.7 Операция AVA_VAN.1-11

Оценщик должен привести в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) ее источник (например, стала известна при выполнении действий по оценке, известна оценщику, прочитана в публикации);

б) не отвечает ТФБ;

в) описание;

г) пригодна ли она для использования в предопределенной среде или нет (т.е., пригодная ли для использования или является остаточной уязвимостью);

д) количество времени, уровень анализа, уровень знаний ОО, уровень возможности и оборудование необходимое для выполнения идентификации уязвимости, и соответствующие значения, используя Таблицу В.2 и В.3 Приложения В.4.

13.2.2 Оценка подвида деятельности (AVA_VAN.2)

13.2.2.1 Цели

Цель этого подвида деятельности определить имеет ли ОО в своей преопределенной среде уязвимости пригодные нарушителю, обладающему низким потенциалом нападения

13.2.2.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект ОО;

г) описание структуры безопасности;

д) руководства;

е) ОО, пригодный для тестирования;

Оставшиеся подразумевающиеся свидетельства оценки для этого подвида деятельности зависят от компонентов, которые включены в пакет доверия. Свидетельства обеспечивающие каждый компонент, используются, как исходные в данном подвиде деятельности.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа по подтверждению соответствия).

13.2.2.3 Замечания по применению

Оценщик должен продумать выполнение дополнительных тестов потенциальных уязвимостей выявленных во время выполнения других действий по оценке.

13.2.2.4 Действие AVA_VAN.2.1E

ОО должен быть пригоден для тестирования.

13.2.2.4.1 Операция AVA_VAN.2-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена возможностями УК (ALC_CMC) подвидом деятельности и идентифицирована во вводной части ЗБ.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ.

Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ.

Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. Например, предположение относительно допусков пользователей может не касаться среды тестирования, однако, предположение относительно единой точки подключения к сети, как правило, касается среды тестирования

При использовании, каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика

13.2.2.4.2 Операция AVA_VAN.2-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами.

Например, предшествующее успешное завершение подвида деятельности ADO_IGS.1 позволит считать выполненной данную операцию, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данная операция могла бы удовлетворить операцию ADO_IGS.1-2.

13.2.2.5 Действие AVA_VAN.2.2E. Операция AVA_VAN.2-3

Оценщик должен исследовать источники общедоступной информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик должен исследовать источник общедоступной информации, чтобы обеспечить идентификацию возможных потенциальных уязвимостей в ОО. Существует много источников общедоступной информации, которые должны быть исследованы такие как:

а) специализированные издания (журналы, книги);

б) научные статьи.

Оценщик не должен ограничивать свои исследования общедоступной информации вышеуказанными источниками, а должен исследовать любую другую важную доступную информацию

Наряду с анализом предоставленных свидетельств оценщик будет использовать информацию в общедоступных источниках для последующих поисков. Ели оценщик идентифицирует область интересов, оценщик должен изучить общедоступную информацию, связанную с этой областью интересов. Доступность информации, легко доступной нарушителю помогает идентифицировать и способствует нападению, существенно действует, увеличивая потенциал нападения данным взломщиком. Доступность информации об уязвимостях и изощренных средствах взлома в Интернете увеличивает вероятность того, что эта информация будет использована в попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска такой информации делают её легко доступной для оценщика и определение противодействия к опубликованным потенциальным уязвимостям и хорошо известным простым атакам может быть достигнута высокоэффективным способом.

Поиск общедоступной информации должен быть сфокусирован на ресурсах, которые занимаются продуктами, к типу которых относится ОО. Экстенсивность такого поиска должна определяться следующими факторами: тип ОО, опыт работы оценщика с ОО такого типа, вероятность потенциальных атак и уровень ADV по имеющимся свидетельствам.

Процесс идентификации повторяющийся, где идентификация одной потенциальной уязвимости

может привести к идентификации другой интересующей области, которая требует дальнейшего исследования.

Оценщик должен указать, какие действия были проделаны, чтобы идентифицировать потенциальные уязвимости в общедоступной информации.

Однако, при таком методе поиска оценщик, возможно, не сможет описать операцию по идентификации потенциальных уязвимостей перед началом исследования, так как метод может быть выявлен в результате полученных во время поиска.

Оценщик укажет исследованные свидетельства по окончании поиска потенциальных уязвимостей.

Данная выборка свидетельств может быть получена из источников определенных оценщиком связанных со свидетельствами, которые нарушитель предполагается, может достичь или в соответствии с другими логическими обоснованиями, предоставленными оценщиком.

13.2.2.6 Действие AVA_VAN.2.3E

13.2.2.6.1 Операция AVA_VAN.2-4

Оценщик должен изучить ЗБ, руководства, функциональную спецификацию, проект ОО, описание структуры безопасности, чтобы идентифицировать потенциальные уязвимости в ОО.

Поиск свидетельств должен быть закончен в соответствии с этим спецификации и документы ОО должны быть проанализированы и после этого строятся гипотезы и предположения об уязвимостях в ОО

Затем перечень предполагаемых уязвимостей упорядочивается по приоритетам на основе оцененной вероятности существования уязвимости и, предполагая, что уязвимость существует, на основе потенциала нападения, требуемого для ее использования, а также возможностей, предоставляющихся нарушителю, или предполагаемого ущерба, который обусловлен конкретной уязвимостью. Упорядоченный по приоритетам перечень потенциальных уязвимостей используется для руководства тестированием проникновения в ОО.

Описание структуры безопасности предусматривает анализ разработчиком уязвимостей, вследствие чего в нем задокументировано как ФБО защищается от вмешательства недоверенных субъектов и предотвращает обход требований функции безопасности. Вследствие этого оценщик должен использовать данные описания защиты ФБО как основу для поиска возможных путей нарушения ФБО.

Исходя из конкретных угроз, присутствующих в предопределенной среде, оценщику при независимом анализе уязвимостей следует рассмотреть характерные уязвимости под каждой из следующих рубрик:

а) уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом по сертификации;

б) обход;

в) вмешательство;

г) прямые нападения;

д) наблюдение;

е) неправильное применение.

Пункты б) - е) объясняются более детально в Приложении В.

Описания структуры безопасности должны быть исследованы в отношении вышеуказанных характерных потенциальных уязвимостей.

Каждая потенциальная уязвимость должна быть исследована на предмет наличия возможных путей, при которых обходятся защита ФБО и разрушаются ФБО.

13.2.2.6.2 Операция AVA_VAN.2-5

Оценщик должен указать в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к ОО в его предопределенной среде.

Возможно, будет установлено, что нет необходимости в дальнейшем исследовании потенциальных уязвимостей, если оценщик идентифицирует что меры в предопределенной среде, ни в ИТ ни в другой среде не предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования

Если оценщик определить, что потенциальная уязвимость непригодна в преопределенной среде, оценщик указывает полностью причины для отказа от исследования потенциальной уязвимости.

В остальных случаях, оценщик указывает потенциальные уязвимости для дальнейших исследований.

Список потенциальных уязвимостей пригодных к ОО в его предопределенной среде, и которые могут быть использованы для выполнения тестов проникновения, должны быть указаны в ТОО оценщиком.

13.2.2.7 Действие AVA_VAN.2.4E

13.2.2.7.1 Операция AVA_VAN.2-6

Оценщик должен разработать тесты проникновения, основанные на независимом поиске потенциальных уязвимостей.

Оценщик должен достаточно подготовиться к тестированию проникновения, чтобы определить восприимчивость ОО в его преопределенной среде к потенциальным уязвимостям, идентифицированным в ходе поиска в источниках общедоступной информации. Любая текущая информация, предоставленная оценщику третьей стороной (например, органом по сертификации) относящаяся к известным потенциальным уязвимостям должна быть исследована оценщиком наряду, с любой потенциальной уязвимостью выявленной в ходе выполнения других действий по оценке.

Оценщик извещается, что для анализа описаний структуры безопасности в поиске уязвимостей (как детализировано в AVA_VAN.3-4), тестирование должно производиться с подтверждением свойств структуры. Вероятно, что

потребуется тест с отрицательным результатом опровергающий свойства структуры безопасности. В разработке стратегии тестирования проникновения, оценщик должен убедиться, что все аспекты описании структуры безопасности протестированы, как тестирование функциональности так и тестирование проникновения оценщиком.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение.

Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

Руководство по вычислению необходимого потенциала нападения для использования потенциальной уязвимости дано в Приложение В.4.

Уязвимости, предполагаемые как пригодные для использования только нарушителями, обладающими низким, умеренным или высоким потенциалом нападения, не приводят к отрицательному заключению по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то соответствующие уязвимости в дальнейшем не рассматриваются в качестве исходных данных для тестирования проникновения. Однако такие уязвимости приводятся в ТОО в качестве остаточных уязвимостей.

Уязвимости, предполагаемые как потенциально пригодные для использования нарушителем, обладающим низким потенциалом нападения, и приводящие к нарушению целей безопасности, следует отнести к самым высокоприоритетным потенциальным уязвимостям, содержащимся в перечне, используемом для руководства тестированием проникновения в ОО.

13.2.2.7.2 Операция AVA_VAN.2-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на перечне потенциальных уязвимостей, детализация, которой достаточна, чтобы обеспечить повторяемость тестов. Тестовая документация должна включать:

а) идентификацию явной уязвимости, на предмет которой тестируется ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения конкретного теста проникновения;

в) инструкции по установке всех предварительных начальных условий выполнения теста проникновения;

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого после тестового состояния ОО.

Оценщик готовится к тестированию проникновения основанным на перечне потенциальных уязвимостей идентифицированных в ходе поисков в общедоступных местах и анализа свидетельств оценки.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости.

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы ИФБО или другого ОО, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции; (Возможно, что оценщику потребуется интерфейс к ОО другой не ОФБ, чтобы продемонстрировать свойства ОФБ описанные в описаниях структуры безопасности (как того требует ADV_ARC). Это должно быть учтено, хотя, данные интерфейсы ОО предполагают способы тестирования свойств ФБО, они не являются объектами тестирования;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь;

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости);

г) замена физического тестирования теоретическим анализом особенно существенна, когда результаты первоначально анализа могут быть экстраполированы чтобы продемонстрировать что повторяющиеся попытки атак вероятно, будут иметь успех после определенного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной явной уязвимости.

Цель определения данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат.

13.2.2.7.3 Операция AVA_VAN.2-8

Оценщик должен провести тестирование проникновения

Оценщик использует документацию для тестов проникновения, разработанную на операции AVA_VAN.2-6 как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может придумать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если выполнялись оценщиком, заносятся в документацию для тестов проникновения. Такие тесты могут потребоваться, чтобы разобраться с непредвиденными результатами или наблюдениями или исследовать потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

Если тест проникновения показал, что предполагавшейся потенциальной уязвимости не существует, оценщик должен определить был ли собственный анализ оценщика неправильным, или подготовленная оценка неверная или недостаточная.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение

Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

13.2.2.7.4 Операция AVA_VAN.2-9

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общий результат должен быть идентичным. Любые неожиданные результаты тестирования должны быть исследованы. Влияние на оценку должны быть установлены и обоснованы.

13.2.2.7.5 Операция AVA_VAN.2-10

Оценщик должен привести в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления этой информации состоит в том, чтобы дать краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных операций тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по сертификации получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения.

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) ИФБО подвергшиеся тестированию проникновения. Краткий перечень ИФБО, и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

в) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

13.2.2.7.6 Операция AVA_VAN.2-11

Оценщик должен проанализировать результаты всех тестов проникновения и определить имеет ли ОО в своей преопределенной среде уязвимости пригодные нарушителю, обладающему низким потенциалом нападения.

Если результаты показывают, что ОО, находящийся в своей предопределенной среде, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по данному действию оценщиком делается отрицательное заключение.

Чтобы определить потенциал атаки необходимый для использования конкретной уязвимости и может ли она вследствие этого использоваться в заданной среде должен использоваться Пункт В.4 руководства.

Нет необходимости вычислять потенциал атаки каждый раз, за исключением случаев, когда существуют сомнения, может ли или нет

уязвимость использована нарушителем, обладающим потенциалом меньший, чем умеренный.

13.2.2.7.7 Операция AVA_VAN.2-12

Оценщик должен привести в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) ее источник (например, стала известна при выполнении действий по оценке, известна оценщику, прочитана в публикации);

б) не отвечает ТФБ;

в) описание;

г) пригодна ли она для использования в предопределенной среде или нет (т.е., пригодная ли для использования или является остаточной уязвимостью);

д) количество времени, уровень анализа, уровень знаний ОО, уровень возможности и оборудование необходимое для выполнения идентификации уязвимости, и соответствующие значения, используя Таблицу В.2 и В.3 Приложения В.

13.2.3 Оценка подвида деятельности (AVA_VAN.3)

13.2.3.1 Цели

Цель этого подвида деятельности определить имеет ли ОО в своей преопределенной среде уязвимости пригодные нарушителю, обладающему низким потенциалом нападения

13.2.3.2 Исходные данные

Свидетельствами оценки для данного подвида деятельности являются:

а) ЗБ;

б) функциональная спецификация;

в) проект ОО;

г) описание структуры безопасности

д) реализация выбранного подмножества;

е) руководства;

ж) ОО, пригодный для тестирования;

и) общедоступная информация обеспечивающая идентификацию потенциальных уязвимостей.

Оставшиеся подразумевающиеся свидетельства оценки для этого подвида деятельности зависят от компонентов, которые включены в пакет доверия. Свидетельства, обеспечивающие каждый компонент, используются, как исходные в данном подвиде деятельности.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа по подтверждению соответствия).

13.2.3.3 Замечания по применению

Во время выполнений действий по оценке оценщик может идентифицировать области интереса.

Это специфические части свидетельств ОО, которые оценщик оставляет, хотя свидетельства отвечают требованиям деятельности, с которыми связаны свидетельства. Для примера, отдельная спецификация интерфейса ищет специальный комплект, и потому будет склонна выдавать ошибки как во время разработки ОО, так и во время эксплуатации ОО. На этой операции потенциальная уязвимость не будет очевидна, требуется дальнейшее исследование. Это не случайно, поэтому требуется дальнейшее исследование.

Специальный метод идентификации потенциальной уязвимости это анализ свидетельств с целью идентификации любой потенциальной уязвимости очевидный в содержащейся информации. Это неструктурированный анализ, так как метод не определен. Последующие руководства, посвященные анализу уязвимостей указаны в Приложении В.

13.2.3.4 Действие AVA_VAN.3.1E

ОО должен быть пригоден для тестирования.

13.2.3.4.1 Операция AVA_VAN.3-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена возможностями УК подвидами деятельности и идентифицирована во вводной части ЗБ.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ.

Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ. Оценщику следует рассмотреть описанные в ЗБ предположения относительно аспектов безопасности среды ОО, которые могут касаться среды тестирования. Например, предположение относительно допусков пользователей может не касаться среды тестирования, однако, предположение относительно единой точки подключения к сети, как правило, касается среды тестирования

При использовании, каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика

13.2.3.4.2 Операция AVA_VAN.3-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно.

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами. Например, предшествующее успешное завершение подвида деятельности (AGD_PRE.1) позволит считать выполненной данную операцию, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данная операция могла бы удовлетворить операцию AGD_PRE.1-3..

13.2.3.5 Действие AVA_VAN.3.2E. Операция AVA_VAN.3-3

Оценщик должен исследовать источники общедоступной информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик должен исследовать общедоступную информацию, чтобы обеспечить идентификацию возможных потенциальных уязвимостей в ОО.

Существует много источников общедоступной информации, которые оценщик должен исследовать, используя такие как, например доступные во всемирной паутине, включая:

а) протоколы конференций;

б) специализированные издания (журналы, книги);

в) научные статьи.

Оценщик не должен ограничивать свои исследования общедоступной информации вышеуказанными источниками, а должен исследовать любую другую важную доступную информацию.

Наряду с анализом предоставленных свидетельств оценщик будет использовать информацию в общедоступных источниках для последующих поисков. Когда оценщик определить интересующую область, оценщик должен исследовать общедоступную информацию, которая относится к этой интересующей области.

Доступность информации, легко доступной нарушителю помогает идентифицировать и способствует нападению, существенно действует, увеличивая потенциал нападения данного взломщика. Доступность информации об уязвимостях и изощренных средствах взлома в Интернете увеличивает вероятность того, что эта информация будет использована в попытках идентифицировать потенциальные уязвимости в ОО и использовать их. Современные средства поиска такой информации делают её легко доступной для оценщика и определение противодействия к опубликованным потенциальным уязвимостям и хорошо известным простым атакам может быть достигнута высокоэффективным способом.

Поиск общедоступной информации должен быть сфокусирован на ресурсах, которые занимаются продуктами, к типу которых относится ОО. Экстенсивность такого поиска должна определяться следующими факторами: тип ОО, опыт работы оценщика с ОО такого типа, вероятность потенциальных атак и уровень ADV по имеющимся свидетельствам.

Процесс идентификации повторяющийся, где идентификация одной потенциальной уязвимости может привести к идентификации другой интересующей области, которая требует дальнейшего исследования.

Оценщик должен указать, какие действия были проделаны, чтобы идентифицировать потенциальные уязвимости по свидетельствам. Однако при таком методе поиска оценщик, возможно, не сможет описать операцию по идентификации потенциальных уязвимостей перед началом исследования так как метод может быть выявлен в результате полученных данных во время поиска.

Оценщик укажет исследованные свидетельства по окончании поиска потенциальных уязвимостей. Данная выборка свидетельств может быть получена из источников определенных оценщиком связанных со свидетельствами, которые нарушитель, предполагается, может достичь или в соответствии с другими логическими обоснованиями, предоставленными оценщиком.

13.2.3.6 Действие AVA_VAN.3.3E

13.2.3.6.1 Операция AVA_VAN.3-4

Оценщик должен изучить ЗБ, руководства, функциональную спецификацию, проект ОО, описание структуры безопасности, чтобы идентифицировать потенциальные уязвимости в ОО.

Следует использовать методологию гипотез о недостатках, посредством которой анализируются спецификации, разработка и руководства, а после этого строятся гипотезы и предположения об уязвимостях в ОО.

Оценщик использует знание проекта и эксплуатации ОО полученные от поставленной ОО чтобы строить предположения о недостатках, чтобы идентифицировать потенциальные недостатки в разработке ОО и потенциальных ошибках в данных методах функционирования ОО.

Описание структуры безопасности предусматривает анализ разработчиком уязвимостей, вследствие чего в нем задокументировано как ФБО защищается от вмешательства недоверенных субъектов и предотвращает обход требований функции безопасности. Поэтому, оценщик должен опираться на понимание защиты ФБО полученных от анализа этих свидетельств и лишь, затем развивать их на знаниях полученных от анализа свидетельств других разработок ADV.

Данный метод, указанный областями интересов идентифицированных во время анализа свидетельств в ходе осуществлений действий по оценке и

гарантированный характерными образцам разработок и руководств, представленных для оценки определяется.

Руководство по выборке смотрите в Приложении А. Данное руководство должно быть изучено при выборе подмножества, обосновывая следующее:

а) подход, использованный в выборе;

б) пригодность свидетельства к такому методу

Область интересов может быть связана с достаточностью свойств специфической защиты детализированной в описании структуры безопасности.

Свидетельства, исследуемые в ходе оценки, могут быть связаны со свидетельствами, которыми нарушитель предполагается, будет обладать. Для примера, разработчик может защитить проект ОО и представления реализации, следовательно, информация, которая будет доступна нарушителю это лишь функциональная спецификация и руководства (общедоступные). Поэтому, несмотря на то, что объекты для доверия в ОО гарантируют, что проект ОО и представление реализации отвечают требованиям представления проекта и могут использоваться только для дальнейших исследований области интересов

С другой стороны, если источник общедоступен можно обоснованно полагать, что нарушитель имеет доступ к ресурсу и сможет использовать его для попытки нападения на ОО. Поэтому источник должен быть исследован специальным анализирующим методом.

Ниже приводятся образцы для выборки из подмножества анализируемых свидетельств:

а) для оценки, где все уровни абстракции проекта представлены от функциональной спецификации до представления реализации, анализ информации в функциональной спецификации и представления реализации могут быть выбраны как функциональная спецификация делающая детали интерфейса доступными для нарушителя, и представление реализации объединяющая решения проекта выполненных во всех других абстракциях проекта.

Поэтому, информация о проекте ОО будет исследована как часть реализации представления.

б) анализ отдельного подмножества информации в каждом представлении проекта предусматривает оценку.

в) покрытие отдельных ТФБ посредством каждого представления проекта предусматривает оценку.

г) анализ каждой из представлений проекта представленной на оценку, исследующих различные ТФБ внутри каждого представления проекта.

д) анализ аспектов свидетельств представленных на оценку связана с информацией о данных потенциальными уязвимостях полученных оценщиком (например, из системы оценок)

Этот метод идентификации потенциальной уязвимости это принять упорядоченный и планомерный подход к использованию системы для анализа

Оценщик описывает использованные методы в значении, какие свидетельства были исследованы, анализируемая информация внутри свидетельств, способ которым информация анализировалась, предположения которые сделаны.

Ниже приводятся примеры предположений, которые могли быть сделаны:

а) анализ деформированного входа для интерфейсов доступен нарушителю с внешнего интерфейса;

б) анализ ключа механизма безопасности ссылающегося на описание структуры безопасности, такие как разделение процесса, предполагается переполнение буфера, которое может повлечь ухудшение разделение;

в) поиск, направленный на идентификацию любого объекта в реализации представлении ОО полностью контролируется, а потом нет ФБО и могут быть использованы нарушителем, чтобы подорвать ТФБ.

Например, оценщик может идентифицировать, что интерфейсы являются слабой стороной ОО и определить метод поиска, по которому «спецификации всех интерфейсов представленные в функциональной спецификации и проекте ТОО будут рассмотрены на предположение потенциальных уязвимостей» и продолжать объяснять методы, используемые для предположений.

Процесс идентификации повторяющийся, где идентификация одной потенциальной уязвимости может привести к идентификации другой интересующей области, которая требует дальнейшего исследования.

Оценщик должен указать, какие действия были проделаны, чтобы идентифицировать потенциальные уязвимости в свидетельствах. Однако, при таком методе поиска оценщик, возможно, не сможет описать операции по идентификации потенциальных уязвимостей перед началом исследования, так как метод может быть выявлен в результате полученных во время поиска.

Оценщик укажет исследованные свидетельства по окончании поиска потенциальных уязвимостей.

Эта выборка свидетельств может исходить из тех областей интересов, которые идентифицировал оценщик, связанный со свидетельствами которые нарушитель предполагается, может достичь, или в соответствии с логическими обоснованиями, представленными оценщиком.

Исходя из конкретных угроз, присутствующих в предопределенной среде, оценщику при независимом анализе уязвимостей следует рассмотреть характерные уязвимости под каждой из следующих рубрик

а) уязвимости, характерные для конкретного типа оцениваемого ОО, которые могут быть указаны органом по подтверждению соответствия;

б) обход;
в) вмешательство;
г) прямые нападения;
д) наблюдение;
е) неправильное применение.

Пункты б) - е) объясняются более детально в Приложении В.

Описания структуры безопасности должны быть исследованы в отношении каждой из вышеуказанных характерных потенциальных уязвимостей. Каждая потенциальная уязвимость должна быть исследована на предмет наличия возможных путей, при которых обходятся защита ФБО и разрушаются ФБО

13.2.3.6.2 Операция AVA_VAN.3-5

Оценщик должен указать в ТОО идентифицированные потенциальные уязвимости, которые являются кандидатами на тестирование и применимы к ОО в его предопределенной среде.

Возможно, будет установлено, что нет необходимости в дальнейшем исследовании потенциальных уязвимостей, если оценщик идентифицирует что меры в предопределенной среде, ни ИТ ни не-ИТ среде предотвращают использование уязвимости в предопределенной среде. Например, ограничивая физический доступ к ОО только уполномоченными пользователями, можно фактически сделать уязвимость ОО к вмешательству непригодной для использования

Если оценщик что потенциальная уязвимость не применима в предопределенной среде, то указывает все причины для отказа от исследования потенциальной уязвимости.

В остальных случаях, оценщик указывает потенциальные уязвимости для дальнейших исследований.

Список потенциальных уязвимостей пригодных к ОО в его предопределенной среде, и которые могут быть использованы для выполнения тестов проникновения, должны быть указаны в ТОО оценщиком.

13.2.3.7 Действие AVA_VAN.3.4E

13.2.3.7.1 Операция AVA_VAN.3-6

Оценщик должен разработать тесты проникновения, основанные на независимом поиске потенциальных уязвимостей.

Оценщик должен достаточно подготовиться к тестированию проникновения, чтобы определить восприимчивость ОО в его преопределенной среде к потенциальным уязвимостям, идентифицированным в ходе поиска в источниках общедоступной информации. Любая текущая информация, предоставленная оценщику третьей стороной (например, органом по сертификации) относящаяся к известным потенциальным уязвимостям должна быть исследована

оценщиком наряду, с любой потенциальной уязвимостью выявленной в ходе выполнения других действий по оценке.

Оценщик извещается, что для анализа описаний структуры безопасности в поиске уязвимостей (как детализировано в AVA_VAN.3-4), тестирование должно производиться с подтверждение свойств структуры. Если требования из ATE_DPT включены в ТФБ, разработчик, тестирующий свидетельства включит тестирование, подтверждающее соответствующие представления всех специальных устройств детализированных в описании структуры безопасности. Однако тесты разработчика не обязательно должны включать в себя тестирование всех аспектов описании структур, которые защищают ФБО, столько же такое тестирование будет отрицательным, в сущности, пытаться опровергнуть свойства. В разработке стратегии тестирования проникновения, оценщик должен убедиться, что все аспекты описания структуры безопасности протестированы, как тестирование функциональности (как исследовано в 13) так и тестирование проникновения оценщиком.

Вероятно, будет целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной уязвимости.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

Руководство по определению необходимого потенциала нападения необходимого чтобы использовать потенциальную уязвимость находится в Приложении В.

Уязвимости, предполагаемые как пригодные для использования только нарушителями, обладающими умеренным или высоким потенциалом нападения, не приводят к отрицательному заключению по этому действию оценщика. Когда материалы анализа подтверждают данную гипотезу, то соответствующие уязвимости в дальнейшем не рассматриваются в качестве исходных данных для тестирования проникновения. Однако такие уязвимости приводятся в ТОО в качестве остаточных уязвимостей.

Уязвимости, предполагаемые как потенциально пригодные для использования нарушителем, обладающим низким потенциалом нападения, и приводящие к нарушению целей безопасности, следует отнести к самым

высокоприоритетным потенциальным уязвимостям, содержащимся в перечне, используемом для руководства тестированием проникновения в ОО.

13.2.3.7.2 Операция AVA_VAN.3-7

Оценщик должен разработать тестовую документацию для тестов проникновения, основанных на списке потенциальных уязвимостей детализация, которой достаточна, чтобы обеспечить воспроизводимость тестов.

Тестовая документация должна включать

а) идентификацию тестируемой уязвимости ОО;

б) инструкции по подключению и установке всего требуемого тестового оборудования, как требуется для проведения теста проникновения;

в) инструкции по установке всех предварительных начальных условий выполнения теста проникновения;

г) инструкции по инициированию ФБО;

д) инструкции по наблюдению режима выполнения ФБО;

е) описание всех ожидаемых результатов и необходимого анализа, который выполняется по отношению к наблюдаемому режиму выполнения ФБО для сравнения с ожидаемыми результатами;

ж) инструкции по завершению тестирования и установке необходимого после тестового состояния ОО.

Оценщик готовится к тестированию проникновения, основанным на списке потенциальных уязвимостей идентифицированных в ходе поисков в общедоступных источниках.

Не предполагается определение оценщиком пригодности использования уязвимостей помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в результате исследований в ходе оценки оценщик может обнаружить уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения. Такие уязвимости приводятся в ТОО как остаточные уязвимости

Поняв предполагаемую уязвимость, оценщик определяет наиболее подходящий способ протестировать восприимчивость ОО. В частности оценщик рассматривает:

а) интерфейсы ИФБО или другого ОО, которые будут использоваться для инициирования выполнения ФБО и наблюдения их реакции; (Возможно, что оценщику потребуется интерфейс к ОО другой не ОФБ, чтобы продемонстрировать свойства ОФБ описанные в описаниях структуры безопасности (как того требует ADV_ARC). Это должно быть учтено, хотя, данные интерфейсы ОО предполагают способы тестирования свойств ФБО, они не являются объектами тестирования;

б) начальные условия, которые будут необходимы для выполнения теста (т.е., какие-либо конкретные объекты или субъекты, которые будут необходимы, и атрибуты безопасности, которые им необходимо будет иметь;

в) специальное оборудование для тестирования, которое потребуется либо для инициирования ИФБО, либо для наблюдения за ИФБО (хотя маловероятно, что специальное оборудование потребовалось бы для использования явной уязвимости);

г) замена физического тестирования теоретическим анализом особенно существенна, когда результаты первоначально анализа могут быть экстраполированы чтобы продемонстрировать что повторяющиеся попытки атак, вероятно, будут иметь успех после определенного числа попыток.

Оценщик, вероятно, посчитает целесообразным выполнить тестирование проникновения, используя ряд наборов тестов, где каждый набор тестов будет использоваться для тестирования конкретной явной уязвимости.

Цель определения данного уровня детализации в тестовой документации – дать возможность другому оценщику повторить тесты и получить эквивалентный результат.

13.2.3.7.3 Операция AVA_VAN.3-8

Оценщик должен провести тестирование проникновения

Оценщик использует документацию для тестов проникновения, разработанную на операции AVA_VAN.3-6 как основу для выполнения тестов проникновения по отношению к ОО, но это не препятствует оценщику выполнить дополнительные специальные тесты проникновения. Если потребуется, оценщик может придумать специальные тесты в результате изучения информации в процессе тестирования проникновения, которые, если выполнялись оценщиком, заносятся в документацию для тестов проникновения. Такие тесты могут потребоваться, чтобы разобраться с непредвиденными результатами или наблюдениями или исследовать потенциальные уязвимости, существование которых предположил оценщик во время предварительно запланированного тестирования.

Если тест проникновения показал, что предполагавшейся потенциальной уязвимости не существует, оценщик должен определить был ли собственный анализ оценщика неправильным, или подготовленная оценка неверная или недостаточная.

Не предполагается тестирования оценщиком на предмет наличия уязвимостей (в том числе известных из общедоступных источников), помимо тех, для которых требуется низкий потенциал, чтобы осуществить нападение. Однако в некоторых случаях необходимо будет выполнить тест прежде, чем требуемый потенциал нападения может быть определен. Когда в результате исследований в ходе оценки оценщик обнаруживает потенциальную уязвимость, которая является пригодной для использования только нарушителем с большим, чем низкий, потенциалом нападения, она приводится в ТОО как остаточная уязвимость

13.2.3.7.4 Операция AVA_VAN.3-9

Оценщик должен зафиксировать фактические результаты тестов проникновения.

Хотя некоторые специфические детали фактических результатов выполнения тестов могут отличаться от ожидаемых (например, поля времени и даты в записи аудита), общий результат должен быть идентичным. Любые неожиданные результаты тестирования должны быть исследованы. Влияние на оценку должны быть установлены и обоснованы.

13.2.3.7.5 Операция AVA_VAN.3-10

Оценщик должен привести в ТОО информацию об усилиях оценщика по тестированию проникновения, вкратце изложив подход к тестированию, тестируемую конфигурацию, глубину и результаты тестирования.

Информация о тестировании проникновения, приводимая в ТОО, позволяет оценщику передать общий подход к тестированию проникновения и усилия, затраченные на этот подвид деятельности. Цель предоставления этой информации состоит в том, чтобы дать краткий содержательный обзор усилий оценщика по тестированию проникновения. Это не означает, что информация в ТОО относительно тестирования проникновения является точным воспроизведением конкретных операций тестирования или результатов отдельных тестов проникновения. Целью является предоставить достаточные подробности, чтобы позволить другим оценщикам и сотрудникам органа по подтверждению соответствия получить некоторое понимание выбранного подхода к тестированию проникновения, объема выполненного тестирования проникновения, тестируемых конфигураций ОО и общих результатов действий по тестированию проникновения

Информация об усилиях оценщика по тестированию проникновения, которую обычно можно найти в соответствующем разделе ТОО, включает:

а) тестируемые конфигурации ОО. Конкретные конфигурации ОО, которые подвергались тестированию проникновения;

б) ИФБО подвергшиеся тестированию проникновения. Краткий перечень ИФБО, и других интерфейсов ОО, на которых было сосредоточено тестирование проникновения;

в) вердикт по данному подвиду деятельности. Общее решение по результатам тестирования проникновения.

Данный перечень ни в коем случае не является исчерпывающим и предназначен только для того, чтобы дать некоторое представление о типе информации, касающейся тестирования проникновения, выполненного оценщиком в процессе оценки, которую следует представить в ТОО.

13.2.3.7.6 Операция AVA_VAN.3-11

Оценщик должен проанализировать результаты всех тестов проникновения и определить имеет ли ОО в своей преопределенной среде уязвимости пригодные нарушителю, обладающему низким потенциалом

нападения. Если результаты показывают, что ОО, находящийся в своей предопределенной среде, имеет уязвимости, пригодные для использования нарушителем, обладающим меньшим, чем умеренный, потенциалом нападения, то по данному действию оценщиком делается отрицательное заключение.

Чтобы определить потенциал атаки необходимый для использования конкретной уязвимости и может ли она вследствие этого использоваться в заданной среде, должен использоваться Пункт В.4 Приложения В. Нет необходимости вычислять потенциал атаки каждый раз, за исключением случаев, когда существуют сомнения, может ли или нет уязвимость использована нарушителем, обладающим потенциалом меньший, чем умеренный

13.2.3.7.7 Операция AVA_VAN.3-12

Оценщик должен привести в ТОО информацию обо всех пригодных для использования уязвимостях и остаточных уязвимостях, детализируя для каждой:

а) ее источник (например, стала известна при выполнении действий по оценке, известна оценщику, прочитана в публикации);

б) не отвечает ТФБ;

в) описание;

г) пригодна ли она для использования в предопределенной среде или нет (т.е., пригодная ли для использования или является остаточной уязвимостью);

д) количество времени, уровень анализа, уровень знаний ОО, уровень возможности и оборудование необходимое для выполнения идентификации уязвимости, и соответствующие значения, используя Таблицу В.2 и В.3 Приложения В.

13.2.4 Оценка подвида деятельности (AVA_VAN.4)

13.2.4.1 Цели

Цель этого подвида деятельности определить имеет ли ОО в своей преопределенной среде уязвимости пригодные нарушителю, обладающему умеренным потенциалом нападения

13.2.4.2 Исходные данные

а) ЗБ;

б) функциональная спецификация;

в) проект ОО;

г) описание структуры безопасности

д) реализация выбранного подмножества;

е) руководства;

ж) ОО, пригодный для тестирования;

и) общедоступная информация, обеспечивающая идентификацию потенциальных уязвимостей.

Оставшиеся подразумевающиеся свидетельства оценки для этого подвида деятельности зависят от компонентов, которые включены в пакет доверия. Свидетельства, обеспечивающие каждый компонент, используются, как исходные в данном подвиде деятельности.

Дополнительным исходным материалом для данного подвида деятельности является текущая информация касательно явных уязвимостей (например, от органа по подтверждению соответствия).

13.2.4.3 Замечания по применению

Метод систематического анализа принимает форму структурированного анализа свидетельств. Этот метод требует от оценщика точно описать структуру и форму проводимого анализа (то есть способ, которым анализ проводиться заранее предопределен, в отличие от специализированного анализа). Метод устанавливается с помощью данных, которые будут анализироваться и как/зачем они будут анализироваться. Следующие руководства систематического анализа описаны в Приложении В.

13.2.4.4 Действие AVA_VAN.4.1E

ОО должен быть пригоден для тестирования.

13.2.4.4.1 Операция AVA_VAN.4-1

Оценщик должен исследовать ОО, чтобы сделать заключение, согласуется ли тестируемая конфигурация с оцениваемой конфигурацией, определенной в ЗБ.

ОО, упомянутый в плане тестирования разработчика, должен иметь ту же самую уникальную маркировку, которая установлена возможностями УК подвидами деятельности (ALC_CMC) и идентифицирована во вводной части ЗБ.

В ЗБ может быть определено несколько подлежащих оценке конфигураций. ОО может состоять из ряда различных аппаратных и программных реализаций, которые подлежат тестированию на соответствие ЗБ.

Оценщик верифицирует, что все тестируемые конфигурации согласованы с ЗБ. Оценщику следует рассмотреть описанные в ЗБ требования безопасности к рабочей среде, которые могут быть применимы к среде тестирования и убедиться, что они соответствуют тестовому окружению. Могут существовать требования к тестовой среде, которые неприменимы к тестовой среде. Например, предположение относительно допусков пользователей может не касаться среды тестирования, однако, предположение относительно единой точки подключения к сети, как правило, касается среды тестирования

При использовании, каких бы то ни было средств тестирования (например, измерителей, анализаторов) обеспечить правильную калибровку этих средств будет обязанностью оценщика

13.2.4.4.2 Операция AVA_VAN.4-2

Оценщик должен исследовать ОО, чтобы сделать заключение, правильно ли он установлен и находится ли в состоянии, которое известно

Оценщик имеет возможность сделать заключение о состоянии ОО несколькими способами.

Например, предшествующее успешное завершение подвида деятельности (AGD_PRE.1) позволит считать выполненной данную операцию, если оценщик все еще уверен, что тестируемый ОО был должным образом установлен и находится в известном состоянии. Если это не так, то оценщику рекомендуется следовать процедурам разработчика, чтобы установить, сгенерировать и запустить ОО, используя только поставляемое руководство.

Если оценщику приходится выполнить процедуры установки вследствие того, что ОО находится в неизвестном состоянии, то при успешном завершении данная операция могла бы удовлетворить операцию AGD_PRE.1-3..

13.2.4.5 Действие AVA_VAN.4.2E

13.2.4.5.1 Операция AVA_VAN.4-3

Оценщик должен исследовать источники общедоступной информации, чтобы идентифицировать потенциальные уязвимости в ОО.

Оценщик должен исследовать общедоступную информацию, чтобы обеспечить идентификацию возможных потенциальных уязвимостей в ОО.

Существует много источников общедоступной информации, которые оценщик должен исследовать, используя такие как, например доступные во всемирной паутине, включая:

а) специализированные издания (журналы, книги);

б) научные статьи.

в) протоколы конференций.

Оценщик не должен ограничивать свои исследования общедоступной информации вышеуказанными источниками, а должен исследовать любую другую важную доступную информацию.

Наряду с анализом предоставленных свидетельств оценщик будет использовать информацию в общедоступных источниках для последующих поисков. Когда оценщик определить интересующую область, оценщик должен исследовать общедоступную информацию, которая относится к этой интересующей области.

Доступность информации, легко доступной нарушителю помогает идентифицировать и способствует нападению, существенно действует, увеличивая потенциал нападения данного взломщика. Доступность информации об уязвимостях и изощренных средствах взлома в Интернете увеличивает вероятность того, что эта информация будет использована в

попытках идентифицировать потенциальные уязвимости в ОО и использовать их.

Современные средства поиска такой информации делают её легко доступной для оценщика и определение противодействия к опубликованным потенциальным уязвимостям и хорошо известным простым атакам может быть достигнута высокоэффективным способом.

Поиск общедоступной информации должен быть сфокусирован на ресурсах, которые занимаются продуктами, к типу которых относится ОО. Экстенсивность такого поиска должна определяться следующими факторами: тип ОО, опыт работы оценщика с ОО такого типа, вероятность потенциальных атак и уровень ADV по имеющимся свидетельствам.

Процесс идентификации повторяющийся, где идентификация одной потенциальной уязвимости

может привести к идентификации другой интересующей области, которая требует дальнейшего исследования.

Оценщик должен описать метод, используемый для идентификации потенциальной уязвимости в общедоступных местах, детализируя выполненный поиск. Это может быть подсказано такими факторами как область интересов идентифицированных оценщиком, связанных со свидетельствами, которыми нарушитель, предполагается, будет обладать.

Однако известно, что при этом виде поиска метод может в последующем развиваться в результате полученных данных в ходе поиска. Вследствие, оценщик также укажет все действия, предпринятые вдобавок к этим описанным в методе дальнейшее исследования вопроса, которые, считается, приведет к потенциальным уязвимостям, и укажет исследованные свидетельства по окончании поиска потенциальных уязвимостей.

13.2.4.6 Действие AVA_VAN.4.3E

13.2.4.6.1 Операция AVA_VAN.4-4

Методологический анализ ЗБ, документация указания, функциональная спецификация, проект ОО, описание структуры безопасности и реализация работы должны вестись оценщиком для распознания возможных потенциальных уязвимостей в ОО.

Общее указания по систематичному анализу уязвимости представлено в Приложении Б.

Данный метод распознания потенциальной уязвимости должен быть упорядочен и спланирован. Такая система применяется на осмотрах. Оценщик описывает метод, используемый в условиях данного характера, в котором учитывается данная информация и создается гипотеза.

Оценщику стоит использовать методологию гипотезы недостатка посредством ЗБ, анализировать свидетельство разработки (функциональная спецификация, проект ОО и реализация работы) и общего указания, а затем построить гипотезу об уязвимости в ОО или просто поразмышлять.

Он использует успехи проекта и работы ОО, полученные от поставки ОО для ведения гипотезы недостатка и распознания потенциальных дефектов разработки ОО и потенциальных ошибок в конкретном методе эксплуатации ОО.

Описание структуры безопасности дает разработчику анализ уязвимости, так как он информирует о том, как ФБО предохраняется от помех опасных объектов и предотвращает упущение функциональность безопасного принуждения. Поэтому оценщик основывается на защиту ФБО, полученную при анализе свидетельства, а затем разрабатывает это на опыте других разработок свидетельств ADV.

Метод, используемый в методологическом исследовании уязвимости, учитывает все сферы, распознанные в результате оценки разработки оценщика и общих указаний свидетельств. Тем не менее, оценщиком также должен учитываться каждый аспект анализа структуры безопасности для нахождения моментов, где защита ФБО может быть подорвана. Конструкция методологического анализа может быть полезна на основе материалов описания структуры безопасности, что позволит представить интересы соответствующих ADV свидетельств. Анализ может разрабатываться дальше, при гарантии, что всё другие материалы ADV свидетельства будут учитываться.

При осмотре свидетельства могут быть построены следующие гипотезы:

а) рассмотрение деформированного выхода на функции безопасности, доступные для нападающего во внешних функциях безопасности;

б) осмотр ключевого механизма безопасности привлеченного в описание структуры безопасности, такие как разделение процесса, построение гипотезы по избытку внутреннего резерва, которое может привести к снижению качества разделения;

в) распознание объектов в реализации работ ОО, которые не полностью под контролем, и может быть использованы нападающими для подрыва механизма безопасности ТФБ.

К примеру, оценщик распознает, что функции безопасности являются сферой потенциальной уязвимости ОО и определит метод для поиска, в котором изучаются все детали функции безопасности свидетельства, создаст гипотезу по потенциальной уязвимости и объяснит методы используемые в ней.

В дополнении, оценщик установил сферы интереса в течение осмотра свидетельства при ведении оценочной деятельности. Сферы интереса могут быть также обнаружены при исполнении других операций совместно с данным компонентом, в частности AVA_VAN.4-7, AVA_VAN.4-5 и AVA_VAN.4-6, где разработка и исполнение тестов на проникновение определяют дальнейшие сферы интереса исследований или потенциальную уязвимость.

Однако при данных строгих мерах не разрешен осмотр подмножества свидетельств разработки и общих указаний или их содержимого. Метод описания доказывает завершенность данного методологического подхода, и гарантирует, что в методе учитывается вся информация, предоставленная в тех поставках.

Данный метод распознания потенциальной уязвимости должен быть упорядочен и спланирован; применять систему при осмотре. Оценщик должен описать метод, который используется в условиях рассмотрения свидетельства, характера учитываемой информации и создаваемой гипотезы. Данный метод должен быть согласован с руководством оценочных работ, руководство также может предоставить детали любых дополнительные методов для анализа уязвимости и дополнительную информацию на рассмотрение оценщика. Хотя система распознания потенциальной уязвимости предопределена, идентификационный процесс может оставаться многократным, то есть идентификация потенциальной уязвимости может привести к другой сфере, которая в свою очередь потребует дальнейших исследований.

При условии ТФБ, ОО применяется в операционной среде, где независимый анализ уязвимости оценщика должен учитывать характерную потенциальную уязвимость соответственно каждому следующему заголовку:

а) характерная потенциальная уязвимость релевантная для оцененного типа ОО, также может замененная оценочным руководством;

б) упущение;

в) фальсификация;

г) прямые атаки;

д) мониторинг;

е) злоупотребление.

Пункты б-е детально разъясняются в приложении Б.

Описание структуры безопасности следует учитывать по выше указанным пунктам характерных потенциальных уязвимостей. Каждая потенциальная уязвимость должна рассматриваться для поиска возможных путей отмены защиты ФБО и ФБО подрыва.

13.2.4.6.2 Операция AVA_VAN.4-5

Оценщик должен вести запись опознанных потенциальных уязвимостей в ТОО, которые претендуют на тест и применяются в операционной среде ОО.

Может быть установлено, что дальнейшее рассмотрение потенциальной уязвимости больше не потребуется, если, к примеру, оценщик обнаружит эти меры в операционной среде, или предыдущая эксплуатация, ИТ или не ИТ использование потенциальной уязвимости в той же операционной среде. Например, ограничение физического доступа уполномоченных пользователей к ОО может только показать на потенциальную уязвимость.

Если оценщик решит, что потенциальная уязвимость не применима больше в операционной среде, то он составляет список причин исключения потенциальной уязвимости из дальнейшего рассмотрения.

В противном случае рассматривает.

Перечень потенциальных уязвимостей ОО, используемые для ввода в деятельность теста проникновения, должен быть предоставлен оценщиками в ТОО.

13.2.4.7 Действие AVA_VAN.4.4E

13.2.4.7.1 Операция AVA_VAN.4-6

Оценщик должен разработать тест на пенетрацию, основанный на независимом поиске уязвимости.

При подготовке теста оценщику необходимо определить восприимчивость ОО в операционной среде на опознанную среди общедоступной информации потенциальную уязвимость. Любая текущая информация, полученная от третьего лица (например, Оценочное руководство), вместе с любой другой информацией деятельности оценки должна учитываться оценщиком.

Оценщик знает, что, учитывая описание структуры безопасности (как изложено в AVA_VAN.4-3), тест должен подтверждать свойства структуры. Если требования ATE_DPT включены в ТАБ,то свидетельство теста разработчика будет содержать тест, подтверждающий корректную эксплуатацию любого конкретного механизма, описываемого в структуре безопасности. Однако, наличие теста на все аспекты свойств структуры не обязательно, так как большое количество данных тестов по своей сущности являются негативными, опровергающими все свойства. Работая над стратегией теста на пенетрацию, оценщик гарантирует проверку всех аспектов описания структуры безопасности, либо на функциональном тесте, либо на тесте на пенетрацию.

Оценщику удобно будет провести тест на пенетрацию, используя серию контрольных примеров, где каждый контрольный пример проверит на конкретную потенциальную уязвимость.

Оценщику не обязательно тестировать (включая те, что в общественном домене) на потенциальную уязвимость, не указанные в Среднем потенциале атаки. В некоторых случаях необходимо провести тест перед эксплуатацией. Где в результате оценочной экспертизы оценщик находит наличие уязвимости, что вне Среднего потенциала атаки, а в ТОО это сообщается как остаток элемента уязвимости.

В приложении Б.4 можете найти указания по определению необходимой возможной атаки для использования потенциальной уязвимости.

Потенциальная уязвимость, по гипотезе используемая нападающим, обладающая Средним потенциалом атаки и отображаясь на нарушении

целей, должна быть самой преимущественной, включая в себя перечень, направленный против ОО.

13.2.4.7.2 Операция AVA_VAN.4-7.

Оценщик должен предоставить документацию теста на пенетрацию для многократности других тестов, основанных на детально изложенного списка потенциальных уязвимостей. Документация теста должна включать следующее:

а) идентификационный лист на потенциальную уязвимость, ради которого проверяется ОО;

б) инструкция по соединению и установке всего оборудования необходимого для проведения теста на пенетрацию;

в) инструкция по определению всех первоначальных условий;

г) инструкция по усилению деятельности ФБО;

д) инструкция по наблюдению деятельности ФБО;

е) описание ожидаемого результата и необходимого анализа, их сравнение друг с другом;

ж) инструкция по заключению теста и определению необходимого положения ОО после проверки.

Оценщик готовит тест на пенетрацию на основе списка потенциальной уязвимости, опознанного при поиске общественного домена и свидетельства оценки.

Маловероятно, что оценщик определит функцию эксплуатации потенциальной уязвимости помимо тех, на которых необходимо влиять Среднему потенциалу атаки. Однако, в результате экспертизы оценки, оценщик может обнаружить эксплуатацию потенциальной уязвимости нападающим значительнее, чем Средний потенциал атаки. О таких уязвимостях должны сообщать в ТОО как об остаточных уязвимостях.

Наряду с потенциальной уязвимостью, оценщик определяет наиболее возможные пути проверки ОО на восприимчивость.

В особенности оценщик учитывает:

а) функции безопасности ФБОІ или ОО, используемые для стимуляции работы ФБО и наблюдения реакций (Возможно использование функций безопасности ОО чем ФБОІ для демонстрации свойств ФБО (как указано в ADV_ARC). Нужно отметить, что функции безопасности ОО определяют средство проверки свойств ФБО, и не являются главной целью теста);

б) первоначальные условия, необходимые для проведения теста (конкретные объекты или субъекты, атрибуты безопасности);

в) специальное тестовое оборудование как для стимуляции работы ФБОІ, так и для наблюдений за ФБОІ;

г) могут ли теоретические анализы заменить практические проверки, в частности важно, где экстраполированными могут быть результаты начального теста для демонстрации многочисленных попыток.

Для оценщика будет наиболее практично проведение теста на пенетрацию, используя серию контрольных примеров, каждый пример будет предназначен для конкретной потенциальной уязвимости.

Целью данной степени детализации в документации является помощь в проведении подобных тестов и получении эквивалентных результатов.

13.2.4.7.3 Операция AVA_VAN.4-8

Оценщик должен провести тест на пенетрацию.

Для выполнения теста на пенетрацию оценщик использует за основу документацию, полученную в результате операции AVA_VAN.4-6, но даже это не мешает ему выполнить дополнительный специальный тест. В случае необходимости, оценщик в результате информации изученной во время теста на пенетрацию разрабатывает специальные тесты, и если требуется, записывает всё в документации теста на пенетрацию. Такого рода тесты могут быть необходимы при получении неожиданных результатов или наблюдениях, или для исследования потенциальной уязвимости, предложенной оценщику во время планирования тестов.

Если тест на пенетрацию не обнаружит существование потенциальной уязвимости, оценщику следует определить, были ли его собственные анализы верны, или были ли поставки оценок некорректны или незавершенны.

Маловероятно, что оценщик определит функцию эксплуатации потенциальной уязвимости помимо тех, что указаны в Модераторе потенциальной атаки. Однако, в результате экспертизы оценщик может обнаружить функцию эксплуатации потенциальной уязвимости только нападающего значительнее чем Модератор потенциальной атаки. Такая уязвимость считается в ТОО как остаточная.

13.2.4.7.4 Операция AVA_VAN.4-9

Оценщик должен вести запись фактических результатов тестов на пенетрацию. Несмотря на то, что определенные детали фактических результатов могут отличаться от ожидаемых (например, время и дата проверки), итоговый результат должен быть идентичным. Любой неожиданный результат должен быть изучен. Влияние на оценку должно быть зафиксированным и обоснованным.

13.2.4.7.5 Операция AVA_VAN.4-10

В отчете оценщик должен информировать ТОО о результатах работ теста на пенетрацию, подчеркивая метод теста, конфигурацию, глубину и результаты.

Данная информация позволит оценщику передать весь метод теста на пенетрацию и результат работы в данном подвиде деятельности. Целью этой информации является показание значимого результата работы оценщика, а вовсе не репродукция работ или результатов конкретного теста индивидуального теста проникновения. Замысел был в обеспечении

достаточно подробной информации, которая позволит другим оценщикам и оценочным руководствам понять выбранный метод теста на пенетрацию, количество выполненных тестов, конфигурацию теста ОО, и полный результат по деятельности теста. Информация в разделе ТОО, благодаря результатам работ теста оценщика, будет следующей:

а) конфигурация теста ОО. Конкретные конфигурации ОО, проверенные тестом проникновения;

б) проверенный на пенетрацию ФБОI. Короткий перечень функций безопасности ФБОI и ОО, сфокусированные на тесте проникновения;

в) Заключение для подвид деятельности. Итоговое решение и результаты теста на пенетрацию.

Данный перечень полон и нацелен лишь на обеспечение конкретного контекста информации, которая должна быть представлена в ТОО касательно теста на пенетрацию во время оценки.

13.2.4.7.6 Операция AVA_VAN.4-11

Оценщику следует осмотреть все результаты теста на пенетрацию, чтобы определить устойчивость ОО в своей операционной среде на попытку Среднего потенциала атаки. Если результаты обнаружат используемые уязвимости попытки Невысокого потенциала атаки в операционной среде ОО, то все действия оценщика не будут иметь успеха. Указание в Б.4 помогут определить потенциальную атаку, требуемую для использования конкретной уязвимости, а также ее способность эксплуатации в нужной среде. Нет необходимости вычислять потенциал атаки в каждом примере, за исключением сомнения используемости уязвимости в попытке Невысокого потенциала атаки.

13.2.4.7.7 Операция AVA_VAN.4-12

Оценщик должен сообщать в ТОО о всех используемых и остаточных уязвимостей, указывая подробности о следующем:

а) источник (например, деятельность методологии оценки была известна оценщику, прочитана в публикации);

б) несоответствие ТФБ(s);

в) описание;

г) используемость в операционной среде;

д) количество времени, уровень экспертизы, уровень познаний об ОО, уровень возможности и оборудования для распознания уязвимости, а также соответствующая важность использования таблиц Б.2 и Б.3 Приложения Б.

13.2.5 Оценка подвида деятельности AVA_VAN.5

Не имеются общие указания; схема для указаний данной подвид деятельности должна быть обсуждена.

14 Класс АСО: Структура

14.1 Введение

Цель данной деятельности является определение интеграции компонентов в методе безопасности, как определено в ЗБ для ОО. Это можно достичь посредством осмотра и теста функций безопасности между компонентами, обеспеченных проектом компонентов и проведения анализа на уязвимость.

14.2 Заметки к применению

Совокупность Устойчивости зависимых компонентов (ACO_REL) распознает, где зависимый компонент наиболее устойчив для обеспечения своей безопасности в своей операционной среде (выполняемый базовым компонентом в оценке ОО). Данная устойчивость распознается в условиях предоставления базовым компонентом функции безопасности. Свидетельство разработки (ACO_DEV) определяет, какую функцию безопасности базового компонента учитывают при оценке базового компонента.

Отмечено, что Устойчивость зависимых компонентов (ACO_REL) не охватывает другое свидетельство необходимое для направления проблемы технической интеграции составных компонентов (например, описание функций безопасности не ФБО элементов операционной системы, правила интеграции, т.д.). Это вопрос функциональной структуры за пределами назначения безопасности.

В виде одной части Составного теста ОО (ACO_CTT), оценщик выполнит проверку составного ОО на уровне функций безопасности ОО и базового компонента для подтверждения их соответствующей работы. Выбранное подмножество будет учитывать возможные влияния изменений конфигурации (использования) базового компонента, использованного в ОО.

Разработчик предоставит свидетельство проверки на каждую функцию безопасности базового компонента (требования зоны охвата согласованы с требованиями оценки базового компонента).

Обоснование структуры (ACO_COR) требует от оценщика определить, соответствующие ли меры гарантии применялись в базовом компоненте, и использовался ли базовый компонент в своей оценочной конфигурации. Это включает в себя определения, вся ли функциональность безопасности охвачена в базовом компоненте ФБО. Требования обоснования структуры (ACO_COR) могут встречаться в свидетельстве демонстрации каждого подтвержденного компонента.

Данное свидетельство может быть в виде цели безопасности и общественного протокола компонента оценки (например, сертификационный протокол).

С другой стороны, если, один из вышеперечисленных компонентов не подтвердиться, то может появиться сомнение по поводу подлинности свидетельства, полученного при первоначальной оценке. Или же будет проведена дополнительная оценка неохваченных ранее аспектов базового компонента.

Данная информация будет внесена в Свидетельство оценки (ACO_DEV).

К примеру, это может быть случаем указанным в Взаимодействии между объектами (смотреть Приложение Б.3, Взаимодействие между составными объектами ИТ в ИСО/МЭК 15408-3), где зависимый компонент запрашивает функциональности безопасности базового компонента в ОО больше чем включено в оценку базового компонента. Это будет определено в течение применения совокупностей Устойчивости зависимых компонентов (ACO_REL) и Свидетельства разработки (ACO_DEV). В таком случае свидетельство для Обоснования структуры (ACO_COR) будет демонстрировать подлинность оценки базового компонента. Этого можно будет достичь посредством средств, включающих в себя:

а) выполнение повторной оценки базового компонента, сфокусированной на свидетельстве продленной части ФБО;

б) демонстрацию того, что продленная часть ФБО не влияет на другие части ФБО, а также предоставление свидетельства необходимой функциональности безопасности ФБО.

14.3 Рациональное построение (ACO_COR)

14.3.1 Оценка подвида деятельности (ACO_COR.1)

14.3.1.1 Ввод

Оценочными данными для этой функциональной подгруппы являются:

а) составное ЗБ;

б) рациональное построение;

в) информация доверия;

г) информация разработки;

д) уникальный идентификатор.

14.3.1.2 Действие ACO_COR.1.1E

Рациональное построение демонстрирует, что уровень доверия, в меньшей степени, столь выше, сколько зависимый компонент, приобретенный в поддержку функциональных возможностей основного компонента, в свою очередь, последний сформирован как необходимая поддержка ФБО зависимого компонента.

14.3.1.2.1 Операция ACO_COR.1-1

Оценщик рассмотрит анализ соответствия между информацией разработки и информацией доверия, чтобы определить на какие интерфейсы (области соединения), которые не детализированы в информации разработки, полагается зависимый компонент.

В этой операции оценщик имеет следующие цели:

а) установить какие интерфейсы, на которые полагается зависимый компонент, применяют подходящую меру доверия;

б) определить пакет доверия, примененный к основному компоненту, в то время как оценка основного компонента содержит те же требования доверия, что и в пакете, примененным зависимым компонентом во время его оценки, или требования доверия, стоящие иерархически выше.

Оценщик может использовать соответствие, обнаруженное в информации разработки, совершенствованное во время проявления данных разработки (ACO_DEV) (например, ACO_DEV.1-2, ACO_DEV.2-4, ACO_DEV.3-6), чтобы помочь определить интерфейсы, идентифицированные в информации доверия и не рассматривающиеся в информации разработки.

Оценщик запишет усиление интерфейсов ИОС (интенсивность отказов системы), описанных в информации доверия, но не содержащиеся в информации разработки. Это обеспечит ввод в операцию ACO_COR.1-3, помогая определить порцию основного компонента, в котором требуется дальнейшее доверие.

Если и основной, и зависимый компоненты были оценены напротив одного и того же пакета доверия, то уровень доверия в порциях внутри оценки основного компонента, в меньшей степени, столь выше, сколько обычный зависимый компонент. Если, однако, пакеты доверия, примененные к компонентам во время оценки компонентов, различаются, то оценщику необходимо определить, что требования доверия, примененные к основному компоненту, иерархически выше требований доверия, примененных к зависимому компоненту.

14.3.1.2.2 Операция ACO_COR.1-2

Оценщик рассмотрит рациональное построение, чтобы определить обсуждение интерфейсов, включенных в основной компонент, и на которые полагается зависимый ФБО, во время оценки основного компонента.

Задание по безопасности, отчет компонента общественной оценки (например, отчет о свидетельстве) и документы по руководству основного компонента, все они обеспечивают информацией в пределах границ основного компонента. ЗБ обеспечивает деталями логической области и границ составного Объекта оценки, позволяющего оценщику определить, относится ли интерфейс к порции продукта в пределах области оценки. Документы по руководству обеспечивают деталями использования всех интерфейсов составного ОО. Также документы по руководству могут включать детали интерфейсов в продукте, находящиеся и вне области оценки, любой такой интерфейс должен быть опознаваем, либо через наблюдение информации в ЗБ, либо через порцию управления, связанную с оценочной конфигурацией. Отчет общественной оценки может обеспечить

любые дополнительные ограничения на использование составного ОО, что является также необходимым атрибутом.

Поэтому комбинация этих вводов позволяет оценщику определить, имеет ли интерфейс, описанный в рациональном построении, необходимое доверие, связанное с ним, или обязательно ли дальнейшее доверие. Оценщик запишет те интерфейсы основного компонента, для которых необходимо дополнительное доверие, на обсуждение во время ACO_COR.1-3.

14.3.1.2.3 Операция ACO_COR.1-3

Оценщик рассмотрит рациональное построение, чтобы определить, как необходимые меры доверия применяются к основному компоненту. Оценочный вердикт, и получившееся в результате доверие, могут быть снова использованы для основного компонента, обеспечивая теми же его порциями; используются последовательно в составном ОО.

Для того чтобы определить применены ли уже необходимые меры доверия к компоненту, и порции, для которых еще необходимо применение мер доверия, оценщик должен использовать продукцию деятельности ACO_DEV.*.2E и операции ACO_COR.1-1 и ACO_COR.1-2:

а) Интерфейсы, определенные в информации доверия (Доверие зависимого компонента (ACO_REL)), но не обсуждаемые в информации разработки (Данные развития (ACO_DEV)), дополнительная информация требуется. (Идентифицировано в ACO_COR.1-1.)

б) Интерфейсы, использованные в Объекте оценки несовместимо с основным компонентом (различие между информацией, снабженной Данными развития (ACO_DEV) и в Доверии зависимого компонента (ACO_REL)), влияние этих различий требует обоснованности. (Идентифицировано в ACO_DEV.*.2E.)

в) Интерфейсы, определенные в рациональном построении, для которых предварительно не было приобретено доверие, дополнительная информация требуется. (Идентифицировано в ACO_COR.1-1.)

г) Интерфейсы, описанные в соответствии с информацией доверия, рациональным построением и информацией разработки, не требуется никаких дальнейших действий, так как результаты оценки основного компонента могут быть использованы снова.

Интерфейсы основного компонента, служащие для использования информацией доверия, но не включенные в информацию разработки, указывают порции основного компонента, где требуется дальнейшее доверие.

Интерфейсы определяют входную точку в основной компонент.

Оценщик определяет интерфейсы, которые содержатся и в информации разработки, и в информации доверия, в их использовании в Объекте оценки по способу связанности с оценкой основного компонента. Метод использования интерфейса будет рассмотрен во время деятельности Данных

развития (ACO_DEV), чтобы определить последовательность использования интерфейса в обоих компонентах и Объекте оценки. Оставшимися действиями является определение связности конфигурации основного компонента и Объекта оценки. Для того чтобы определить это, оценщик рассмотрит документы по руководству каждого для гарантирования их связности (смотрите руководство ниже касательно связности документов по руководству). Любые отклонения в документации будут в дальнейшем проанализированы оценкой для определения возможных эффектов.

То, что интерфейсы, которые сообразно были описаны в информации разработки и информации доверия, а руководство связано с основным компонентом и Объектом оценки, требуемый уровень доверия считается проведенным.

Определение последовательности между доверием, полученным в основном компоненте, данными, полученными с помощью объекта оценки, и анализом, проведенным оценщиком на примерах, где были установлены противоречивости:

а) разработка.

Информация доверия определяет интерфейсы в зависимом компоненте, которые подобраны основным компонентом. Если интерфейс, определенный в информации доверия, не определен в информации разработки, то рациональное построение предоставляет положение о том, как основной компонент обеспечивает требуемыми интерфейсами.

Если интерфейс, определенный в информации доверия, определен в информации разработки, но между описаниями есть противоречия, то требуется дальнейший анализ. Оценщик определяет различия в использовании основного компонента, как рассматривается в оценке основного компонента, и составного Объекта оценки. Оценщик разработает план выполнения проверки интерфейса (во время испытания составного Объекта оценки (ACO_CTT)).

Статус патча основного и зависимого компонентов, использованный в составном Объекте оценки, должен быть сравним со статусом патча компонентов во время их оценки. Если любые патчи применены к компонентам, то рациональное построение должно содержать детали этих патчев, включая потенциальное воздействие оценочного компонента ИОС. Оценщик должен рассмотреть детали полученных изменений и проверить правильность потенциального воздействия изменения на компонент ИОС. Затем оценщик рассмотрит необходимость проверки изменения, сделанные патчем, в ходе испытания, и установит необходимость прохождения испытания. Проверка может принять форму повторного применения оценщиком/разработчиком выполнения испытания для оценочного компонента, или она может быть необходима для оценщика, чтобы разработать новые проверки подтверждения изменения компонента.

Если любой из индивидуальных компонентов был предметом доверия интенсивности действий, начиная с завершения оценочного компонента, то оценщик рассмотрит изменения, оцененные в доверии интенсивности действий во время независимого, уязвимого анализа, проведенного для составного объекта оценки (Составление уязвимого анализа (ACO_VUL)).

б) руководство.

Руководство к составному объекту оценки осуществляет существенное обращение к индивидуальным компонентам. К минимуму руководство относит необходимым определение любого упорядочения зависимостей в применении руководства к зависимому и основному компонентам, особенно во время установки составного объекта оценки.

В дополнение к применению семейств Подготовительных процедур (AGD_PRE) и Операционного руководства пользователя (AGD_OPE) к руководству для составного объекта оценки, необходимо проанализировать связность между руководствами к компонентам и составному Объекту оценки, определить любые отклонения.

Если руководство составного Объекта оценки направляется за пределы руководств основного и зависимого компонентов, то обсуждение последовательности является ограниченным по сравнению с последовательностью между документациями по руководству, примененными для каждого из компонентов (то есть между руководствами основного и зависимого компонентов). Тем не менее, если дополнительное руководство, применимое для составного Объекта оценки, используется и для компонентов, то требуется большой анализ, так как связность также требуется между документацией по руководству для компонентов и документацией по руководству для составного Объекта оценки.

Связность в этом случае означает, что либо руководства одинаковы, либо она придает дополнительное давление на операции индивидуальных компонентов, будучи сгруппированными, подобным способом для уточнения функциональных/гарантийных компонентов.

С доступной информацией (которая используется как ввод для данных развития (ACO_DEV) или подходы развития, обсужденные выше) оценщик в состоянии определить все возможные воздействия отклонений от конфигураций основного компонента, указанных в оценочном компоненте. Тем не менее, для высокого Оценочного уровня доверия (где оценка основного компонента включает требования плана Объекта оценки (ADV_TDS)) это возможно, за исключением того, что детальные спланированные абстракции основного компонента переданы как часть информации разработки составного Объекта оценки, возможные воздействия изменений на руководство не могут быть вполне определенными, так как внутренняя область неизвестна. В этом случае оценщик доложит остаточный риск анализа.

Эти остаточные риски содержат любые общественные оценочные сообщения для составного Объекта оценки.

Оценщик обратит внимание на эти разногласия в руководстве по вводу в действия независимого испытания оценщика (испытание Составного Объекта оценки (ACO_CTT)).

Руководство к составному Объекту оценки может присоединиться к руководству к компонентам, особенно в условиях установки и упорядочения установочных операций основного компонента по отношению к установочным операций зависимого компонента. Порядок установочных операций индивидуальных компонентов не должен меняться, однако, они могут чередоваться. Оценщик рассмотрит это руководство, чтобы гарантировать соприкосновение его с требованиями действий AGD_PRE, совершившееся во время оценки компонентов.

Это может быть случаем, когда информация доверия устанавливает, что интерфейсы основного компонента, в дополнение тех, определенных как Интерфейсы ФБО основного компонента, на которые полагается зависимый компонент, определяются в информации о доверии. Для руководства может быть необходимо обеспечить использование любых таких дополнительных интерфейсов основного компонента. Обеспеченный потребитель составного Объекта оценки необходим для получения документации по руководству основного компонента, затем результаты вердиктов AGD_PRE и AGD_OPE основного компонента могут быть использованы снова для тех интерфейсов, которые рассматриваются в основном компоненте.

Однако, для дополнительных интерфейсов, на которые полагается зависимый компонент, оценщик должен определить, что документации по руководству основного компонента соприкасаются с требованиями AGD_PRE и AGD_OPE, как применялось в оценках основного компонента.

Для интерфейсов, рассмотренных во время оценки основного компонента, и поэтому, для которых доверие уже усилилось, оценщик убедится в том, что руководство по использованию каждого интерфейса составного Объекта оценки связано с руководством основного компонента. Чтобы определить связано ли руководство составного объекта оценки с руководством основного компонента, оценщик должен отобразить каждый интерфейс в руководствах и составного объекта оценки, и основного компонента. Затем оценщик сравнивает руководства, чтобы определить связность.

Образцами дополнительных связей, обеспеченных в руководстве составного Объекта оценки, которые рассматривались как связанные с руководством основного компонента, являются (руководство к компоненту дается следом за образцом руководства составного Объекта оценки, что обосновано как дополнительная связность):

Компонент: Длина пароля должна быть не менее 8 знаков, включая

алфавитные и числовые.

Составной ОО: Длина пароля должна быть не менее 10 знаков, включая алфавитные и числовые, и, в меньшей степени, одного из следующих специальных наборов знаков: ( ) { } ^ < > - _

ПРИМЕЧАНИЕ Будет только приемлемо увеличение длины пароля на [целое число > 8] знаков, в то время как, удаляя поручение на добавление алфавитных и числовых знаков для составного ОО, если такая же длина или выше была достигнута для усиления оценки (учитывая вероятность взлома пароля).

Компонент: Следующие настройки непригодны в регистрационных настройках: WWW Издательские услуги и услуги ICDB Докладчика.

Составной ОО: Следующие настройки непригодны в регистрационных настройках: Издательские услуги, услуги ICDB Докладчика, Протокол

Дистанционного Вызова Процедур(RPC), Услуги Локатора и Вызова Процедур (RPC).

Компонент: Выберете следующие атрибуты, содержащиеся в учетном журнале регистрации: дата, время, тип события, предмет идентификатора и успех/провал.

Составной ОО: Выберете следующие атрибуты, содержащиеся в учетном журнале регистрации: дата, время, тип события, предмет идентификатора, успех/провал, сообщение о событии и процесс последовательности команд.

Если руководство составного объекта оценки отклоняется (но не уточняется) от руководства основного компонента, то оценщик оценит возможные риск изменения руководства. Оценщик использует доступную информацию (включая применяемую в общественном домене, архитектурное описание основного компонента в отчете общественной оценки (например, отчет о свидетельстве), остаточный контекст руководства с документации по руководству), чтобы определить вероятное воздействие изменения в руководстве на ИОС составного Объекта оценки.

Если в течение оценки зависимого компонента пробная установка использовала основной компонент, чтобы удовлетворить требования, окружающие зависимый компонент, то эта операция для составного ОО будет считаться удовлетворенной. Если основной компонент не был использован в удовлетворение операции AGD_PRE.1-3 во время оценки зависимого компонента, то оценщик применит процедуры пользователя, основанных для составного ОО, чтобы приготовить составной ОО, в соответствии с руководством, указанным в AGD_PRE.1-3. Это позволит оценщику определить, что подготовительное руководство составного ОО является достаточным для подготовки составного ОО и операционной окружающей безопасности.

в) жизненный цикл.

Доставка

Если имеется различный механизм доставки, использующийся для доставки составного ОО (то есть компоненты не доставляются потребителю в соответствии с процедурой безопасной доставки, определенной и оцененной во время оценки компонентов), то процедура доставки составного ОО потребует оценки против требований Доставки (ALC_DEL), примененных во время оценки компонентов.

Составной ОО может быть доставлен как комплексный продукт или может потребовать компонент, чтобы быть доставленным отдельно.

Если компоненты доставляются отдельно, то результаты доставки основного и зависимого компонентов используются снова. Доставка основного компонента проверяется в течение пробной установки оценщика зависимого компонента, используя при этом указанное руководство и проверяя аспекты доставки, которые являются ответственностью пользователя, как описано в документации по руководству основного компонента.

Если составной ОО доставлен как нечто новый объект, то метод доставки этого объекта должен быть рассмотрен в оценочных действиях составного ОО.

Оценка процедур доставки пунктов составного ОО выполняется в соответствии с методологией Доставки (ALC_DEL), как и для любого другого [компонента] ОО, гарантируя любые дополнительные пункты (то есть дополнительные документы по руководству составного ОО), рассматривается процедурами доставок.

Способности УК

Уникальная идентификация составного ОО обосновывается в течение применения Оценки функциональной подгруппы (ALC_CMC.1), и пункты, содержащие в себе составной ОО, рассматриваются в течение применения Оценки функциональной подгруппы (ALC_CMS.2).

Также дополнительное руководство может быть выработано для составного ОО, уникальная идентификация этого руководства (обоснованная как часть уникальной идентификации составного ОО в течение Оценки функциональной подгруппы (ALC_CMC.1)) рассматривается обоснованным контролем руководства.

Вердикты оставшегося (не обоснованного выше) Класса ALC: проявления поддержки Жизненного цикла могут быть использованы снова из оценки основного компонента, так как никакого дальнейшего развития во время интеграции составного ОО не будет выполнено.

Нет никаких дополнительных обоснований безопасности развития, так как интеграция придумана либо со стороны потребителя, либо на примере того, что составной ОО доставлен как комплексный продукт, на стороне разработчика зависимого компонента. Контроль со стороны потребителя

находится вне обоснования ИСО/МЭК 15408. Нет необходимости в дополнительных требованиях или руководствах, если интеграция находится на той же стороне, что и зависимого компонента, так как все компоненты обосновываются как пункты конфигураций составного ОО, и поэтому, в любом случае, должны быть рассмотрены разработчиком безопасных процедур зависимого компонента.

Приемы и техника, усвоенные во время интеграции, будут рассмотрены данными, применяемыми разработчиком зависимого компонента. Любые важные приемы/техника основного компонента будут рассмотрены во время оценки основного компонента. Например, если основной компонент доставлен как исходный код и требует компиляции потребителя (например, разработчик зависимого компонента, выполняющий интеграцию), то компилятор будет указан и оценен, параллельно соответствующего аргумента, во время оценки основного компонента.

Нет никакого определения жизненного цикла, применимого к составному ОО, так как нет дальнейших развитий пунктов.

Результаты исправления дефектов компонента не применимы для составного ОО. Если исправление дефекта входит в пакет доверия составного ОО, то требования исправления дефекта (ALC_FLR) применимы в течение оценки составного ОО (как для любого увеличения).

г) проверка.

Составной ОО будет испытан во время управления класса ATE: Действия проверки оценки зависимого компонента, при которой конфигурации использовали для проверки зависимого компонента, должны включать основной компонент, чтобы удовлетворить требования Информационной технологии в операционном окружении. Если основной компонент не был использован для проверки оценки зависимого компонента, или конфигурация компонента различалась от их оценочных конфигураций, то разработчик проверки, основанной для оценки зависимого компонента, удовлетворит Класс ATE: Требуемые проверки будут повторены для составного объекта оценки.

14.4 Данные разработки (ACO_DEV)

14.4.1 Оценка подвида деятельности (ACO_DEV.1)

14.4.1.1 Цели

Целью этой функциональной подгруппы является определение того, что подходящая практичность безопасности применяется основным компонентом в поддержку зависимого компонента. Это будет достигнуто посредством обследования интерфейсов основного компонента, чтобы определить, что они связаны с интерфейсами, указанными в информации доверия; которые употребляются зависимым компонентом.

Описание интерфейсов основного компонента применяется на уровне

детальной связи с Оценкой функциональной подгруппы (ADV_FSP.2), также не все аспекты, требуемые для удовлетворения Оценки функциональной подгруппы (ACO_DEV.1), требуются для Оценки функциональной подгруппы (ADV_FSP.2); интерфейс был определен, и цель, описывающая остаточную деталь, специфики интерфейса, могла быть повторена в использовании основного компонента.

14.4.1.2 Ввод

Оценочными данными для этой функциональной подгруппы являются:

а) составное ЗБ;

б) информация разработки;

в) информация доверия.

14.4.1.3 Действие ACO_DEV.1.1E

Информация разработки опишет цель каждого интерфейса основного компонента, использованного в составном ОО.

14.4.1.3.1 Операция ACO_DEV.1-1

Оценщик рассмотрит информацию разработки, чтобы определить, что она описывает цель каждого интерфейса.

Основной компонент обеспечивает интерфейсы в поддержку взаимодействия с зависимым компонентом в обеспечении зависимого ФБО. Цель каждого интерфейса - это описание его на том же уровне, что и описание интерфейсов зависимого компонента ФБО, так как было бы применимо между подсистемами в плане ОО (Оценка функциональной подгруппы (ADV_TDS.1)). Это описание применимо для читателя с пониманием того, как основной компонент обеспечивает услуги, требуемые зависимым компонентом ФБО.

Эта операция может быть удовлетворена обеспечением функциональной специфики основного компонента для тех интерфейсов, которые являются Интерфейсами ФБО основного компонента.

Информация разработки показывает соответствие между интерфейсами, использованными в составном ОО, основным и зависимым компонентами в поддержку ФБО зависимого компонента.

14.4.1.3.2 Операция ACO_DEV.1-2

Оценщик рассмотрит информацию разработки, чтобы определить, что соответствие, между интерфейсами основного компонента и интерфейсами, на которые полагается зависимый компонент, верно.

Соответствие между интерфейсами основного компонента и интерфейсами, на которые полагается зависимый компонент, может принять форму матрицы или таблицы. Интерфейсы, на которые полагается зависимый компонент, определяются в информации доверия (как было рассмотрено в течение проявления Доверия зависимого компонента (ACO_REL)).

В течение этого действия, нет никакого требования определить полноту

сферы деятельности интерфейсов, на которые может полагаться зависимый компонент, только что соответствие верно, и гарантия, что интерфейсы основного компонента отображены с интерфейсами, требуемыми зависимым компонентом, всегда возможно.

Полнота сферы деятельности рассматривается в действии Рационального построения (ACO_COR).

14.4.1.4 Действие ACO_DEV.1.2E

14.4.1.4.1 Операция ACO_DEV.1-3

Оценщик рассмотрит информацию разработки и информацию доверия, чтобы определить, что интерфейсы описаны последовательно.

Целью оценщика в этой операции является определение того, что интерфейсы, описанные в информации разработки для основного компонента, и информации доверия для зависимого компонента представлены последовательно.

14.4.2 Оценка подвида деятельности (ACO_DEV.2)

14.4.2.1 Цели

Целью этой функциональной подгруппы является определение того, что подходящая функциональная безопасность обеспечена основным компонентом в поддержку зависимого компонента. Это будет достигнуто посредством обследования интерфейсов и связанного безопасного образа действий основного компонента, чтобы определить, что они связаны с интерфейсами, указанными в информации доверия; которые употребляются зависимым компонентом.

14.4.2.2 Ввод

Оценочными данными для этой функциональной подгруппы являются:

а) составное ЗБ;

б) информация разработки;

в) информация доверия.

14.4.2.3 Действие ACO_DEV.2.1E

Информация по разработке должна описывать цель и метод каждой функции базового компонента в составном ОО.

14.4.2.3.1 Операция ACO_DEV.2-1

Оценщик должен проверять информацию по разработке для определения, что там точно описывается цель каждой функции.

Базовый компонент предоставляет функции безопасности для поддержки взаимодействия с зависимыми компонентами в обеспечении зависимых ФБО. Цель каждой функции направлена на описание функции безопасности на том же самом уровне, что и зависимый компонент, уровень между подсистемами в проекте ОО (Оценка подвид деятельности ADV_TDS.1). Данное описание позволяет читателю понять, как базовый компонент обеспечивает функциями необходимыми для зависимого компонента ФБО.

Выполнение этого действия может быть проведено посредством функциональной спецификацией для базового компонента ФБОI.

14.4.2.3.2 Операция ACO_DEV.2-2

Оценщик должен проверять информацию по разработке для определения, что там точно описывается метод использования каждой функции.

Метод использования функции безопасности резюмирует о том, каким образом применяется функция для активации операций и получения результатов. Оценщик должен самостоятельно понять использование функции исходя из данного материала о разработке. Совсем не обязательно иметь отдельные способы для использования каждой функции, а также распознания их, применяя общий стиль.

Выполнение этого действия может быть проведено посредством функциональной спецификацией для базового компонента ФБОI.

Информация по разработке должна содержать полное описание поведения базового компонента, поддерживающее давление на зависимый компонент ТФБ.

14.4.2.3.3 Операция ACO_DEV.2-3

Оценщик должен проверять информацию по разработке для определения, что там точно описывается поведение базового компонента, поддерживающее давление на зависимый компонент ТФБ. Зависимый компонент активизирует функции безопасности базового компонента для обеспечения необходимых функций. Для функций безопасности активированного базового компонента информация по разработке включает в себя полное описание безопасного поведения базового компонента. Описание безопасного поведения базового компонента указывает на необходимые функции данного компонента при вызове функций безопасности. Данное описание должно соответствовать уровню для ADV_TDS.1.4C. Поэтому, свидетельство проекта ОО выполнит данная операция, где функции безопасности активированы зависимым компонентом ФБОI. Если активация произошла не посредством ФБОI базового компонента, то безопасное поведение не обязательно описывать в свидетельстве проекта ОО.

Информация по разработке должна показывать соответствие между функциями безопасности базового и зависимого компонента, используемое в составном ОО, для поддержки ФБО зависимого компонента.

14.4.2.3.4 Операция ACO_DEV.2-4

Оценщик должен проверить информацию о развитии, чтобы определить точность соответствия между интерфейсами базового компонента и интерфейсами, на которые опирается зависимый компонент.

Соответствие между интерфейсами базового компонента и интерфейсами, на который опирается зависимый компонент, может иметь

форму матрицы или таблицы. Интерфейсы, на которые опирается зависимый компонент, выявляются в информации зависимости (как проверено во время Зависимости зависимого компонента (ACO_REL)).

Во время выполнения такого действия не возникает иного требования проверить полноту охвата интерфейса, на которую опирается зависимый компонент, кроме требования проверить точность соответствия и подтвердить, что интерфейсы базового компонента при необходимости преобразованы в интерфейсы, необходимые для зависимых компонентов.

Полнота охвата учитывается в операциях логического обоснования (ACO_COR) состава.

14.4.2.4 Действие ACO_DEV.2.2E

14.4.2.4.1 Операция ACO_DEV.2-5

Оценщик должен проверить информацию о развитии, а также информацию о зависимости, чтобы определить, что интерфейсы описываются последовательно.

Целью вычислителя в данной единице работы является определение того, что интерфейсы, описываемые в информации о развитии для базового компонента, и информация о зависимости для зависимого компонента представлены последовательно.

14.4.3 Оценка подвида деятельности (ACO_DEV.3)

14.4.3.1 Цели

Целью данного подвида деятельности является определение, что, базовым компонентом обеспечена функциональная возможность надлежащей безопасности для поддержки зависимого компонента. Это достигается путем проверки интерфейсов безопасного поведения базового компонента, чтобы определить, что они согласуются с интерфейсами указанными в информации о зависимости, необходимые для зависимого компонента.

Кроме описания интерфейса также будут описаны подсистемы базового компонента, которые обеспечивают функциональную возможность безопасности, необходимую для зависимого компонента, чтобы оценщик мог определить, составлял ли тот интерфейс часть ФБО базового компонента.

14.4.3.2 Исходные данные

Свидетельством оценки для данного подвида действия является:

а) составной ЗБ;

б) информация о развитии;

в) информация о зависимости.

14.4.3.3 Действие ACO_DEV.3.1E

Информация о развитии должна описывать цель и метод применения для каждого интерфейса базового компонента, используемого в составном ОО.

14.4.3.3.1 Операция ACO_DEV.3-1

Оценщик должен проверить информацию о развитии, чтобы определить, что она описывает цель каждого интерфейса.

Базовый компонент предоставляет интерфейсы для поддержки взаимодействия с зависимым компонентом в обеспечении зависимого ФБО. Цель каждого интерфейса заключается в его описании на том же уровне, что и описание интерфейсов для функциональной возможности зависимого компонента ФБО , которое может быть обеспечено между подсистемами в проекте ОО (Оценка дополнительного действия (ADV_TDS.1)). Данное описание должно представить считывателю понимание того, как базовый компонент предоставляет услуги, требуемые зависимым компонентом ФБО.

Такая единица работы может быть выполнена обеспечением функциональной спецификации для базового компонента для таких интерфейсов, которые являются ФБОI базового компонента.

14.4.3.3.2 Операция ACO_DEV.3-2

Оценщик должен проверить информацию о развитии, чтобы определить, что она описывает метод применения для каждого интерфейса.

Метод применения для интерфейса подводит итог того, как обрабатывается интерфейс для того, чтобы активизировать операции и получить результаты, связанные с интерфейсом. Оценщик должен уметь определить способ применения интерфейса от считывания данного материала в информации о развитии. Это необязательно должно означать, что имеется необходимость в отдельном методе применения каждого интерфейса, так как можно дать общее описание того, как например активизируются APIA и затем выявить каждый интерфейс используя общий стиль.

Такая единица работы может быть выполнена обеспечением функциональной спецификации для базового компонента для таких интерфейсов, которые являются ФБОI базового компонента.

Информация о развитии должна выявлять подсистемы базового компонента, которые обеспечивают интерфейсы базового компонента, используемый в составном ОО.

14.4.3.3.3 Операция ACO_DEV.3-3

Оценщик должен проверять информацию о развитии, чтобы определить, что выявлены все подсистемы базового компонента, которые обеспечивают интерфейсы для зависимого компонента.

Для таких интерфейсов, которые считаются составляющей ФБОI базового компонента, подсистемы связанные с интерфейсом будут подсистемами, рассматриваемыми в проектируемом процессе ОО (ADV_TDS) во время оценки базового компонента. Интерфейсы, на которые опирается зависимый компонент, и, которые не составляли часть ФБОI базового компонента, будут преобразованы к подсистемам за пределами ФБО базового компонента.

Информация о развитии должна предоставлять высокоуровневое описание поведения подсистем базового компонента, которые поддерживают принуждение ТФБ зависимых компонентов.

14.4.3.3.4 Операция ACO_DEV.3-4

Оценщик должен проверить информацию о развитии, чтобы определить, что она описывает поведение подсистем базового компонента, которые поддерживают принуждение ТФБ зависимого компонента.

Зависимый компонент активизирует интерфейсы базового компонента, чтобы базовый компонент предоставлял услуги. Для активизируемых интерфейсов базового компонента информация о развитии должна содержать высокоуровневое описание связанной безопасности поведения базового компонента. Описание безопасного поведения базового компонента обрисует, как базовый компонент предоставляет необходимую услугу, когда производится вызов интерфейса. Такое описание должно быть на том же уровне, что и для ADV_TDS.1.4C. Следовательно, обеспечение расчетного свидетельства ОО от оценки базового компонента удовлетворит единицу работы, если интерфейсы, активизируемые зависимыми компонентами, являются ФБОI базового компонента. Если интерфейсы, активизируемые зависимыми компонентами, не являются ФБОI базового компонента, то связанная безопасность поведения может и не описываться в расчетном свидетельстве ОО базового компонента.

Информация о развитии должна содержать преобразование от интерфейсов к подсистемам базового компонента.

14.4.3.3.5 Операция ACO_DEV.3-5

Оценщик должен проверить информацию о развитии, чтобы определить, точность соответствия между интерфейсами и подсистемами базового элемента.

Если после оценки базового компонента стали доступны расчетное свидетельство ОО и свидетельство спецификации функциональной возможности, то они могут быть использованы для проверки точности соответствия между интерфейсами и подсистемами базового компонента, как использовалось в составном ОО. Те интерфейсы базового компонента, которые составляли часть ФБОI базового компонента, будут описаны в спецификации функциональной возможности базового компонента, и связанные подсистемы будут описаны в расчетном свидетельстве ОО базового компонента.

Если, однако, интерфейс базового компонента не составлял часть ФБОI базового компонента, то описание поведения подсистемы содержащееся в информации о развитии будет использовано для проверки точности соответствия.

Информация о развитии должна показывать соответствие между интерфейсами, используемыми в составном ОО базового компонента и зависимым компонентом для поддержки ФБО зависимого компонента.

14.4.3.3.6 Операция ACO_DEV.3-6

Оценщик должен проверить информацию о развитии, чтобы определить точность соответствия между интерфейсами базового компонента и интерфейсами, на которые опирается зависимый компонент.

Соответствие между интерфейсами базового компонента и интерфейсами, на которые опирается зависимый компонент, может иметь форму матрицы или таблицы. Интерфейсы, на которые опирается зависимый компонент, выявляются в информации зависимости (как проверено во время Зависимости зависимого компонента (ACO_REL)).

Во время выполнения такого действия не возникает иного требования проверить полноту охвата интерфейса, на которую опирается зависимый компонент, кроме требования проверить точность соответствия и подтвердить, что интерфейсы базового компонента при необходимости преобразованы к интерфейсам, необходимые для зависимых компонентов.

Полнота охвата учитывается в операциях Логического обоснования (ACO_COR) состава.

14.4.3.4 Действие ACO_DEV.3.2E

14.4.3.4.1 Операция ACO_DEV.3-7

Оценщик должен проверить информацию о развитии, а также информацию о зависимости, чтобы определить, что интерфейсы описываются последовательно.

Целью вычислителя в данной единице работы является определение того, что интерфейсы, описываемые в информации о развитии для базового компонента, и информация о зависимости для зависимого компонента представлены последовательно.

14.5 Зависимость зависимого компонента (ACO_REL)

14.5.1 Оценка подвида деятельности (ACO_REL.1)

14.5.1.1 Цели

Целью данного подвида деятельности является определение того, достаточно ли информации предоставляет свидетельство зависимости разработчика, чтобы определить доступность необходимой функциональной возможности в базовом компоненте и средство, с помощью которого активизируется такая функциональная возможность. Такая задача выполняется в условиях высокоуровневого описания.

14.5.1.2 Исходные данные

Свидетельством оценки для данного подвида деятельности является:

а) составной ЗБ;

б) функциональная спецификация зависимого компонента;

в) проект зависимого компонента;

г) проектирование архитектуры зависимого компонента;

д) информация зависимости.

14.5.1.3 Замечания по применению

Зависимый компонент, ФБО которого взаимодействует с базовым компонентом требует функциональную возможность, предоставленную таким базовым компонентом (например, дистанционная аутентификация, дистанционное хранение данных проверки). В таких случаях активизируемые услуги необходимо описать для тех, которые отвечают за конфигурацию составных ОО для конечных пользователей. Логическим обоснованием требования такой документации является помощь интеграторам составных ОО, в определении того, какие услуги базового компонента могут иметь негативное влияние на зависимый компонент, и предоставить информацию, по которой определяется совместимость компонентов при использовании семейства свидетельств Развития (ACO_DEV).

14.5.1.4 Действие ACO_REL.1.1E

Соответственная информация содержит описание функционального назначения базовых компонентных аппаратных средств, микропрограмм и (или) программного обеспечения, которое полагается на зависимый компонент ФБО.

14.5.1.4.1 Операция ACO_REL.1-1

Оценщик проверяет соответствие информации, чтобы определить, что она содержит описание функционального назначения базовых зависимых аппаратных средств, микропрограмм и (или) программного обеспечения, которое полагается на зависимый компонент ФБО.

Оценщик оценивает описание функций безопасности, которых требует зависимый компонент ФБО, включая обеспеченность базовыми компонентными аппаратными средствами, микропрограммами и программным обеспечением. Акцент этого рабочего устройства делается на уровень деталей этого описания, а не на оценку информационной точности.

(Оценка точности информации является предметом следующего рабочего устройства).

Описание базового компонентного функционального назначения не должно быть подробнее уровня описания компонента ФБО, как приведено в проекте ОО (Проект ОО (ADV_TDS).

14.5.1.4.2 Операция ACO_REL.1-2

Оценщик проверяет соответствие информации, чтобы определить, что она точно отражает цели, определенные для операционной среды зависимого компонента.

Соответствующая информация содержит описание базовых компонентных функций безопасности, рассчитанных на зависимый компонент. Чтобы проверить соответствие надежности информации

ожиданиям операционной среды зависимого компонента, оценщик сравнивает информацию надежности с изложением целей среды в ЗБ для зависимого компонента.

Например, если информация надежности требует, чтобы зависимый компонент ФБО полагался на базовый компонент, чтобы хранить и защищать данные ревизии, пока другое оценочное доказательство (например, разработка зависимого компонента) дает понять, что сам зависимый компонент ФБО хранит и защищает данные ревизии, это указывает на погрешность.

Следует отметить, что задачи операционной среды могут содержать цели, которые соответствуют мере не-IT. Пока услуги, которые базовая компонентная среда предполагает обеспечить, указаны в описании целей ИТ для операционной среды в зависимом компоненте ЗБ, не требуется, чтобы все такие предположения в отношении среды указывались в информации надежности.

Информация надежности описывает все взаимодействия, посредством которых зависимый компонент ФБО запрашивает услуги базового компонента.

14.5.1.4.3 Операция ACO_REL.1-3

Оценщик проверяет информацию надежности, чтобы определить, что он описывает все взаимодействия между зависимым компонентом и базовым компонентом, посредством которого зависимый компонент ФБО запрашивает услуги базового компонента.

Зависимый компонент ФБО может запрашивать услуги базового компонента, которые не входят в пределы ФБО базового компонента (смотри В.3, Взаимодействия между составными сущностями ИТ в СТ РК ИСО/МЭК 15408-3).

Интерфейсы к базовому функциональному назначению компонента описаны на том же уровне, что и описание интерфейсов к зависимому функциональному назначению компонента ФБО, как предусматривается подсистемами в проекте ОО (Оценка функциональной подгруппы (ADV_TDS.1).

Цель описания взаимодействий зависимых компонентов и базовых компонентов - обеспечить понимание того, как зависимый компонент ФБО полагается на базовый компонент для предоставления услуг поддержания действия функций безопасности зависимого компонента. Эти взаимодействия не нуждаются в характеристике на уровне реализации (например, параметры, переданные с одной подпрограммы компонента в подпрограмму другого компонента), но элементы данных, идентифицированные для определенного компонента, которые будут использоваться другим компонентом, следует включить в это описание. Эта

формулировка поможет читателю понять, в общих чертах, почему необходимо взаимодействие.

Точность и полнота интерфейсов основаны на функции безопасности, предоставляемой базовым компонентом, которая необходима ФБО, как установлено в рабочих устройствах ACO_REL.1-1 и ACO_REL.1-2. Должно быть возможным отображать все функциональные назначения, описанные в более ранних рабочих устройствах к интерфейсам, идентифицированным в этом рабочем устройстве, и наоборот. Интерфейс, который не соответствует описанному функциональному назначению, должен также указывать на несоответствие.

Информация надежности описывает, как зависимый ФБО защищает себя от помеха и подделок базовым компонентом.

14.5.1.4.4 Операция ACO_REL.1-4

Оценщик проверяет информацию доверия, чтобы подтвердить, что она описывает, как зависимый ФБО защищает себя помех и подделок базовым компонентом.

Описание того, как зависимый компонент защищает себя помех и подделок базовым компонентом должно быть приведено на том же уровне деталей, как необходимо для ADV_ARC.1-4.

14.5.2 Оценка подвида деятельности (ACO_REL.2)

14.5.2.1 Цели

Целями этой функциональной подгруппы являются определение обеспечивает ли разработчик оценочное доказательство достаточности информации, чтобы определить, что необходимое функциональное назначение доступно в базовом компоненте, и средствах, при помощи которых запущено функциональное назначение. Это обеспечивается в условиях интерфейсов между зависимым и базовым компонентом, и возвращаемые значения тех интерфейсов вызываются зависимым компонентом.

14.5.2.2 Исходные данные

Оценочное доказательство для этой функциональной подгруппы:

а) составной ЗБ;

б) функциональная спецификация зависимого компонента;

в) разработка зависимого компонента;

г) представление реализации зависимого компонента;

д) архитектурная разработка зависимого компонента;

е) информация надежности.

14.5.2.3 Замечания по применению

Зависимый компонент, чье ФБО взаимодействует с базовым компонентом, требует функционального назначения, предусмотренного этим базовым компонентом (например, дистанционная аутентификация,

дистанционное хранение данных ревизии). В этих случаях, запущенные услуги должны быть описаны для несущих ответственность за планирование конфигурации составных ОО для конечных пользователей. Логическое обоснование требований документации заключается в поддержке интеграторов составных ОО определять, какие услуги в базовом компоненте могут иметь неблагоприятные воздействия на зависимый компонент, против которых предоставлять информацию и определять совместимость компонентов при применении доказательств разработки (ACO_DEV) семейства.

14.5.2.4 Действие ACO_REL.2.1E

Информация надежности описывает функциональное назначение базовых компонентных аппаратных средств, микропрограмм и (или) программного обеспечения, которое полагается на зависимый компонент ФБО.

14.5.2.4.1 Операция ACO_REL.2-1

Оценщик проверяет соответствие информации, чтобы определить, что она содержит описание функционального назначения базовых зависимых аппаратных средств, микропрограмм и (или) программного обеспечения, которое полагается на зависимый компонент ФБО.

Оценщик оценивает описание функций безопасности, которых требует зависимый компонент ФБО, включая обеспеченность базовыми компонентными аппаратными средствами, микропрограммами и программным обеспечением. Акцент этого рабочего устройства делается на уровень деталей этого описания, а не на оценку информационной точности.

Оценка точности информации является предметом следующего рабочего устройства.

Описание базового компонентного функционального назначения не должно быть подробнее уровня описания компонента ФБО, как приведено в проекте ОО (Проект ОО (ADV_TDS).

14.5.2.4.2 Операция ACO_REL.2-2

Оценщик проверяет соответствие информации, чтобы определить, что она точно отражает цели, определенные для операционной среды зависимого компонента.

Соответствующая информация содержит описание базовых компонентных функций безопасности, рассчитанных на зависимый компонент. Чтобы проверить соответствие надежности информации ожиданиям операционной среды зависимого компонента, оценщик сравнивает информацию надежности с изложением целей среды в ЗБ для зависимого компонента.

Например, если информация надежности требует, чтобы зависимый компонент ФБО полагался на базовый компонент, чтобы хранить и защищать данные ревизии, пока другое оценочное доказательство (например,

разработка зависимого компонента) дает понять, что сам зависимый компонент ФБО хранит и защищает данные ревизии, это указывает на погрешность.

Следует отметить, что задачи операционной среды могут содержать цели, которые соответствуют мере не-IT. Пока услуги, которые базовая компонентная среда предполагает обеспечить, указаны в описании целей ИТ для операционной среды в зависимом компоненте ЗБ, не требуется, чтобы все такие предположения в отношении среды указывались в информации надежности.

Информация надежности описывает все взаимодействия, посредством которых зависимый компонент ФБО запрашивает услуги базового компонента.

14.5.2.4.3 Операция ACO_REL.2-3

Оценщик проверяет информацию надежности, чтобы определить, что он описывает все взаимодействия между зависимым компонентом и базовым компонентом, посредством которого зависимый компонент ФБО запрашивает услуги базового компонента.

Зависимый компонент ФБО может запрашивать услуги базового компонента, которые не входят в пределы ФБО базового компонента (смотри В.3, Взаимодействия между составными сущностями ИТ в СТ РК ИСО/МЭК 15408-3).

Интерфейсы к базовому функциональному назначению компонента описаны на том же уровне, что и описание интерфейсов к зависимому функциональному назначению компонента ФБО, как предусматривается подсистемами в проекте ОО (Оценка функциональной подгруппы (ADV_TDS.1).

Цель описания взаимодействий зависимых компонентов и базовых компонентов - обеспечить понимание того, как зависимый компонент ФБО полагается на базовый компонент для предоставления услуг поддержания действия функций безопасности зависимого компонента. Эти взаимодействия не нуждаются в характеристике на уровне реализации (например, параметры, переданные с одной подпрограммы компонента в подпрограмму другого компонента), но элементы данных, идентифицированные для определенного компонента, которые будут использоваться другим компонентом, следует включить в это описание. Эта формулировка поможет читателю понять, в общих чертах, почему необходимо взаимодействие.

Точность и полнота интерфейсов основаны на функции безопасности, предоставляемой базовым компонентом, которая необходима ФБО, как установлено в рабочих устройствах ACO_REL.2-1 и ACO_REL.2-2. Должно быть возможным отображать все функциональные назначения, описанные в более ранних рабочих устройствах к интерфейсам, идентифицированным в

этом рабочем устройстве, и наоборот. Интерфейс, который не соответствует описанному функциональному назначению, должен также указывать на несоответствие.

Информация надежности описывает, как зависимый ФБО защищает себя от помеха и подделок базовым компонентом.

14.5.2.4.4 Операция ACO_REL.2-4

Информация надежности описывает каждое взаимодействие с точки зрения используемого интерфейса и возвращаемых значений с тех интерфейсов.

Идентификацию интерфейсов, используемых зависимым компонентом ФБО при подготовке запросов об услугах базового компонента, позволяет интегратору определять обеспечивает ли базовый компонент все необходимые соответствующие интерфейсы. Это понимание далее усиливается при помощи спецификации возвращаемых значений, ожидаемых зависимым компонентом. Оценщик проверяет, чтобы интерфейсы описывались для каждого определенного взаимодействия (как проанализировано в ACO_REL.2-3).

Информация надежности описывает, как зависимый ФБО защищает себя от помех и подделок базовым компонентом.

14.5.2.4.5 Операция ACO_REL.2-5

Оценщик проверяет информацию надежности, чтобы определить, что он описывает, как зависимый ФБО защищает себя от помех и подделок базовым компонентом.

Описание того, как зависимый компонент защищает себя от помех и подделок базовым компонентом должно обеспечиваться на том же уровне детали как необходимо для ADV_ARC.1-4.

14.6 Составное тестирование TOE (ACO_CTT)

14.6.1 Оценка подвида деятельности (ACO_CTT.1)

14.6.1.1 Цели

Целью данного подвида деятельности является определение, правильно ли разработчик выполнил и документально оформил испытания каждого из базовых компонентных интерфейсов, на которые полагается зависимый компонент. Как часть этого определения оценщик повторяет испытание образцов, выполненное разработчиком и выполняет любые дополнительные испытания, необходимые для того, чтобы гарантировать ожидаемое поведение всех составных ОО ТФБ и интерфейсов базового компонента, на который полагается зависимый компонент.

14.6.1.2 Исходные данные

Оценочное доказательство для этой функциональной подгруппы:

а) составной TOE, подходящий для испытания;

б) доказательство испытания составного TOE компонента;

в) надежная информация;

г) информация о разработке.

14.6.1.3 Действие ACO_CTT.1.1E

Составной TOE и испытательная документация интерфейса базового компонента состоит из планов испытаний, ожидаемых результатов испытаний и фактических результатов испытаний.

14.6.1.3.1 Операция ACO_CTT.1-1

Оценщик проверяет испытательную документацию составного TOE, чтобы определить, что в нее входят планы испытаний, ожидаемые результаты испытаний и фактические результаты испытаний.

Это рабочее устройство может быть удовлетворено предоставлением доказательств испытаний, исходя из оценки зависимого компонента, если базовый компонент был использован, чтобы удовлетворять требования для ИТ в операционной среде зависимого компонента.

Все рабочие устройства, необходимые для удовлетворения ATE_FUN.1.1E применяются для определения:

а) что испытательная документация состоит из планов испытаний, ожидаемых результатов испытаний и фактических результатов испытаний;

б) что испытательная документация содержит информацию, необходимую для гарантии повторяемости испытаний;

в) уровня усилий разработчика, которые были приложены к испытанию базового компонента.

14.6.1.3.2 Операция ACO_CTT.1-2

Эксперт должен изучить тестовую документацию интерфейса базового компонента, чтобы определить, что она состоит из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования.

Данная операция может быть удовлетворена посредством предоставления испытательного доказательства на основе оценки базового компонента для тех интерфейсов, полагающихся на составленный ОО зависимым компонентом, которые являются ИФБО успешно оцененного базового компонента. Определение того, являлись ли фактически интерфейсами основного компонента, основанного на зависимом компоненте, ИФБО оцененного основного компонента, делается во время деятельности ACO_COR.

Все операции, необходимые для удовлетворения ATE_FUN.1.1E, будут применяться для определения:

а) того, что тестовая документация состоит из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования;

б) того, что тестовая документация содержит информацию, необходимую для того чтобы гарантировать, что тесты могут быть воспроизведены повторно;

в) уровень усилий разработчика, которые были применены к тестированию основного компонента.

тестовая документация по выполнению разработчиком составленных тестов ОО должна продемонстрировать, что ФБО работает как определено.

14.6.1.3.3 Операция ACO_CTT.1-3

Эксперт должен исследовать тестовую документацию, чтобы определить, что выполнение разработчиком составленных тестов ОО должны продемонстрировать, что ФБО работает, как определено.

Эксперт должен создать графическое отображение между тестами, описанными в плане тестирования ТФБ, определенном для составленного ОО, чтобы идентифицировать, какие ТФБ были проверены разработчиком.

Руководство по данной операции находится в п. 12.2.1 и п. 12.2.2.

Выводы из успешного выполнения тестов, как определено для ATE_FUN.1.3C, могут быть сравнены с графическим отображением, чтобы решить, что ТФБ составленного ОО, как проверено разработчиком, работает, как и ожидалось.

тестовая документация по выполнению разработчиком тестирования интерфейса базового компонента должна продемонстрировать, что интерфейс базового компонента, на который полагается зависимый компонент, работает как определено.

14.6.1.3.4 Операция ACO_CTT.1-4

Эксперт должен изучить тестовую документацию, чтобы установить, что выполнение разработчиком тестов интерфейса базовых компонентов должно продемонстрировать, что интерфейсы базовых компонентов, на которые полагается зависимый компонент, ведут себя как определено.

Эксперт должен создать графическое отображение между тестами, описанными в плане по тестированию и интерфейсах базового компонента, на который полагается зависимый компонент (как определено в достоверных источниках информации, изученной ACO_REL), чтобы идентифицировать какие интерфейсы базового компонента были проверены разработчиком.

Руководство по данной операции находится в п. 12.2.1 и п. 12.2.2.

Выводы из успешного выполнения тестов, как оценено для ATE_FUN.1.3C, могут быть сравнены с графическим отображением, чтобы определить, что интерфейсы базового компонента, проверенные разработчиком, работают, как и ожидалось, базовый компонент должен быть подходящим для тестирования.

14.6.1.3.5 Операция ACO_CTT.1-5

Эксперт должен изучить составленный ОО, чтобы определить, что он был установлен должным образом и находится в известном режиме.

Будут применены операции ATE_IND.2-1 и ATE_IND.2-2 к составленному ОО, чтобы определить, что составленный ОО был установлен должным образом и находится в известном режиме.

14.6.1.3.6 Операция ACO_CTT.1-6

Эксперт должен изучить совокупность ресурсов, предоставленных разработчиком, чтобы определить, что они эквивалентны совокупности ресурсов, используемых разработчиком базового компонента для того, чтобы функционально проверить базовый компонент.

Будет применена операция ATE_IND.2-3, чтобы определить, что совокупность предоставленных ресурсов эквивалентна используемым, для того чтобы функционально проверить базовый компонент, который используется в составленном ОО.

14.6.1.4 Действие ACO_CTT.1.2E

14.6.1.4.1 Операция ACO_CTT.1-7

Эксперт должен выполнить тестирование в соответствии с ATE_IND.2.2E, для подмножества ТФБ, определенного в составленном задании по безопасности, чтобы проверить результаты тестирования разработчика.

Эксперт должен применить все операции, необходимые для удовлетворения ATE_IND.2.2E, сообщающие в ТОО для составленного ОО все анализы, результаты и заключения как продиктовано сопутствующими операциями.

14.6.1.5 Действие ACO_CTT.1.3E

14.6.1.5.1 Операция ACO_CTT.1-8

Эксперт должен выполнить тестирование в соответствии с ATE_IND.2.3E, для подмножества ТФБ, определенного в составленном задании по безопасности, чтобы подтвердить, что ФБО работает так, как определено.

Эксперт должен применить все операции, необходимые для удовлетворения ATE_IND.2.3E, сообщающие в ТОО для составленного ОО все анализы, результаты и заключения как продиктовано операциями.

Выбирая для тестирования интерфейсы ФБО составленного ОО, эксперт должен принять во внимание любые модификации компонентов из оцененной версии или конфигурации. Модификации компонентов из оцененного, могут включать введенные исправления, различную конфигурацию, в результате измененной руководящей документации, степень использования дополнительной части компонента, которая не была в пределах компонента ФБО.

Данные модификации будут идентифицированы во время деятельности по составлению обоснования (ACO_COR).

14.6.2 Оценка подвида деятельности (ACO_CTT.2)

14.6.2.1 Цели

Цель данной подвида деятельности состоит в том, чтобы определить, правильно ли разработчик выполнял и регистрировал тесты для каждого интерфейса базового компонента, на который полагается зависимый компонент. Как часть данного определения эксперт повторяет выборку тестов, выполненных разработчиком, и выполняет любые дополнительные тесты, требуемые, чтобы полностью продемонстрировать ожидаемый режим работы составленного ОО и интерфейсов базового компонента, на который полагается зависимый компонент.

14.6.2.2 Исходные данные

Данными оценки для этой подвида деятельности являются:

а) составленный ОО, подходящий для тестирования;

б) составленный ОО, проверяющий данные;

в) достоверная информация;

г) информация разработки.

15.6.2.3 Действие ACO_CTT.2.1E

СТ РК ИСО/МЭК 15408-3 ACO_CTT.2.1C: составленный ОО и документация тестирования интерфейса базового компонента должны состоять из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования.

14.6.2.3.1 Операция ACO_CTT.2-1

Эксперт должен изучить тестовую документацию составленного ОО, чтобы установить, что она состоит из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования.

Данная операция может быть удовлетворена предоставлением доказательства тестирования оценки зависимого компонента, если использовался базового компонент, чтобы удовлетворить требования для ИТ в операционной среде зависимого компонента.

Будут применены все операции, необходимые для удовлетворения ATE_FUN.1.1E для того, чтобы определить:

а) что тестовая документация состоит из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования;

б) что тестовая документация содержит информацию, необходимую для того, чтобы гарантировать, что тесты могут быть воспроизведены повторно;

в) уровень усилия разработчика, который был применен для тестирования базового компонента.

14.6.2.3.2 Операция ACO_CTT.2-2

Эксперт должен изучить тестовую документацию интерфейса базового компонента, чтобы установить, что она состоит из планов проведения

тестирования, ожидаемых результатов тестирования и фактических результатов тестирования.

Данная операция может быть удовлетворена предоставлением доказательства тестирования оценки базового компонента, для тех интерфейсов, на которые полагаются в составленном ОО зависимым компонентом, ФБОI успешно оцененного базового компонента.

Определение того, были ли интерфейсами базового компонента те, на который полагается зависимый компонент, фактически оцененного базового компонента ИФБО, сделано во время деятельности ACO_COR.

Будут применены все операции, необходимые для удовлетворения ATE_FUN.1.1E для того, чтобы определить:

а) что тестовая документация состоит из планов проведения тестирования, ожидаемых результатов тестирования и фактических результатов тестирования;

б) что тестовая документация содержит информацию, необходимую для того, чтобы гарантировать, что тесты могут быть воспроизведены повторно;

в) уровень усилия разработчика, который был применен для тестирования базового компонента.

Тестовая документация по выполнению разработчиком тестов составленного ОО должна продемонстрировать, что ФБО ведет себя так, как определено и завершен.

14.6.2.3.3 Операция ACO_CTT.2-3

Эксперт должен изучить тестовую документацию, чтобы установить, что она обеспечивает точное соотношение между тестами в документации тестирования, касающейся тестирования составленного ОО и ТФБ составленного ОО в задании по безопасности составленного ОО.

Простая перекрестная таблица может быть достаточной, чтобы показать соотношение тестирования. Идентификация соотношения между тестами и ТФБ, представленные в документации тестирования, должна быть точно выраженной.

14.6.2.3.4 Операция ACO_CTT.2-4

Эксперт должен изучить тестовую документацию, чтобы установить, что выполнение разработчиком тестов составленного ОО демонстрирует, что ФБО ведет себя так, как определено.

Руководство по данной операции находится в п. 12.2.1 и п. 12.2.2.

Выводы успешного выполнения тестов, как определено для ATE_FUN.1.3C, могут быть сравнены с графическим отображением, чтобы определить, что ТФБ составленного ОО, проверенного разработчиком, ведет себя, как и ожидается.

Тестовая документация по выполнению разработчиком тестов интерфейса базового компонента должна продемонстрировать, что

интерфейс базового компонента, на который полагается зависимый компонент, ведет себя так, как определено и завершен.

14.6.2.3.5 Операция ACO_CTT.2-5

Эксперт должен изучить тестовую документацию, чтобы установить, что она обеспечивает точное соотношение между тестами в документации тестирования, касающейся тестирования интерфейсов базового компонента, на которые полагается зависимый компонент и интерфейсы, определенные в источниках достоверной информации.

Может быть достаточно простой перекрестной таблицы, чтобы показать соотношение тестирования. Идентификация соотношения между тестами и интерфейсами, представленными в документации тестирования, должна быть точно выраженной.

14.6.2.3.6 Операция ACO_CTT.2-6

Эксперт должен изучить тестовую документацию, чтобы установить, что выполнение разработчиком тестов интерфейса базового компонента демонстрирует, что интерфейсы базового компонента, на которые полагается зависимый компонент, ведут себя, как и определено.

Руководство по данной операции находится в п. 12.2.1 и п. 12.2.2.

Выводы из успешного выполнения тестов как оценено для ATE_FUN.1.3C могут быть сравнены с графическим отображением, чтобы определить, что интерфейсы базового компонента, проверенные разработчиком, ведут себя, как и ожидается.

Базовый компонент должен быть подходящим для тестирования.

14.6.2.3.7 Операция ACO_CTT.2-7

Эксперт должен изучить составленный ОО, чтобы определить, что он был установлен должным образом и находится в известном режиме.

Будут применены операции ATE_IND.2-1 и ATE_IND.2-2 к ОО, предоставленному разработчиком для тестирования, чтобы определить, что составленный ОО был установлен должным образом и находится в известном режиме.

14.6.2.3.8 Операция ACO_CTT.2-8

Эксперт должен изучить совокупность ресурсов, предоставленных разработчиком, чтобы установить, что они эквивалентны совокупности ресурсов, используемых разработчиком базового компонента для того, чтобы функционально проверить базовый компонент.

Будет применена операция ATE_IND.2-3, чтобы установить, что совокупность предоставленных ресурсов эквивалентна используемым для того, чтобы функционально проверить базовый компонент который используется в составленном ОО.

14.6.2.4 Действие ACO_CTT.2.2E

14.6.2.4.1 Операция ACO_CTT.2-9

Тесты должны быть выбраны и выполнены в соответствии с ATE_IND.2.2E, чтобы продемонстрировать правильный режим работы ТФБ, определенного в задании по безопасности составленного ОО.

Эксперт применит все операции, необходимые для удовлетворения ATE_IND.2.2E, сообщающие в ТОО для составленного ОО все анализы, результаты и заключения как продиктовано сопутствующими операциями.

14.6.2.5 Действие ACO_CTT.2.3E

14.6.2.5.1 Операция ACO_CTT.2-10

Эксперт должен выполнить тестирование в соответствии с ATE_IND.2.3E, для подмножества ТФБ, определенного в составленном задании по безопасности, подтвердить, что ФБО работает так, как определено.

Эксперт применит все операции, необходимые для удовлетворения ATE_IND.2.3E, сообщающие в ТОО для составленного ОО все анализы, результаты и заключения как продиктовано сопутствующими операциями.

Выбирая интерфейсы ФБО составленного ОО для тестирования, эксперт должен принять во внимание любые модификации компонентов из оцененной версии или конфигурации. Модификации компонентов из оцененного могут включать введенные исправления, различную конфигурацию в результате измененной документации руководства, уверенность в том, что дополнительная часть компонента, не находиться внутри компонента ФБО.

Данные модификации будут идентифицированы во время деятельности по составлению обоснования (ACO_COR).

14.6.2.5.2 Операция ACO_CTT.2-11

Эксперт должен выполнить тестирование, в соответствии с оценкой подвида деятельности (ATE_IND.2), для подмножества интерфейсов до основного компонента, чтобы подтвердить, что они работают так, как определено.

Эксперт применит все операции, необходимые для удовлетворения ATE_IND.2.3E, сообщающие в ТОО для составленного ОО все анализы, результаты и заключения, как продиктовано сопутствующими операциями.

Выбирая интерфейсы базового компонента для тестирования, эксперт должен принять во внимание любые модификации базовых компонентов из оцененной версии или конфигурации. В частности эксперт должен полагать, что разработка тестов демонстрирует правильное поведение интерфейсов базового компонента, которые не рассмотрели во время оценки базового компонента. Эти дополнительные интерфейсы и другие модификации базового компонента будут идентифицированы во время деятельности по составлению обоснования (ACO_COR).

14.7 Составление анализа уязвимости (ACO_VUL)

14.7.1 Оценка подвида деятельности (ACO_VUL.1)

14.7.1.1 Цели

Цель данной подвида деятельности состоит в том, чтобы определить, имеется ли легко используемая уязвимость у составленного ОО, в его операционной среде.

Разработчик предоставляет детали любых остаточных уязвимостей, представленных из оценки компонентов. Эксперт выполняет анализ диспозиции переданной остаточной уязвимости, а также выполняет осмотр общего домена, чтобы идентифицировать любую новую потенциальную уязвимость в компонентах (то есть те проблемы в общественном пользовании, о которых сообщили, начиная с оценки базового компонента). Эксперт затем выполняет тестирование преодоления защиты, чтобы продемонстрировать, что потенциальная уязвимость не может использоваться взломщиком с основными атакующими возможностями в ОО, в его операционной среде.

14.7.1.2 Исходные данные

Данными оценки для этой подвида деятельности являются:

а) составной ОО, подходящий для тестирования;

б) составленное ЗБ;

в) составление обоснования;

г) руководящая документация;

д) общедоступная информация для поддержки идентификации возможной уязвимости безопасности;

е) остаточная уязвимость, представленная во время оценки каждого компонента.

14.7.1.3 Замечания по применению

См. примечания по применению для оценки подвида деятельности (AVA_VAN.1).

14.7.1.4 Действие ACO_VUL.1.1E

составленный ОО должен быть подходящим для тестирования.

14.7.1.4.1 Операция ACO_VUL.1-1

Эксперт должен изучить составленный ОО, чтобы определить, что он был установлен должным образом и находится в известном режиме.

Будут применены к составленному ОО операции ATE_IND.2-1 и ATE_IND.2-2, чтобы определить, что составленный ОО был установлен должным образом и находится в известном режиме.. Если пакет гарантии включает компонент из семейства ACO_CTT, то эксперт может обратиться к результату операции ACO_CTT*-1, чтобы продемонстрировать, что данное условие было удовлетворено.

14.7.1.4.2 Операция ACO_VUL.1-2

Эксперт должен изучить конфигурацию составленного ОО, чтобы установить, что любые предположения и цели в компонентах ЗБ, касающиеся объектов ИТ, выполнены другими компонентами.

ЗБ для компонента может включать предположения о других компонентах, которые может использовать компонент, с которым ЗБ имеет отношение, например ЗБ для используемой операционной системы, поскольку базовый компонент может включать предположение, что любые приложения, загруженные в операционную систему, не работают в привилегированном режиме. Эти предположения и цели должны быть выполнены другими компонентами в составленном ОО.

14.7.1.5 Действие ACO_VUL.1.2E

14.7.1.5.1 Операция ACO_VUL.1-3

Эксперт должен изучить остаточные уязвимости из оценки базового компонента, чтобы установить, что они не являются пригодными для использования в составленном ОО, в его операционной среде.

Список уязвимостей, идентифицированных в продукте во время оценки базового компонента, продемонстрировавшие непригодность для использования в базовом компоненте, должен использоваться как внесение в эту деятельность. Эксперт определит, что предпосылка (ки), по которой уязвимость, как посчитали, была непригодной для использования, есть в составном ОО, или имеет ли комбинации повторно введенную потенциальную уязвимость. Например, если бы во время оценки базового компонента предполагалось, что специфический сервис операционной системы, который задействован в оценке составного ОО, был бы заблокирован, то любую потенциальную уязвимость, касающуюся того сервиса, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки базового компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, зависимого компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в изоляции, является пригодной для использования, когда интегрирована с объектом ИТ, содержащим другую потенциальную уязвимость.

14.7.1.5.2 Операция ACO_VUL.1-4

Эксперт должен изучить остаточные уязвимости из оценки зависимого компонента, чтобы установить, что они не являются пригодными для использования в составном ОО, в его операционной среде.

Список уязвимостей, идентифицированный в продукте во время оценки зависимого компонента, продемонстрировавшие непригодность для использования в зависимом компоненте, должен использоваться как

внесение в эту деятельность. Эксперт определит, что предпосылка (ки), по которой уязвимость, как посчитали, была непригодной для использования, имеется в составном ОО, или имеет ли комбинации повторно введенную потенциальную уязвимость. Например, если бы во время оценки зависимого компонента предполагалось, что ИТ, отвечающая операционным требованиям среды, не будет возвращать определенное значение в ответ на запрос сервиса, который предоставлен базовым компонентом в оценке составленного ОО, то любую потенциальную уязвимость, касающуюся того возвращаемого значения, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки зависимого компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, базового компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в изоляции, является пригодной для использования во время интегрирования с объектом ИТ, содержащий другую потенциальную уязвимость.

14.7.1.6 Действие ACO_VUL.1.3E

14.7.1.6.1 Операция ACO_VUL.1-5

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в базовом компоненте, которая стала известной, начиная с завершения оценки базового компонента.

Эксперт будет использовать информацию в общем домене, как описано в AVA_VAN.1-2 для того, чтобы найти уязвимость в базовом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки базового компонента, не должна быть далее изучена, если для эксперта не очевидно, что возможность атаки, требуемая взломщиком для использования потенциальной уязвимости, была значительно уменьшена. Это может быть через внедрение некоторых новых технологий, начиная с оценки базового компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.1.6.2 Операция ACO_VUL.1-6

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в зависимом компоненте, которая стала известной, начиная с завершения оценки зависимого компонента.

Эксперт будет использовать информацию в общем домене, как описано в AVA_VAN.1-2, чтобы найти уязвимость в зависимом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки зависимого компонента, не должна быть далее изучена, если для

эксперта не очевидно, что возможность атаки, требуемая взломщиком для использования потенциальной уязвимости, была значительно уменьшена.. Это может быть через внедрение некоторых новых технологий, начиная с оценки зависимого компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.1.6.3 Операция ACO_VUL.1-7

Эксперт должен сделать запись идентифицированных потенциальных уязвимостей безопасности в ТОО, которые являются кандидатами на тестирование и применимы к составленному ОО, в его операционной среде.

ЗБ, руководящая документация, и функциональная спецификация используются, чтобы определить, относится ли уязвимость к составному ОО в его операционной среде.

Эксперт делает запись любых оснований для исключения уязвимости из дальнейшего рассмотрения, если эксперт определит, что уязвимость не применима в операционной среде. Иначе эксперт делает запись потенциальной уязвимости для дальнейшего рассмотрения.

Список потенциальных уязвимостей, применимые к составному ОО в его операционной среде, который может использоваться как вклад в тестовые действия преодоления защиты (то есть ACO_VUL.1.4E), будет передан экспертами в ТОО.

14.7.1.7 Действие ACO_VUL.1.4E

14.7.1.7.1 Операция ACO_VUL.1-8

Эксперт должен провести тестирование преодоления защиты, как подробно рассказано для AVA_VAN.1.3E.

Эксперт применит все операции, необходимые для удовлетворения действия эксперта AVA_VAN.1.3E, передавая в ТОО для составленного ОО все анализы и заключения, как продиктовано операциями.

Эксперт будет также применять операции для действия эксперта AVA_VAN.1.1E, чтобы определить, что составленный ОО, предоставленный разработчиком, является подходящим для тестирования.

14.7.2 Оценка подвида деятельности (ACO_VUL.2)

14.7.2.1 Цели

Цель данной подвида деятельности состоит в том, чтобы определить, есть ли у составленного ОО, в его операционной среде, уязвимость, пригодная для использования взломщиками, обладающими основным потенциалом атаки.

Разработчик предоставляет анализ диспозиции любых остаточных уязвимостей, полученных для компонентов и любых уязвимостей, внедренных через комбинацию базового и зависимого компонентов. Эксперт осуществляет осмотр общего домена, чтобы идентифицировать любую новую потенциальную уязвимость в компонентах (то есть те проблемы в общем домене, которые получены, начиная с завершения оценки

компонентов). Эксперт также выполнит независимый анализ уязвимости составленного ОО и тестирование преодоления защиты.

14.7.2.2 Исходные данные

Данными оценки для этой подвида деятельности являются:

а) составленный ОО подходящий для тестирования;

б) составное ЗБ;

в) составление обоснования;

г) достоверная информация;

д) руководящая документация;

е) публично доступная информация, чтобы поддержать идентификацию возможной уязвимости безопасности;

ж) остаточные уязвимости, переданные во время оценки каждого компонента.

14.7.2.3 Замечания по применению

См. примечания по применению для оценки подвида деятельности (AVA_VAN.2).

14.7.2.4 Действие ACO_VUL.2.1E

Составленный ОО должен быть подходящим для тестирования.

14.7.2.4.1 Операция ACO_VUL.2-1

Эксперт должен изучить составленный ОО, чтобы определить, что он был установлен должным образом и находится в известном режиме.

Будут применены к составному ОО операции ATE_IND.2-1 и ATE_IND.2-2 для определения, что составной ОО был установлен должным образом и находится в известном режиме.

Если пакет гарантии включает семейство ACO_CTT, то эксперт может сослаться на результат тестирования операции составленного ОО (ACO_CTT) *-1, чтобы продемонстрировать, что данное условие было удовлетворено.

14.7.2.4.2 Операция ACO_VUL.2-2

Эксперт должен изучить конфигурацию составленного ОО, чтобы определить, что любые предположения и цели в компонентах ЗБ, касающиеся объектов ИТ, выполнены другими компонентами.

ЗБ для компонента может включать предположения о других компонентах, которые может использовать компонент, с которым ЗБ имеет отношение, например ЗБ для используемой операционной системы, поскольку базовый компонент может включать предположение, что любые приложения, загруженные в операционную систему, не работают в привилегированном режиме. Эти предположения и цели должны быть выполнены другими компонентами в составном ОО.

14.7.2.5 Действие ACO_VUL.2.2E

14.7.2.5.1 Операция ACO_VUL.2-3

Эксперт должен изучить остаточные уязвимости из оценки базового компонента, чтобы установить, что они не являются пригодными для использования в составном ОО, в его операционной среде.

Список уязвимостей, идентифицированный в продукте во время оценки базового компонента, продемонстрировавшие непригодность в использовании в базовом компоненте, должен использоваться как вклад в эту деятельность. Эксперт определит, что предпосылка (ки), по которой уязвимость, как посчитали, была непригодной для использования, имеется в составном ОО, или имеет ли комбинации повторно введенную потенциальную уязвимость. Например, если бы во время оценки базового компонента предполагалось, что специфический сервис операционной системы, который задействован в оценке составленного ОО, был бы заблокирован, то любую потенциальную уязвимость, касающуюся того сервиса, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки базового компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, зависимого компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в изоляции, является пригодной для использования, когда интегрирована с объектом ИТ, содержащим другую потенциальную уязвимость.

14.7.2.5.2 Операция ACO_VUL.2-4

Эксперт должен изучить остаточные уязвимости из оценки зависимого компонента, чтобы установить, что они не являются пригодными для использования в составном ОО, в его операционной среде.

Список уязвимостей, идентифицированный в продукте во время оценки зависимого компонента, продемонстрировавшие непригодность в использовании в зависимом компоненте, должен использоваться как вклад в эту деятельность. Эксперт определит, что предпосылка (ки), по которой уязвимость, как посчитали, была непригодной для использования, поддержана в составном ОО, или имеет ли комбинации повторно введеную потенциальную уязвимость. Например, если бы во время оценки зависимого компонента предполагалось, что ИТ, отвечающая операционным требованиям среды, не будет возвращать определенное значение в ответ на запрос сервиса, который предоставлен базовым компонентом в оценке составленного ОО, то любую потенциальную уязвимость, касающуюся того возвращаемого значения, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки зависимого компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, базового компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в изоляции, является пригодной для использования во время интегрирования с объектом ИТ, содержащий другую потенциальную уязвимость.

14.7.2.6 Действие ACO_VUL.2.3E

14.7.2.6.1 Операция ACO_VUL.2-5

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в зависимом компоненте, которая стала известной, начиная с завершения оценки базового компонента.

Эксперт будет использовать информацию общего пользования, как описано в AVA_VAN.1-2, чтобы найти уязвимость в базовом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки базового компонента, не должна быть далее изучена, если для эксперта не очевидно, что возможность атаки, требуемая взломщиком для использования потенциальной уязвимости, была значительно уменьшена. Это может быть через внедрение некоторых новых технологий, начиная с оценки базового компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.2.6.2 Операция ACO_VUL.2-6

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в зависимом компоненте, которая стала известной, начиная с завершения оценки зависимого компонента.

Эксперт будет использовать информацию в общем домене, как описано в AVA_VAN.1-2, чтобы найти уязвимость в зависимом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки зависимого компонента, не должна быть далее изучена, если для эксперта не очевидно, что возможность атаки, требуемая взломщиком для использования потенциальной уязвимости, была значительно уменьшена. Это может быть через внедрение некоторых новых технологий, начиная с оценки зависимого компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.2.6.3 Операция ACO_VUL.2-7

Эксперт должен сделать запись идентифицированных потенциальных уязвимостей безопасности в ТОО, которые являются кандидатами на тестирование и применимы к составленному ОО, в его операционной среде.

ЗБ, руководящая документация, и функциональная спецификация используются, чтобы определить, относится ли уязвимость к составленному ОО в его операционной среде.

Эксперт делает запись любых оснований для исключения уязвимости из дальнейшего рассмотрения, если эксперт определит, что уязвимость не применима в операционной среде. Иначе эксперт делает запись потенциальной уязвимости для дальнейшего рассмотрения.

Список потенциальных уязвимостей, применимые к составленному ОО в его операционной среде, который может использоваться как вклад в преодоление защиты, действиями тестирования (то есть ACO_VUL.1.4E), будет передан экспертами в ТОО.

14.7.2.7 Действие ACO_VUL.2.4E

14.7.2.7.1 Операция ACO_VUL.2-8

Эксперт должен провести осмотр ЗБ, руководящей документации, достоверной информации и составление обоснования составленного ОО, чтобы идентифицировать возможную уязвимость безопасности в составленном ОО.

Рассмотрение компонентов составленного ОО в независимом анализе уязвимости примет немного другую форму в отличие от зарегистрированной в AVA_VAN.2.3E для оценки компонента, поскольку оно не будет обязательно учитывать все уровни абстракции разработки, относящиеся к пакету достоверности. Их уже рассмотрят во время оценки компонентов, но сведения не могут быть доступными для оценки составленного ОО. Однако, общий подход, описанный в операциях, связанных с AVA_VAN.2.3E, применим и должен сформировать основание из поиска экспертом потенциальной уязвимости в составленном ОО.

Анализ уязвимости индивидуальных компонентов, используемых в составленном ОО, будет уже выполнен во время оценки индивидуальных компонентов. Фокус анализа уязвимости во время оценки составленного ОО должен идентифицировать любую уязвимость, внедренную в результате интеграции компонентов или из-за любых изменений в использовании компонентов между конфигурацией оцененного компонента относительно конфигурации составленного ОО.

Эксперт будет использовать понимание конструкции компонента как детализировано в достоверной информации для зависимого компонента, и информация разработки и составлении обоснования для базового компонента, вместе с зависимым компонентом проектируют информацию. Данная информация позволит эксперту получить понимание того, как базовый компонент и зависимый компонент взаимодействуют и идентифицируют потенциальную уязвимость, которая может быть внедрена в результате этого взаимодействия.

Эксперт будет рассматривать любое новое руководство, предусмотренное для установки, запуска и деятельности составленного ОО, чтобы идентифицировать любую потенциальную уязвимость, внедренную через данное пересмотренное руководство.

Если любой из индивидуальных компонентов был через действия непрерывности достоверности, начиная с завершения оценки компонента, то эксперт рассмотрит исправление (я) в независимом анализе уязвимости.

Информация, связанная с изменением, предоставленным в открытом отчете действий непрерывности достоверности (например, отчёт о результатах технического обслуживания), будет основным источником входного материала для изменения. Это будет дополнено любыми обновлениями руководящей документации, получающейся из изменения и любой информации относительно изменения, доступной в общем пользовании, например вебсайт производителя.

Любые риски, идентифицированные из-за нехватки данных для установления полного воздействия любых исправлений, или отклонений в конфигурации компонента от оцененной конфигурации должны быть зарегистрированы в анализе уязвимости эксперта.

14.7.2.8 Действие ACO_VUL.2.5E

14.7.2.8.1 Операция ACO_VUL.2-9

Эксперт должен провести тестирование преодоления защиты, как подробно рассказано для AVA_VAN.2.4E.

Эксперт должен применить все операции, необходимые для удовлетворения действия эксперта AVA_VAN.2.4E, сообщающего в ТОО для составленного ОО все анализы и заключения как продиктовано операциями.

Эксперт будет также применять операции для действия эксперта AVA_VAN.2.1E, чтобы определить, что составленный ОО, предоставленный разработчиком, является подходящим для тестирования.

14.7.3 Оценка подвида деятельности (ACO_VUL.3)

14.7.3.1 Цели

Цель данной подвида деятельности состоит в том, чтобы определить, есть ли у составленного ОО, в его операционной среде, уязвимость, пригодная для использования взломщиками, обладающими улучшенным потенциалом атаки.

Разработчик предоставляет анализ диспозиции любых остаточных уязвимостей, полученных для компонентов и любых уязвимостей, внедренных через комбинацию базового и зависимого компонентов. Эксперт осуществляет осмотр общего домена, чтобы идентифицировать любые новые потенциальные уязвимости в компонентах (то есть те проблемы в общем домене, которые получены, начиная с завершения оценки компонентов). Эксперт также выполнит независимый анализ уязвимости составленного ОО и тестирование преодоления защиты.

14.7.3.2 Исходные данные

Данными оценки для данной подвида деятельности являются:

а) составленный ОО, подходящий для тестирования;

б) составленное ЗБ;

в) составление обоснования;

г) достоверная информация;

д) руководящая документация;

е) публично доступная информация для поддержки идентификацию возможной уязвимости безопасности;

ж) остаточные уязвимости, переданные во время оценки каждого компонента.

14.7.3.3 Замечания по применению

См. примечания по применению для оценки подвида деятельности (AVA_VAN.3).

14.7.3.4 Действие ACO_VUL.3.1E

Составленный ОО должен быть подходящим для тестирования

14.7.3.4.1 Операция ACO_VUL.3-1

Эксперт должен изучить составленный ОО, чтобы определить, что он был установлен должным образом и находится в известном режиме.

Будут применены операции ATE_IND.2-1 и ATE_IND.2-2 к составленному ОО, чтобы определить, что составленный ОО был установлен должным образом и находится в известном режиме.

Если пакет гарантии включает семейство ACO_CTT, то эксперт может сослаться на результат тестирования операции составленного ОО (ACO_CTT) -один, чтобы продемонстрировать, что данное условие было удовлетворено.

14.7.3.4.2 Операция ACO_VUL.3-2

Эксперт должен изучить конфигурацию составленного ОО, чтобы определить что любые предположения и цели в компонентах ЗБ, касающиеся объектов ИТ, выполнены другими компонентами.

ЗБ для компонента может включать предположения о других компонентах, которые могут использовать компонент, с которым ЗБ имеет отношение, например ЗБ для используемой операционной системы, поскольку базовый компонент может включать предположение, что любые приложения, загруженные в операционную систему, не работают в привилегированном режиме. Эти предположения и цели должны быть выполнены другими компонентами в составленном ОО.

14.7.3.5 Действие ACO_VUL.3.2E

14.7.3.5.1 Операция ACO_VUL.3-3

Эксперт должен изучить остаточные уязвимости из оценки базового компонента, чтобы установить, что они не являются пригодными для использования в составленном ОО, в его операционной среде.

Список уязвимостей, идентифицированных в продукте во время оценки базового компонента, продемонстрировавших непригодность для использования в базовом компоненте, должен использоваться как вклад в эту деятельность. Эксперт определит, что предпосылка(ки), по которой уязвимость, как посчитали, была непригодной для использования, поддержана в составленном ОО, или имеет ли комбинации повторно введенную потенциальную уязвимость. Например, если бы во время оценки базового компонента предполагалось, что специфический сервис операционной системы, который задействован в оценке составленного ОО, был бы заблокирован, то любую потенциальную уязвимость, касающуюся того сервиса, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки базового компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, зависимого компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в изоляции, является пригодной для использования когда интегрирована с объектом ИТ, содержащим другую потенциальную уязвимость.

14.7.3.5.2 Операция ACO_VUL.3-4

Эксперт должен изучить остаточные уязвимости из оценки зависимого компонента, чтобы установить, что они не являются пригодными для использования в составном ОО, в его операционной среде.

Список уязвимостей, идентифицированных в продукте во время оценки зависимого компонента, продемонстрировавших непригодность для использования в зависимом компоненте, должен использоваться как вклад в эту деятельность. Эксперт определит, что предпосылка(ки), по которой уязвимость, как посчитали, была непригодной для использования, поддержана в составном ОО, или имеет ли комбинации повторно введенную потенциальную уязвимость. Например, если бы во время оценки зависимого компонента предполагалось, что ИТ, отвечающая операционным требованиям среды, не будет возвращать определенное значение в ответ на запрос сервиса, который предоставлен базовым компонентом в оценке составленного ОО, то любую потенциальную уязвимость, касающуюся того возвращаемого значения, выбранного ранее, необходимо теперь рассмотреть.

Кроме того, этот список известной, непригодной для использования уязвимости, полученной из оценки зависимого компонента, необходимо рассмотреть в индикаторе любой известной, непригодной для использования уязвимости для других компонентов (например, базового компонента) в пределах составленного ОО. Необходимо рассмотреть случай, где потенциальная уязвимость, являющаяся непригодной для использования в

изоляции, является пригодной для использования во время интегрирования с объектом ИТ, содержащий другую потенциальную уязвимость.

14.7.3.6 Действие ACO_VUL.3.3E

14.7.3.6.1 Операция ACO_VUL.3-5

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в базовом компоненте, которая стала известной, начиная с завершения оценки базового компонента.

Эксперт должен использовать информацию в общем домене, как описано в AVA_VAN.3-2 для того, чтобы отыскать уязвимость в базовом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки базового компонента, не должна быть далее изучена, если для эксперта не очевидно, что потенциал атаки, требуемый взломщиком для использования потенциальной уязвимости, был значительно уменьшен. Это может быть через внедрение некоторых новых технологий, начиная с оценки базового компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.3.6.2 Операция ACO_VUL.3-6

Эксперт должен изучить публично доступные источники информации, чтобы поддержать идентификацию возможной уязвимости безопасности в зависимом компоненте, которая стала известной, начиная с завершения оценки зависимого компонента.

Эксперт должен использовать информацию в общем домене, как описано в AVA_VAN.3-2 для того, чтобы отыскать уязвимость в зависимом компоненте.

Та потенциальная уязвимость, которая была публично доступна до оценки зависимого компонента, не должна быть далее изучена, если для эксперта не очевидно, что потенциал атаки, требуемый взломщиком для использования потенциальной уязвимости, был значительно уменьшен. Это может быть через внедрение некоторых новых технологий, начиная с оценки зависимого компонента, которые означают, что использование потенциальной уязвимости было упрощено.

14.7.3.6.3 Операция ACO_VUL.3-7

Эксперт должен сделать запись идентифицированных потенциальных уязвимостей безопасности в ТОО, которые являются кандидатами на тестирование и применимы к составленному ОО, в его операционной среде.

ЗБ, руководящая документация, и функциональная спецификация используются, чтобы определить, относится ли уязвимость к составленному ОО в его операционной среде.

Эксперт делает запись любых оснований для исключения уязвимости из дальнейшего рассмотрения, если эксперт определит, что уязвимость не

применима в операционной среде. Иначе эксперт делает запись потенциальной уязвимости для дальнейшего рассмотрения.

Список потенциальных уязвимостей, применимые к составленному ОО в его операционной среде, который может использоваться как вклад в преодоление защиты, действиями тестирования (то есть ACO_VUL.1.4E), будет передан экспертами в ТОО.

14.7.3.7 Действие ACO_VUL.3.4E

14.7.3.7.1 Операция ACO_VUL.3-8

Эксперт должен провести изучение ЗБ, руководящей документации, достоверной информации и составление обоснования составленного ОО, чтобы идентифицировать возможную уязвимость безопасности в составленном ОО.

Рассмотрение компонентов составленного ОО в независимом анализе уязвимости примет немного другую форму в отличие от зарегистрированной в AVA_VAN.3.3E для оценки компонента, поскольку оно не будет обязательно учитывать все уровни абстракции разработки, относящиеся к пакету достоверности. Их уже рассмотрят во время оценки компонентов, но сведения не могут быть доступными для оценки составленного ОО. Однако, общий подход, описанный в операциях, связанных с AVA_VAN.3.3E, применим и должен сформировать основание из поиска экспертом потенциальной уязвимости в составленном ОО.

Анализ уязвимости индивидуальных компонентов, используемых в составленном ОО, будет уже выполнен во время оценки индивидуальных компонентов. Фокус анализа уязвимости во время оценки составленного ОО должен идентифицировать любую уязвимость, внедренную в результате интеграции компонентов или из-за любых изменений в использовании компонентов между конфигурацией компонента, определенного во время оценки компонента и конфигурации составленного ОО.

Эксперт будет использовать понимание конструкции компонента, как подробно описано в достоверной информации для зависимого компонента, и информация разработки и составлении обоснования для базового компонента, вместе с зависимым компонентом проектируют информацию. Данная информация позволит эксперту получить понимание того, как базовый компонент и зависимый компонент взаимодействуют.

Эксперт будет рассматривать любое новое руководство, предусмотренное для установки, запуска и деятельности составленного ОО, чтобы идентифицировать любую потенциальную уязвимость, внедренную через данное пересмотренное руководство.

Информация, связанная с изменением действий непрерывной достоверности, представлена в открытом отчете (например, отчёт о результатах технического обслуживания). Это будет дополнено любыми обновлениями руководящей документации, получающейся из изменения и

любой информации относительно изменения, доступной в общем пользовании, например вебсайт производителя.

Любые риски, идентифицированные из-за нехватки данных для установления полного воздействия любых исправлений, или отклонений в конфигурации компонента от оцененной конфигурации должны быть зарегистрированы в анализе уязвимости эксперта.

14.7.3.8 Действие ACO_VUL.3.5E

14.7.3.8.1 Операция ACO_VUL.3-9

Эксперт должен провести тестирование преодоления защиты, как подробно описано для AVA_VAN.3.4E.

Эксперт должен применить все операции, необходимые для удовлетворения действия эксперта AVA_VAN.3.4E, сообщающего в ТОО для составленного ОО все анализы и заключения, как продиктовано операциями.

Эксперт будет также применять операции для действия эксперта AVA_VAN.3.1E, чтобы определить, что составленный ОО, предоставленный разработчиком, является подходящим для тестирования.

Приложение А
(информационное)

Общие указания по оценке

А.1 Цели

Цель данного раздела состоит в том, чтобы охватить общие вопросы руководства обеспечением технического подтверждения результатов оценки. Использование такого общего руководства помогает достичь объективности, повторяемости и воспроизводимости работы, выполненной оценщиком.

А.2 Выборка

Данное Приложение содержит общие указания по осуществлению выборки. Конкретная и подробная информация дана в тех операциях, соответствующих определенным элементам действий оценщика, где выборку необходимо выполнить. Выборка – определенная процедура, выполняемая оценщиком, посредством которой некоторое подмножество требуемой совокупности свидетельств оценки исследуется и полагается репрезентативным (представительным) для совокупности в целом. Это позволяет оценщику получить достаточную уверенность в правильности конкретного свидетельства оценки без его анализа в полном объеме.

Выборка производится для экономии ресурсов при поддержании адекватного уровня доверия. Выборка из свидетельства может приводить к двум возможным результатам.

а) На подмножестве не обнаружено никаких ошибок, что дает оценщику определенную уверенность в том, что совокупность в целом корректна;

б) На подмножестве найдены ошибки, и поэтому правильность совокупности в целом подвергается сомнению. Даже устранение всех обнаруженных ошибок может оказаться недостаточным для получения оценщиком необходимой уверенности, и поэтому оценщику придется либо увеличить размер подмножества, либо прекратить использование выборки для этого конкретного свидетельства.

Выборка — это метод, который может использоваться для получения заслуживающих доверия выводов, когда состав свидетельства относительно однороден по существу, например, если свидетельство является результатом полностью определенного процесса.

Выборка в случаях, указанных в ОК или специально оговоренных в операциях, признается как рентабельный подход к действиям, выполняемым оценщиком. Выборка в других областях разрешается только в исключительных случаях, там, где выполнение конкретного вида деятельности в целом потребовало бы усилий, непропорциональных другим видам деятельности, и где оно не повысило бы соответственно доверие. В

таких случаях потребуется обоснование применения выборки в этой области. Ни тот факт, что ОО является объемным и сложным, ни то, что он имеет много функциональных требований безопасности, не является достаточным обоснованием, так как при оценке объемных и сложных ОО как раз и могут потребоваться большие усилия. Скорее предполагается, что это исключение ограничивается такими случаями, когда подход к разработке ОО дает большое количество материала для конкретного требования ОК, который обычно весь требуется проверить или исследовать, и когда не ожидается, что такое действие повысит соответственно степень доверия.

Выборка нуждается в строгом обосновании, принимая во внимание возможное влияние на цели безопасности и угрозы ОО. Влияние зависит от того, что может быть пропущено в результате выборки. Необходимо также учитывать характер свидетельства, проверяемого выборочно, и требование не игнорировать любые функции безопасности и не снижать их роль.

Следует признать, что выборка из свидетельства, прямо связанного с реализацией ОО (например, результатов теста разработчика) требует подхода, отличного от применяемого при выборке, связанного с вынесением заключения, правильно ли выполнялся процесс. Во многих случаях, когда от оценщика требуется определить, что процесс действительно выполняется, рекомендуется стратегия выборки. Подход здесь отличается от того, который применяется при выборке результатов тестирования разработчиком. Это происходит, потому что в первом случае речь идет об уверенности в том, что процесс выполняется, а во втором мы имеем дело с определением корректности реализации ОО. Как правило, более объемные выборки приходится анализировать в случаях, связанных с правильной реализацией ОО, нежели с необходимостью удостовериться, что процесс выполняется.

В определенных случаях для оценщика может быть подходящим придать особое значение многократности теста разработчика. К примеру, в случае выполнения независимых тестов, включенная туда обширная совокупность тестов будет различаться лишь внешне (возможно из-за выполнения больше тестов, чем необходимо для соответствия критериям ATE_COV и ATE_DPT), далее соответственно оценщику следует сфокусироваться на многократности теста разработчика. Отметим, что это не подразумевает собой требование для высокопроцентной выборки многократности теста разработчика, а наоборот данная обширная совокупность тестов может быть обоснована низкопроцентной выборкой.

Обычно при использовании автоматического тестового комплекта для выполнения функционального теста, оценщику проще перепроверить тестовой комплект в целом, чем повторять только выборку теста разработчика. Несмотря на это, оценщик имеет обязательство проверить, что автоматический тест не дает неправильные результаты. Вывод таков, что выборка автоматического тестового комплекта должна быть проверена,

принципиально для выбора определенных тестов преимущественно другим и гарантии достаточного размера выборки, применяемого как равного в этом случае.

При выборке рекомендуется всегда придерживаться следующих принципов:

а) выборка не может быть случайной, напротив следует выбирать так, как выбирают образца всех свидетельств. Размер и структура выборки должна быть обоснована;

б) когда выборка основывается на корректное выполнение ОО, следует, чтобы выборка была репрезентативна по всем аспектам, относящимся к областям применения выборки. В частности, следует, чтобы выборка охватила все разнообразие компонентов, функций безопасности, мест разработки и эксплуатации (если их несколько) и типов аппаратных платформ (если их несколько).

Объем выборки следует сопоставить с рентабельностью оценки, он зависит от некоторых характеристик ОО (например, от размеров и сложности ОО, от объема документации);

в) также, когда выборка касается конкретного получения свидетельства в том, что тест разработчика является повторяемым и воспроизводимым, используемая выборка должна соответствовать всем определенным аспектам теста разработчика, такие как различные тест режимы. Используемая выборка должна соответственно обнаруживать любую системную проблему в функциональном процессе теста разработчика. Содействие оценщика, то есть многократность тестов разработчика и выполнение независимых тестов, должно являться обоснованным касательно указания главных вопросов в ОО;

г) там, где выборка осуществляется для получения свидетельства выполнения некоторого процесса (например, контроля посетителей или анализа проекта), оценщику следует выбрать объем информации, достаточный для получения приемлемой уверенности в выполнении процесса;

д) заявителя и разработчика не следует заблаговременно информировать о точном составе выборки. При этом следует учитывать необходимость обеспечения своевременности поставки выборки и вспомогательных материалов, например, комплексов тестовых программ и оборудования оценщику в соответствии с графиком проведения оценки;

е) следует, чтобы отбор при выборке по возможности был непредвзятым (не стоит выбирать всегда только первый или последний номер в списке). В идеале отбор следует поручить не оценщику, а кому-то другому.

Ошибки, найденные в выборке, могут быть отнесены к двум категориям — систематические или спорадические. Если ошибка систематическая, следует устранить ее причину и полностью выполнить новую выборку. При надлежащем объяснении разработчика вопрос о спорадических ошибках

может быть решен без необходимости новой выборки, хотя такое объяснение следует подтвердить. Оценщику следует руководствоваться здравым смыслом при определении, увеличить ли объем выборки или использовать другую выборку.

А.3 Зависимости

А.3.1 Введение

В общем случае выполнение требуемых видов и подвидов деятельности и действий по оценке возможно в произвольном порядке или параллельно. Тем не менее, имеются различные виды зависимостей, которые необходимо учитывать оценщику.

Этот подраздел представляет общее руководство по учету зависимостей между различными видами и подвидами деятельности и действиями по оценке.

А.3.2 Зависимости между видами деятельности

В некоторых случаях для различных классов доверия может быть рекомендована или даже потребована определенная последовательность выполнения связанных с ними видов деятельности по оценке. Конкретный пример – вид деятельности по оценке ЗБ. Вид деятельности по оценке ЗБ начинается прежде каких-либо видов деятельности по оценке ОО, так как ЗБ обеспечивает основу и контекст их выполнения. Однако сделать итоговое заключение по оценке ЗБ до завершения оценки ОО может оказаться невозможным, т.к. результаты деятельности по оценке ОО могут привести к изменениям в ЗБ.

А.3.3 Зависимости между подвидами деятельности

Оценщику необходимо учитывать зависимости между компонентами, указанные в части 3 ОК.

Большинство зависимостей - односторонние, например, подвид деятельности оценки AVA_VAN.1 требует подвид деятельности оценки ADV_FSP.1 и AGD_OPE.1. Также есть примеры взаимных зависимостей, где оба компонента зависят друг от друга. Пример этому является подвид деятельности оценки ATE_FUN.1 и подвид деятельности оценки ATE_COV.1.

Обычно положительное заключение по подвиду деятельности можно принять только при успешном завершении всех тех подвидов деятельности, от которых зависит данный подвид деятельности. Например, как правило, положительное заключение по AVA_VAN.1 может быть принято, если только по подвидам деятельности, относящимся к ADV_FSP.1 и AGD_OPE.1, также принято положительное заключение. В случае взаимной зависимости, порядок выполнения этих компонентов решается оценщиком. Это указывает на то, что положительное заключение обычно может быть определено, когда оба подвида деятельности успешно завершены.

Поэтому при определении будет ли некоторый подвид деятельности влиять на другой подвид деятельности, оценщику следует выяснить, зависит ли этот подвид деятельности от потенциальных результатов оценки любых зависимых подвидов деятельности. Действительно, может случиться, что зависимый подвид деятельности сам станет влиять на этот подвид деятельности, требуя выполнить заново ранее завершенные действия.

Существенное влияние приобретают зависимости при обнаружении оценщиком недостатков. Если недостаток идентифицирован в результате проведения одного из подвидов деятельности, положительное заключение по зависимому подвиду деятельности может оказаться невозможным до устранения всех недостатков, относящихся к подвиду деятельности, от которого он зависит.

А.3.4 Зависимости между действиями

Может случиться, что результаты, полученные оценщиком во время одного действия, используются при выполнении другого действия. Например, действия по анализу полноты и непротиворечивости не могут быть завершены, пока не завершена проверка содержания и представления свидетельств. Это означает, что, к примеру, оценку на обоснование на ПП/ЗБ следует выполнить только после оценки частей непротиворечивости того же ПП/ЗБ.

А.4 Посещение объектов

А.4.1 Введение

Категория доверия АЛС включает в себя следующие требования:

а) применение управления конфигурации, обеспечивающее сохранность целостности ОО;

б) меры, процедуры и стандарты касательно безопасной доставки ОО, обеспечивающие защиту безопасности для ОО и не подвергающие риску при поставке к пользователю;

в) меры безопасности, для защиты охраны развития окружающей среды.

Посещение объектов разработки – полезный способ определения оценщиком, выполняются ли процедуры способом, не противоречащим своему описанию в документации.

Объекты посещаются для того, чтобы ознакомиться с:

а) использованием системы УК, как описано в плане УК;

б) практическим применением процедур поставки, как описано в документах о доставке;

в) применением мер безопасности во время разработки и поддержания ОО, как описано в документации по безопасности разработок.

Конкретная и подробная информация дана в операциях тех видов деятельности, где предусмотрены такие посещения:

а) УК способности ALC_CMC.n с n>=3 (особенно рабочий период

ALC_CMC.3-10 = ALC_CMC.4-13 = ALC_CMC.5-19);

б) поставка ALC_DEL (особенно рабочий период ALC_DEL.1-2);

в) безопасность разработки ALC_DVS (особенно рабочий период ALC_DVS.1-3 = ALC_DVS.2-4).

А.4.2 Общий метод

Во время оценки часто необходимы несколько встреч оценщика с разработчиком, и один из обычных вопросов рационального планирования – совмещение посещений объектов для уменьшения затрат. Например, можно совмещать посещение объектов для проверки управления конфигурацией, безопасности, обеспечиваемой разработчиком, и выполнения поставок. Могут также оказаться необходимыми несколько посещений одного и того же объекта для проверки всех стадий разработки. Следует учесть, что разработка может происходить в нескольких помещениях одного и того же здания, в нескольких зданиях, расположенных на одной территории, или же в нескольких местах.

Первое посещение объекта следует запланировать на ранних стадиях оценки. Для оценки, которая начинается на стадии разработки ОО, это позволит внести, при необходимости, коррективы. Для оценки, проводимой после завершения разработки ОО, раннее посещение даст возможность предпринять меры по исправлению, если в применяемых процедурах будут выявлены серьезные неточности. Это позволит избежать лишних усилий при оценке.

Интервью также является полезным способом определения, отражают ли документированные процедуры то, что делается в действительности. При проведении подобных интервью оценщику следует стремиться к получению более глубокого понимания анализируемых процедур на месте разработки, их практического использования и применения в соответствии с представленными свидетельствами оценки. Такие интервью дополняют, но не заменяют исследование свидетельств оценки.

Первой операцией в подготовке посещения объекта является выполнение оценщиками оценки, относительно категории доверия АЛС, исключая аспекты, описывающие результаты посещение объекта. Основываясь на информации релевантной документации разработчика и вопросов, оставшихся без ответа, оценщики собрали перечень проверок вопросов, которые подлежат решению посредством посещений объектов.

Первоначальная версия отчета оценки о категории АЛС и перечня проверок воспринимается в качестве основы для совещания касательно посещения объектов с руководством оценочных работ.

Перечень проверок служит путеводителем для посещений объектов, на вопросы которых можно найти ответы в осмотре релевантных мер, их применении и результатов, и через интервью. В соответствующих местах выборка требует определенного уровня доверия (см. Приложение А).

Результаты посещений объектов записываются и служат основой для заключительной версии отчета оценки о категории доверия АЛС.

Тогда следует рассмотреть иные подходы для получения уверенности, предоставляющие эквивалентный уровень доверия (например, проанализировать свидетельства оценки). Любое решение отменить посещение следует принимать после консультации с органом по сертификации. Подходящие критерии безопасности и методология основываются на стандартах Систем Информационного Управления по безопасности.

А.4.3 Справочник-ориентир для подготовки перечня проверок

Ниже указаны определенные ключевые слова, темы которых следует проверить во время проверки.

А.4.3.1 Аспекты управления конфигурации

Основа:

- пункты перечня конфигурации, включая ОО, исходный код, серии выполнения, проектная документация, руководство по разработке ALC_CMC.3-8;
- сопровождение проектной документации, исходный код, путеводитель пользователя по разным версиям ОО;
- объединение системы конфигурации в процесс проектирование и разработки, план теста, анализ теста и качественные процедуры управления.

Анализы теста:

- сопровождение планов теста и результаты по определенным конфигурациям и версиям ОО;
- система контроля доступа и регистрации;
- система определенного проектного назначения или изменения права доступа.

Допуск:

- система допуска ОО и путеводителя для клиентов;
- система для компонентов тестирования и одобрения и для ОО перед распределением.

А.4.3.2 Аспекты безопасности разработки

Инфраструктура:

- меры безопасности для физического контроля доступа на объекты разработки и обоснование эффективности использования данных мер.

Организационные мероприятия:

- организационная структура, в отношении безопасности развития окружающей среды;
- организационная сортировка между разработкой, продукцией, тестом и гарантией качества.

Индивидуальные мероприятия:

- меры по образованию личного состава, в отношении безопасности

разработки;

- меры и правовые соглашения по неразглашению внутренней информации.

Контроль доступа:

- назначение охраняемых объектов (например, ОО, исходный код, серии выполнения, проектная документация, руководство по разработке, путеводители) и системы безопасности;

- системы и обязательства касательно контроля доступа и владение идентификационной информацией;

- системы регистрации для любого вида доступа к объектам разработки и сохранности регистрационных данных. Данные входа, процесса работы и выхода;

- меры безопасности по защите вывода и устройств вывода (принтер, плоттер и дисплеи);

- организация защиты локальной и коммуникационной связи.

Хранение, передача и уничтожение документов, и совокупность данных:

- системы обращения с документами и данными;

- системы и обязательства уничтожения распределенной документации и регистрации данных событий.

Защита данных:

- системы и обязательства защиты данных и информации (например, резервные копии).

План на случай непредвиденных обстоятельств:

- тренировки на случай непредвиденных обстоятельств и других обязанностей;

- документы по мерам применяемых на случай непредвиденных обстоятельств касательно контроля доступа;

- информация личного состава о применяемых тренировках в экстремальных ситуациях.

А.4.4 Пример контрольной таблицы

Примеры контрольных таблиц для осмотра объекта состоят из таблиц для подготовки аудита и для представления результатов аудита.

Данная структура контрольной таблицы является ориентировочной. В зависимости от точного содержания нового руководства, могут потребоваться изменения.

Контрольная таблица состоит из трех подпунктов и приведена в Таблице А.1

а) управления конфигурацией системы;

Таблица А.1 – Пример контрольной таблицы по ОУД 4 (отрывок)

A. Тестирование систем управления конфигурацией (ALC_CMC.4 и ALC_CMS.4)					
№	Операция	Документация разработчика	Оценки	Замечания и вопросы	Результат
A.1	ALC_CMC.4- 11, ALC_CMC.4- 12	“Система управления конфигурацией”, ch.	Система автоматически управляющая файлами исходных кодов, допускающая управление профилями пользователя и ранжированными правами доступа, а также проверку идентификации и аутентификации пользователей.	Требуется ли аутентификация пользователя для чтения или обновления файла исходного кода?	Если у пользователя нет права на доступ к конфиденциальному документу, в списке файлов для него это даже не отображается.
...	...	...	...	...	...
B. Тестирование правил поставки (ALC_DEL.1)					
№.	Операция	Документация разработчика	Оценки	Замечания и вопросы	Результат
B.1	ALC_DEL.1- 1, ALC_DEL.1- 2	“Поставка ОО”, ch. ...	Программное обеспечение, подписанное и шифрованное системой PGP, передано потребителю.	---	Оценщики проверили процесс поставки, и пришли к заключению о его соответствии описанию, дополнительно передается контрольная сумма.
...	...	...	...	...	...
C. Тестирование организационной и инфраструктурной безопасности разработчика (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)					
№	Операция	Документация разработчика	Оценки	Замечания и вопросы	Результат
C.1	ALC_DVS.1- 1, ALC_DVS.1- 2	“Безопасность среды разработки”, ch. ...	Здание защищено ограждением безопасности	Является ли ограждение достаточно сильным?	Оценщики посчитали ограждение….

С. Тестирование организационной и инфраструктурной безопасности разработчика (ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)					
№.	Операция	Документация разработчика	Оценки	Замечания и вопросы	Результат
		(Исходные положения)		Высокий для предотвращения легкого проникновения в здание?	Быть достаточно сильным и высоким
С.2	ALC_DVS.1-1, ALC_DVS.1-2	“Безопасность среды разработки”, ch. ... (Здание)	Здание имеет следующие возможности доступа: главный доступ, который инспектируется приемной и закрыт, если в приемной отсутствует обслуживающий персонал. И доступ в приемную товаров, который защищен двумя роликовыми ставнями.	Является ли перечень возможностей доступа полным?	Кроме указанных возможностей доступа, присутствует аварийный выход, который не может быть открыт снаружи. Роликовые ставни, упомянутые ранее, управляются только с внутренней стороны.

б) правила поставки;

в) меры по обеспечению безопасности в ходе разработки.

Эти подпункты соответствуют действующему СТ РК ИСО / МЭК 15408 классу ALC, особенно возможностям семейств управления конфигурацией (ALC_CMC).n при n> = 3, поставки (ALC_DEL) и безопасности разработки (ALC_DVS).

Далее подпункты подразделяются на строки, соответствующие определенным операциям оценивания настоящего стандарта.

Столбцы контрольной таблицы в свою очередь содержат,

- последовательный номер;
- операции со справочной информацией;
- ссылки на соответствующую документацию разработчика;
- точное воспроизведение оценок разработчика;
- специальные замечания и вопросы, которые должны быть выяснены при осмотре (кроме стандартного задания оценщика верифицировать применение указанных мер);

- результаты тестирования в ходе осмотра.

Если принято решение иметь отдельные контрольные таблицы для подготовки и представления докладов об аудите, колонка результатов не указывается в таблице подготовки, а колонка замечания и вопросы, не указывается в таблице отчетности. Остальные столбцы должны быть идентичны в обеих таблицах.

А.5 Схема обязанностей

Настоящий стандарт описывает минимальные технические работы, которые должны выполнять оценки, проведенные органами надзора (системы). Тем не менее, он также признает, (как прямо, так и косвенно), что существуют виды деятельности или методы, от которых не зависит обоюдное признание результатов оценки. В целях доскональности и ясности, и чтобы лучше определить, где заканчивается настоящий стандарт и начинается методология индивидуальной системы, следующие вопросы остались на усмотрение систем. Системы могут предоставить следующее, хотя могут и что – то оставить неуказанным. (Были приложены все усилия для обеспечения полноты этой таблицы; оценщикам, сталкивающимся с субъектом, который не перечислен ни здесь, ни в настоящем стандарте, следует обращаться за справкой к их системе оценки, чтобы определить, за счет чего падает субъект.)

Вопросы, которые система может указать, включают:

а) что требуется для обеспечения достаточности произведенной оценки - каждая система имеет средства верифицирования технической компетенции, понимания работы и работы ее оценщиков, либо требованием оценщиков

предоставить добытые сведения органам надзора, требуя, чтобы органы надзора повторно выполнили работу оценщика, либо какими-нибудь иными способами, которые заверяют систему об адекватности и сопоставимости всех органов оценки;

б) процесс удаления свидетельств оценки по завершению оценки;

в) любые требования конфиденциальности (со стороны оценщика и неразглашения информации, полученной в ходе оценки);

г) порядок действий, которые должны быть приняты, при столкновении с проблемой в ходе оценки (независимо от того, продолжается ли оценка после того, как проблема устранена, или немедленно заканчивается, исправленный продукт должен быть повторно представлен для оценки);

д) любой специфический (естественный) язык, на котором должна быть предоставлена документация;

е) любые записанные свидетельства, которые должны быть представлены в техническом отчете оценки - настоящий стандарт определяет

минимум для отчета в техническом отчете оценки, однако, индивидуальные системы могут требовать включения дополнительной информации;

ж) любые дополнительные отчеты (кроме технического отчета оценки) требуемые от оценщиков, например, отчеты тестирования;

и) какие-либо конкретные требования, которые могут потребоваться системой, в том числе структура, получатели и т.д. любых из таких требований;

к) любую конкретную структуру содержания какого-либо письменного отчета в результате оценки ЗБ - система может иметь определенный формат для всех своих отчетов, подробно описывающих результаты оценки, будь то оценка ОО или ЗБ;

л) любую дополнительную информацию идентификации ПЗ / ЗБ;

м) любые виды деятельности, для определения пригодности четко сформулированных требований в ЗБ;

н) любые требования для обеспечения свидетельств оценщика в поддержку повторной оценки и повторного использования свидетельств;

о) любую конкретную обработку идентификаторов, логотипов, товарных знаков системы и т.д.;

п) любые конкретные руководства в отношении криптографии;

р) обработку и применение системы, национальных и международных интерпретаций;

с) перечень или характеристики пригодных альтернативных подходов к тестированию, где тестирование недопустимо;

т) механизм, с помощью которого орган оценки может определить, какие меры при тестировании принял оценщик;

у) предпочитаемый подход к тестированию (если таковые имеются): на внутренний интерфейс или на внешний интерфейс;

ф) перечень или характеристику приемлемого средства проведения оценщиком анализа уязвимости (например, методология гипотезы о недостатках);

х) сведения о каких-либо уязвимостях и слабых мест, подлежащих рассмотрению.

Приложение Б
(информационное)

Оценка уязвимости (AVA)

Данное Приложение содержит разъяснения критериев AVA_VAN и примеры их применения. Данное Приложение не определяет AVA критериев; это определение можно найти в ИСО / МЭК 15408-3 подпункт класс AVA:

Оценка уязвимости.

Данное Приложение состоит из 2 основных частей:

а) руководство по завершению независимого анализа уязвимости. Кратко изложено в подпункте Б.1, и более подробно описано в подпункте Б.2. Эти подпункты описывают, каким образом оценщику следует подходить к построению независимого анализа уязвимости;

б) как охарактеризовать и использовать предполагаемый потенциал нападения злоумышленника. Описано в подпунктах Б.3 - Б.5. Эти подпункты содержат пример описания, как потенциал нападения может быть охарактеризован и должен использоваться, а также приводятся примеры.

Б.1 Анализ уязвимости

Цель оценки уязвимости заключается в том, чтобы определить наличие и возможность эксплуатации недостатков и слабых мест ОО в операционной среде. Данное независимое заключение основывается на проведенном оценщиком анализе, и поддерживается тестированием оценщика.

На самом низком уровне анализа уязвимости (AVA_VAN) оценщик просто выполняет поиск общественно доступной информации для выявления каких-либо известных слабостей в ОО, в то время как на более высоких уровнях оценщик осуществляет структурный анализ свидетельств оценки ОО.

Существует три основных фактора при выполнении анализа уязвимости, а именно:

а) идентификация потенциальных уязвимостей;

б) оценка для вынесения независимого заключения, позволяют ли идентифицированные потенциальные уязвимости нарушить функциональные требования безопасности, злоумышленнику, с соответствующим потенциалом нападения;

в) тестирование на проникновение для вынесения независимого заключения, являются ли идентифицированные потенциальные уязвимости используемыми в операционной среде ОО.

Идентификация уязвимостей далее может быть дополнительно разделена на свидетельства для поиска и на то, как трудно вести поиск этих свидетельств, для идентификации потенциальных уязвимостей. В

аналогичном порядке, тестирование на проникновение можно дополнительно разбить на анализ потенциальной уязвимости для идентификации методов нападения и на их демонстрацию.

Эти основные факторы, по сути, являются итеративными, т.е. тестирование на проникновение потенциальных уязвимостей может привести к идентификации дальнейших потенциальных уязвимостей. Таким образом, они выполняются в виде единого анализа уязвимости

Б.2 Метод оценки построения анализа уязвимости

Б.2.1 Введение

Метод оценки анализа уязвимости заключается в том, чтобы определить, что ОО устойчив к проникновению нападений злоумышленника, обладающих основным (для AVA_VAN.1 и AVA_VAN.2), повышенным основным (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения. В первую очередь оценщик оценивает возможность эксплуатации всех идентифицированных потенциальных уязвимостей. Это достигается путем проведения тестирования на проникновение.

При попытке проникнуть в ОО, оценщик должен взять на себя роль злоумышленника с основным (для AVA_VAN.1 и AVA_VAN.2), повышенным основным (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения.

Метод оценки учитывает потенциальные уязвимости, с которыми сталкивается оценщик при проведении других мероприятий по оценке. Метод оценки тестирования на проникновение, определяющий сопротивление ОО этим потенциальным уязвимостям должен быть выполнен, в предполагаемой роли злоумышленника с основным (для AVA_VAN.1 и AVA_VAN.2), повышенным основным (для AVA_VAN.3), умеренным (для AVA_VAN.4) или высоким (для AVA_VAN.5) потенциалом нападения.

Тем не менее, анализ уязвимости не должен проводиться как изолированное мероприятие. Он тесно связан с ADV и AGD. Оценщик выполняет эти мероприятия по оценке с фокусированием на выявлении потенциальных уязвимостей или "проблемных областей". Таким образом, знание оценщиком руководства общей уязвимости (в подпункте В.2.1) обязательно.

Б.2.2 Руководство общей уязвимости

Следующие пять категорий содержат рассмотрение вопроса общих уязвимостей.

Б.2.2.1 Обход

Обход включает любой способ, посредством которого нарушитель мог бы избежать осуществления мер безопасности путем:

а) использования возможностей интерфейсов ОО или утилит, которые могут взаимодействовать с ОО;

б) наследования привилегий или других возможностей, которые следовало бы наоборот запретить;

в) (когда важна конфиденциальность) чтения чувствительных данных, сохраненных или скопированных в недостаточно защищенные области.

В ходе независимого анализа уязвимостей, выполняемого оценщиком, следует рассмотреть (когда это уместно) каждый из следующих аспектов:

а) нападения, основанные на использовании возможностей интерфейсов или утилит, обычно используют в своих целях отсутствие требуемых мер безопасности для этих интерфейсов. Например, получение доступа к функциональным возможностям, которые реализованы на более низком уровне, чем тот, на котором осуществляется управление доступом. Возможные варианты включают:

1) изменение предопределенной последовательности вызова функций;

2) выполнение дополнительной функции;

3) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

4) использование подробностей реализации, представленных в менее абстрактных представлениях;

5) использование задержки между временем проверки доступа и временем использования.

б) изменение предопределенной последовательности вызова компонентов следует рассматривать, когда имеется предусмотренный порядок вызова интерфейсов ОО (например, команд пользователя) для выполнения некоторой функции безопасности (например, открытия файла для доступа и затем чтения данных из него). Если функция безопасности вызывается на одном из интерфейсов ОО (например, проверка управления доступом), то оценщику следует рассмотреть, возможен ли обход функции безопасности путем выполнения соответствующего вызова в более поздней точке последовательности или пропуска ее целиком;

в) выполнение дополнительного компонента (в предопределенной последовательности) является формой нападения, похожей на только что описанную, но включает вызов некоторого другого интерфейса ОО в некоторой точке последовательности. Оно может также включать нападения, основанные на перехвате передаваемых по сети чувствительных данных путем использованием анализаторов сетевого трафика (дополнительным компонентом здесь является анализатор сетевого трафика);

г) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает использование для обхода функции безопасности не относящегося к делу интерфейса ОО,

используя его для достижения цели, которая для него не планировалась или не предопределялась. Скрытые каналы являются примером этого типа нападения. Использование недокументированных интерфейсов (которые могут быть небезопасными) также попадает в эту категорию (включая недокументированные возможности по поддержке и помощи);

д) использование подробностей реализации, представленных в менее абстрактных представлениях, опять включает использование скрытых каналов, через которые нарушитель использует в своих целях дополнительные функции, ресурсы или атрибуты, представленные в ОО как последствия процесса усовершенствования (например, использование переменной типа «блокировка» как скрытого канала). Дополнительные функциональные возможности также могут обеспечиваться тестовыми фрагментами кода, содержащимися в программных модулях ОО;

е) использование задержки между временем проверки доступа и временем использования включает сценарии, в которых выполняется проверка управления доступом и предоставляется доступ, а нарушитель впоследствии способен создать условия, при которых во время выполнения проверки доступа мог бы произойти сбой проверки доступа. Примером является пользователь, порождающий фоновый процесс для чтения и отправки высоко чувствительных данных на терминал пользователя и затем осуществляющий выход из системы и повторный вход в систему на более низком уровне чувствительности. Если фоновый процесс не завершается при выходе пользователя из системы, то проверки в соответствии с мандатным управлением доступом могут быть фактически обойдены;

ж) нападения, основанные на наследовании привилегий, в основном базируются на незаконном приобретении привилегий или возможностей некоторого привилегированного компонента ОС, обычно путем выхода из него неконтролируемым или непредусмотренным способом. Возможные варианты включают:

1) выполнение данных, не предназначенных для выполнения, или преобразование их в возможные для выполнения;

2) генерацию непредусмотренных исходных данных для некоторого компонента;

3) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня;

и) выполнение данных, не предназначенных для выполнения, или преобразование их в возможные для выполнения включает нападения с использованием вирусов (например, помещение в некоторый файл выполняемого кода или команд, которые автоматически выполняются при редактировании данного файла или получении доступа к нему, наследуя, таким образом, привилегии, которые имеет владелец файла);

к) генерация непредусмотренных исходных данных для некоторого

компонента может приводить к непредусмотренным результатам, которыми может воспользоваться нарушитель. Например, если ОО является приложением, реализующим функции безопасности, которые можно обойти при получении пользователем доступа к базовой операционной системе, то может оказаться возможным получить такой доступ сразу после выполнения входной последовательности, исследуя, пока пароль аутентифицируется, результаты ввода различных управляющих или *escape*-последовательностей;

л) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает нападения, основанные на выходе из-под действия ограничений приложения для получения доступа к базовой операционной системе, чтобы обойти функции безопасности, реализуемые приложением. В этом случае предположение, которое нарушается, состоит в том, что для пользователя приложения невозможно получить такой доступ. Подобное нападение можно предвидеть, если функции безопасности реализуются приложением, работающим под управлением системы управления базами данных: опять же есть возможность обхода функций безопасности, если нарушитель сможет выйти из-под действия ограничений приложения;

м) нападения, основанные на чтении чувствительных данных, сохраненных в недостаточно защищенных областях (применимо, когда важна конфиденциальность), включают следующие вопросы, которые следует рассматривать как возможные способы получения доступа к чувствительным данным:

1) сбор «мусора» на диске;

2) доступ к незащищенной памяти;

3) использование доступа к совместно используемым по записи файлам или другим совместно используемым ресурсам (например, к файлам подкачки);

4) активация восстановления после ошибок, чтобы определить, какой доступ пользователи могут получить. Например, после отказа автоматическая система восстановления файлов для файлов без заголовков может использовать каталог для потерянных и найденных файлов, которые присутствуют на диске без меток. Если ОО реализует мандатное управление доступом, то важно исследовать, какой уровень безопасности поддерживается для этого каталога (например, высокий системный) и кто имеет доступ к этому каталогу.

Существует несколько различных методов, посредством которых оценщик может идентифицировать «тайный вход», включая две основные техники. Первая, когда оценщик непреднамеренно идентифицирует в период тестирования интерфейс, который может быть использован неправильно. Вторая, посредством тестирования каждого внешнего интерфейса ФБО отладочным способом для идентификации любых модулей, которые не

называются частями тестирования документированных интерфейсов и затем, проверяя код, который не считается «тайным выходом».

Б.2.2.2 Вмешательство

Вмешательство включает любое нападение, основанное на попытке нарушителя повлиять на режим выполнения функции безопасности или механизма (т. е., искажение или блокировка), например, путем:

а) доступа к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности;

б) вынуждения ОО функционировать в необычных или непредусмотренных условиях;

в) отключения или задержки обеспечения безопасности;

г) физическая модификация ОО.

В ходе независимого анализа уязвимостей оценщику следует рассмотреть (когда это уместно) каждый из следующих аспектов:

а) нападения, основанные на доступе к данным, на конфиденциальность или целостность которых полагается функция или механизм безопасности, включают:

1) чтение, запись или модификацию внутренних данных прямо или косвенно;

2) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью;

3) использование взаимного влияния компонентов, которые невидимы на более высоком уровне абстракции.

б) чтение, запись или модификация внутренних данных прямо или косвенно охватывают следующие типы нападений, которые следует рассмотреть:

1) чтение «секретов», хранимых внутри ОО, таких как пароли пользователей;

2) подмена внутренних данных, на которые полагаются механизмы, обеспечивающие безопасность;

3) изменение переменных среды (например, логических имен) или данных в файлах конфигурации или временных файлах;

в) может оказаться возможным обмануть доверенный процесс для модификации защищенного файла, к которому в обычном состоянии доступ не был бы получен;

г) оценщику следует также рассмотреть следующие «опасные характеристики»:

1) исходный текст вместе с компилятором, постоянно имеющиеся в наличии в ОО (например, может оказаться возможным изменение исходного кода, связанного с входом в систему);

2) интерактивный отладчик и средства внесения изменений (например, может оказаться возможным изменение исполняемого образа);

3) возможность внесения изменений на уровне контроллеров устройств, на котором файловой защиты не существует;

4) диагностический код, который присутствует в исходном коде и может быть опционально включен;

5) инструментальные средства разработчика, оставленные в ОО;

д) использование некоторого компонента в непредусмотренном контексте или с непредусмотренной целью включает (например) случай, когда ОО является приложением, полагающимся на операционную систему, а пользователи используют знания пакета текстового процессора или другого редактора, чтобы изменить свой собственный командный файл (например, чтобы приобрести большие привилегии);

е) использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, включает нападения, использующие совместный доступ к ресурсам, когда модификация ресурса одним компонентом может влиять на режим выполнения другого (доверенного) компонента, например, на уровне исходного кода, через использование глобальных данных или косвенных механизмов, таких как совместно используемая память или семафоры;

ж) следует всегда учитывать нападения, основанные на принуждении ОО функционировать в необычных или непредусмотренных обстоятельствах. Возможные варианты включают:

1) генерацию непредусмотренных исходных данных для некоторого компонента;

2) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня;

и) генерация непредусмотренных исходных данных для компонента включает исследование режима функционирования ОО, когда имеет место:

1) переполнение буферов ввода команд (возможно "разрушение стека" или перезапись другой области хранения, которыми нарушитель может быть способен воспользоваться в своих интересах, или принудительная выдача аварийного дампа, который может содержать чувствительную информацию, такую как открытый текст паролей);

2) ввод неправильных команд или параметров (включая установку параметра в состояние «только для чтения» для интерфейса, который предполагает выдачу данных через этот параметр);

3) вставка маркера конца файла (например, CTRL/Z или CTRL/D) или нулевого символа в журнал аудита;

к) нарушение предположений и свойств, на которые полагаются компоненты более низкого уровня, включает нападения, использующие ошибки в исходном коде, где предполагается (явно или неявно), что относящиеся к безопасности данные находятся в конкретном формате или имеют конкретный диапазон значений. В таких случаях оценщику следует,

формируя данные в другом формате или присваивая им другие значения, сделать заключение, могут ли нападения привести к нарушению таких предположений, и если это так, то может ли это дать преимущества нарушителю;

л) корректный режим выполнения функций безопасности может зависеть от предположений, которые нарушаются при критических обстоятельствах, когда исчерпываются лимиты ресурсов или параметры достигают своего максимального значения. Оценщику следует рассмотреть (если это целесообразно) режим функционирования ОО, когда эти пределы достигаются, например:

1) изменение дат (например, исследования, как ведет себя ОО при переходе датой критического порога);

2) переполнение дисков;

3) превышение максимального числа пользователей;

4) заполнение журнала аудита;

5) переполнение очередей сигналов безопасности, выдаваемых на консоль;

6) перегрузка различных частей многопользовательского ОО, который сильно зависит от компонентов связи;

7) забивание сети или отдельных хостов трафиком;

8) заполнение буферов или полей.

м) нападения, основанные на отключении или задержке обеспечения безопасности, включают следующие аспекты:

1) использование прерываний или функций составления расписаний, чтобы нарушить последовательное выполнение операций;

2) нарушения при параллельном выполнении;

3) использование взаимного влияния между компонентами, которое невидимо на более высоком уровне абстракции.

Использование прерываний или функций составления расписаний, чтобы нарушить последовательность выполнения операций, включает исследование режима функционирования ОО при:

1) прерывании команды (по CTRL/C, CTRL/Y и т.п.);

2) порождении второго прерывания до того, как будет распознано первое.

н) необходимо исследовать результаты завершения процессов, критических для безопасности (например, демона аудита). Аналогично, может оказаться возможной такая задержка регистрации записей аудита или выдачи/получения предупреждающих сигналов, что они становятся бесполезными для администратора (так как нападение может уже достичь цели).

о) нарушения при параллельном выполнении включают исследование режима функционирования ОО, когда два или более субъектов

предпринимают попытку одновременного доступа. Возможно, ОО и сможет справиться с блокировкой, необходимой, когда два субъекта предпринимают попытку одновременного доступа, но при этом его поведение станет не полностью определенным при наличии дополнительных субъектов. Например, критичный по безопасности процесс может быть переведен в состояние ожидания получения ресурса, если два других процесса осуществляют доступ к ресурсу, который ему требуется.

п) использование взаимного влияния компонентов, которое невидимо на более высоком уровне абстракции, может обеспечить способ задержки критического по времени доверенного процесса.

р) физические атаки могут быть разделены на категории на физическое исследование, физическая манипуляция, физическая модификация и замещение:

1) физическое исследование при проникновении целевых качеств ОО от ОО, например, чтение на внутренних коммуникационных интерфейсах, линий или памятей;

2) физическая манипуляция может быть внутренними качествами ОО, нацеленными на внутренние модификации ОО (например, при использовании оптической ошибочной индукции как процесс взаимодействия), на внешние интерфейсы ОО (например, при мощности или неточностях часов) и среду ОО (например, при изменении температуры);

3) физическая замена для замены ОО другим объектом ИТ, в период доставки или операции ОО. Замещение во время доставки ОО от среды разработки до пользователя, должно быть предотвращено посредством применения безопасных процедур доставки (такие как те, что рассматриваются под Безопасность разработки (ALC_DVS)). Замещение ОО во время операции может быть рассмотрено при комбинации руководства пользователя и операционной среды, так, чтобы пользователь имел возможность быть уверенным, что они взаимодействуют с ОО.

Б.2.2.3 Прямые нападения

Прямое нападение включает идентификацию любых тестов проникновения, необходимых для подтверждения или опровержения заявленной минимальной стойкости функций безопасности.

Например, может быть неправильным предположением, что особенное выполнение псевдослучайного генератора чисел будет иметь требуемую энтропию, необходимую для отбора механизма безопасности.

Где вероятностный или переустановочный механизм основывается на выборе атрибутного значения безопасности (например, выбор длины пароля) или на введении даты человеком-пользователем (например, выбор пароля), сделанные предположения должны отражать худший случай.

Вероятностный или переустановочный механизмы должны быть идентифицированы во время исследования свидетельства оценки, требуемого

как вводные данные данного подвида деятельности (цель безопасности, функциональная спецификация, проект верхнего уровня, подгруппа представления выполнения) и другие ОО (например, руководство) документации могут идентифицировать дополнительные вероятностные или переустановочные механизмы.

Когда свидетельство проекта или руководство включает утверждения или предположения (например, о том, сколько опознавательных попыток возможны за минуту), оценщик должен независимо подтвердить, что они корректны. Это может быть достигнуто посредством тестирования или через независимый анализ.

Прямые нападения, зависимые от недостатка в криптографическом алгоритме, не должны рассматриваться под Анализом уязвимости (AVA_VAN), так как они находятся за пределами сферы действия ИСО/МК 15408. Корректность выполнения криптографического алгоритма рассматривается во время деятельности ADV и ATE.

Б.2.2.4 Мониторинг

Информация является абстрактным представлением связи между свойствами объектов, т.е. сигнал содержит информацию для системы, если ОО способен реагировать на этот сигнал. ОО снабжает, обрабатывает и хранит информацию предоставленную данными пользователя. Поэтому:

а) информация с данными пользователя может протекать между субъектами, путем передачи в пределах ОО или экспорта из ОО;

б) информация может быть генерирована и передана другим данным пользователя;

в) информация может быть получена посредством мониторинга операций с данными, представляющими информацию.

Чтобы контролировать операции с данными, информация, предоставленная данными пользователя, может быть характеризована такими атрибутами безопасности как, например "уровень секретности", который имеет такие значения как, несекретный, конфиденциальный, секретный, совершенно секретный. Эта информация, и, следовательно, атрибуты безопасности могут быть изменены операциями, например FDP_ACC.2 может описывать уменьшение уровня путем "санитаризации" или увеличение уровня путем сочетания данных. Это один из аспектов анализа информационного потока сосредоточенного на контролируемых операциях контролируемых субъектов с контролируемыми объектами.

Другим аспектом является анализ неразрешенного потока информации. Этот аспект является более общим, чем прямой доступ к объектам, содержащий данные пользователя, адресованные семейством FDP_ACC. Непринудительный сигнальный канал, переносящий информацию под контролем политики управления потоком информации может быть также вызван путем мониторинга обработки любых объектов, содержащих или

связанных с данной информацией (например, боковые каналы). Принудительные сигнальные каналы могут быть идентифицированы посредством ресурсов манипулирования субъектами и пользователя, который наблюдает такую манипуляцию. Классически, скрытые каналы, были идентифицированы как временные или каналы с памятью, согласно с модификацией или модулированием ресурса. Что касается мониторинга других нападений, использование ОО осуществляется в соответствии с функциональными требованиями безопасности.

Скрытые каналы, как правило, применяются в случае, когда ОО имеет ненаблюдаемость и требования политики многоуровневого разделения. Скрытые каналы могут регулярно обнаруживаться в ходе анализа уязвимости и проектных мероприятий, и, следовательно, должны подвергаться тестированию. Тем не менее, в целом мониторинг таких нападений идентифицируется только через специализированные методы анализа, общепринято называемым "анализом скрытых каналов". Эти методы подвергались многочисленным исследованиям, а также существует множество статей, опубликованных по этому вопросу.

Руководство для проведения анализа скрытых каналов должно требоваться от органов оценки.

Мониторинг нападений потока непринудительной информации включает пассивные методы анализа, направленные на раскрытие чувствительных внутренних данных ОО путем управления ОО, таким образом, который соответствует руководящим документам.

Анализ бокового канала включает аналитические методы углубления, основанные на физической утечки ОО. Физическая утечка может произойти из-за временной информации, потребления электроэнергии и излучения энергии при вычислении ФБО. Временная информация может быть также получена злоумышленником (имеющим сетевой доступ к ОО) дистанционно, основанные на энергии информационные каналы требуют, чтобы злоумышленник находился в ближней среде ОО.

Методы прослушивания включают перехват всех видов энергии, например, электромагнитных или оптических излучений компьютерных дисплеев, не обязательно в ближнем поле ОО.

Мониторинг также включает использование потоков протокола, например, нападение на реализацию протокола защищенных сокетов.

Б.2.2.5 Неправильное применение

Неправильное применение может возникнуть из-за:

а) неполной руководящей документации;

б) необоснованного руководства;

в) непреднамеренной ошибки в конфигурации ОО;

г) принудительного исключения режима применения ОО.

Если руководящая документация не является полной, пользователь может не знать, как управлять ОО в соответствии с функциональными требованиями безопасности. Оценщик должен применять знания с ОО, полученных при проведении других мероприятий по оценке для определения того, что руководство является полным. В частности, оценщику следует учитывать функциональную спецификацию. ФБО, описанные в этом документе должны быть, как требуется, описаны в руководстве, для разрешения безопасного управления и использования через ИФБО доступные для пользователей. Кроме того, различные методы работы должны учитываться для обеспечения того, что по всем методам работы представлены руководства.

Оценщик, может, в качестве помощи, подготовить неофициальное построение соответствий между руководством и данными документами. Любые недостатки в этом построении соответствий может свидетельствовать о неполноте.

Руководство считается необоснованным, если оно требует операционную среду или использование ОО, которые являются несовместимыми с ЗБ или чрезмерно обременительным для поддержания безопасности.

ОО может использовать различные пути для оказания помощи потребителю в эффективном использовании этого ОО в соответствии с функциональными требованиями безопасности и в предотвращении непреднамеренной ошибки в конфигурации. ОО может использовать функцию (функции), чтобы предупредить потребителя, когда ОО находится в состоянии, которое несовместимо с функциональными требованиями безопасности, в то время как другие ОО могут быть доставлены с расширенным руководством, содержащим рекомендации, подсказки, процедуры и т.д. в отношении использования существующих функций безопасности наиболее эффективно, например, руководство по использованию функции аудита в качестве вспомогательного инструмента для обнаружения того, когда функциональные требования безопасности компрометируются, то есть небезопасны.

Оценщик учитывает функциональность ОО, ее назначение и цели безопасности для того, чтобы операционная среда пришла к выводу о том, имеются ли разумные основания ожидать, что использование руководства позволит своевременно обнаружить переход в незащищенное состояние.

Потенциал ОО вступить в незащищенное состояние может быть определен с помощью комплекующего узла оценки, как, например, ЗБ, функциональная спецификация и любое другое представление проекта в качестве доказательств для компонентов, включенных в пакет гарантий для ОО (например, спецификация проекта ОО / ФБО, если один из компонентов проекта ОО (ADV_TDS) включен).

Случаи принудительного исключения режима применения ФБО могут включать, но не ограничиваются, следующим:

а) Режим применения ОО, при запуске, закрытии или активировании ошибки восстановления;

б) Режим применения ОО в экстремальных условиях (иногда называется перегрузкой или асимптотическим режимом применения), особенно там, где это может привести к де-активации или отключение частей ФБО;

в) любой потенциал непреднамеренной ошибки в конфигурации или небезопасное использование в связи с нападениями отмеченными в подпункте о воздействии выше.

Б.2.3 Идентификация потенциальных уязвимостей

Потенциальная уязвимость может быть идентифицирована оценщиком в ходе различных мероприятий. Они могут стать очевидными в ходе оценки, либо они могут быть идентифицированы в результате анализа данных для поиска уязвимостей.

Б.2.3.1 Встречная идентификация уязвимостей

Встречная идентификация уязвимостей, это где потенциальные уязвимости определяются оценщиком при проведении оценки, то есть доказательства, не анализируются с определенной целью выявления потенциальных уязвимостей.

Встречный метод идентификации зависит от опыта и знаний оценщика, которые контролируются органом оценки. Это не воспроизводится в подходе, но будет документировано для обеспечения повторяемости выводов из отчета потенциальных уязвимостей.

Для этого метода не существует официального критерия анализа. Потенциальные уязвимости идентифицируются из свидетельств как результат знания и опыта. Однако, этот способ идентификации не ограничивается каким-либо конкретным подмножеством свидетельств.

Оценщик, как предполагается, обладает знаниями совокупности методов типов ОО и известных недостатков в безопасности, как задокументировано в общедоступных источниках. Уровень знаний, состоит из тех, которые могут быть получены из списка безопасности электронной почты, имеющего отношение к типу ОО, регулярных бюллетеней (неисправность, список уязвимостей и недостатков безопасности), опубликованных теми организациями, которые исследуют проблемы безопасности в продуктах и технологиях широкого пользования.

Эта информация не будет расширяться до конкретных конференций или детальных тезисов, полученных путем университетских исследований для AVA_VAN.1 или AVA_VAN.2. Вместе с тем, чтобы обеспечить то, что применение знаний является своевременным, оценщику возможно, потребуется выполнить поиск материалов общедоступных источников.

Для AVA_VAN.3 к AVA_VAN.5 поиск общественно доступной информации будет включать в себя конференции и тезисы, полученные в течение исследовательской деятельности университетов и других соответствующих организаций.

Примеры того, как это может произойти (как оценщик может столкнуться с потенциальными уязвимостями):

а) Пока оценщик рассматривает некоторые свидетельства, возникает память о потенциальных уязвимостях, выявленных в аналогичном типе продукта, который оценщик считает, также будет присутствовать при оценке ОО;

б) при рассмотрении некоторых свидетельств, оценщик обнаруживает недостатки в спецификации интерфейса, что отражает потенциальную уязвимость.

Это может включать осознание потенциальной уязвимости в ОО через чтение об общих уязвимостях в особом типе продукта, в публикации ИТ - безопасности или в списке безопасности электронной почты,на которые подписан оценщик.

Методы нападения могут быть разработаны непосредственно из этих потенциальных уязвимостей. Таким образом, встречные потенциальные уязвимости объединяются во время проведения тестов проникновения, основаных на анализе уязвимостей оценщика. Четких действий оценщика для встречных потенциальных уязвимостей не существует.

Таким образом, оценщик ориентируется на основе неявных действий, указанных в AVA_VAN.1.2E и AVA_VAN .*. 4E.

Настоящая информация в отношении уязвимостей общедоступных источников и нападений может быть предоставлена оценщику, например, органом оценки. Эта информация будет принята оценщиком во внимание, при объединении встречных уязвимостей и методов нападений при разработке тестов проникновения.

Б.2.3.2 Анализ

Выделяются следующие типы анализа представленые в рамках действий оценщика.

Б.2.3.2.1 Неструктурированный анализ

Неструктурированный анализ, который будет выполняться оценщиком (для оценки под - деятельности (AVA_VAN.2)) позволяет оценщику рассматривать общие уязвимости (как говорится в В.2.1). Оценщиком будет также применяться их опыт и знания о недостатках в аналогичных типах технологии.

Б.2.3.2.2 Целенаправленный анализ

В ходе проведения мероприятий по оценке оценщик может также идентифицировать проблемные зоны. Ими являются конкретные части свидетельства ОО по поводу которых оценщик имеет некоторые

резервирования, хотя свидетельство удовлетворяет требованиям для данного вида деятельности, с которыми ассоциируется свидетельство. Например, какая-либо конкретная спецификация интерфейса выглядит особенно сложно, и поэтому может быть подвержена ошибкам либо в разработке ОО либо в операции ОО.

Потенциальная уязвимость не проявляется на данном этапе, требуется дальнейшее расследование. Это выходит за рамки встречной уязвимости, так как требуется дальнейшее расследование.

Различие между потенциальной уязвимостью и проблемной областью:

а) потенциальная уязвимость - Оценщик знает метод атаки, который может быть использован для эксплуатации слабых мест или оценщик знает информацию уязвимости, которая имеет отношение к ОО;

б) проблемная область – Оценщик может посчитать проблему в качестве потенциальной уязвимости на основе информации, представленной в других местах. При чтении спецификации интерфейса, оценщик определяет, что из-за чрезвычайной (ненужной) сложности интерфейса потенциальная уязвимость может залегать в этой области, хотя это и не является очевидными на основе этого первоначального обследования.

Целенаправленным подходом к выявлению уязвимостей является анализ свидетельств с целью выявления любых очевидных потенциальных уязвимостей через содержащуюся информацию. Он представляет собой неструктурный анализ, поскольку такой подход не предопределен. Такой подход к определению возможных уязвимостей может быть использован в ходе независимого анализа уязвимости требуемого оценкой под - деятельности (AVA_VAN.3).

Этот анализ, может быть, достигнут с помощью различных подходов, которые приведут к соизмеримым уровням доверия. Ни один из подходов не имеет жесткий формат для изучения свидетельств, которые будут выполняться.

Принятый подход направлен результатами оценки свидетельств, чтобы определить, что он соответствует требованиям AVA / AGD. Таким образом, исследование свидетельств о существовании потенциальных уязвимостей может быть направлено любой из следующих характеристик:

а) проблемные области, выявленные в ходе рассмотрения свидетельств во время проведения оценки;

б) опора на конкретные функциональные возможности для обеспечения разделения, выявленного в ходе анализа дизайна архитектуры (как и в оценке под - деятельности (ADV_ARC.1)), что требует дополнительного анализа, чтобы определить, что его нельзя обойти;

в) типичное изучение свидетельств для формулирования потенциальных уязвимостей ОО.

Оценщик сообщит, какие меры были приняты для выявления потенциальных уязвимостей в свидетельствах. Однако, оценщик, возможно, не сможет описать операции в выявлении потенциальных уязвимостей до начала обследования. Этот подход будет развиваться как результат по результатам оценки.

Проблемные области, могут возникнуть в результате проверки какого-либо из представленных свидетельств, для удовлетворения требований оценки ОО. Также учитывается общедоступная информация.

Проведенные оценщиком мероприятия могут быть повторены и те же выводы, в зависимости от уровня доверия в ОО, могут быть достигнуты, хотя принятые меры для достижения этих выводов могут отличаться. Так как метод оценки является документированием формы проведенного анализа, принятые меры для достижения этих выводов являются также воспроизводимыми.

Б.2.3.2.3 Систематизированный

Систематизированный подход к анализу принимает форму структурной проверки свидетельств. Этот метод требует от оценщика определить структуру и форму анализа (например, каким образом производится анализ предопределено, в отличие от целенаправленного метода идентификации). Этот метод, указанный в соответствии с информацией, которая будет рассматриваться и как / почему она будет рассматриваться. Такой подход к определению возможных уязвимостей может быть использован в ходе независимого анализа уязвимостей требуемого оценкой под - деятельности (AVA_VAN.4) и (AVA_VAN.5).

Этот анализ свидетельств является преднамеренным и заранее запланированным в подходе, с учетом всех свидетельств, идентифицированных в качестве ввода в анализ.

Все свидетельства предоставлены для удовлетворения требованиям доверия (ADV), указанным в пакете гарантий, используются в качестве ввода в деятельность идентификации потенциальной уязвимости.

«Систематизированный» дескриптор для этого анализа был использован в попытке охватить характеристику, что это определение потенциальной уязвимости заключается в том, чтобы принять заказанного и запланированного подхода. «Метод» или «система», будет применяться при проверке.

Оценщик описывает метод, который будет использоваться в плане того, что свидетельства будут рассмотрены, информация в свидетельствах будет проверена, каким образом эта информация будет рассмотрена, и гипотеза, которая будет сформулирована.

Следующее содержит несколько примеров, которые может принять гипотеза:

а) рассмотрение неправильного входа интерфейсов доступных для злоумышленника на внешних интерфейсах;

б) проверка механизмов безопасности, таких как разделение доменов, формулирование внутреннего буфера, ведущие к деградации в разделении;

в) анализ для выявления каких-либо объектов, созданных в представлении реализации ОО, которые затем не полностью контролируется ФБО, и могут быть использованы злоумышленником для подрыва функциональных требований безопасности.

Например, оценщик может выявить, что интерфейсы являются потенциальными слабыми местами в ОО и определить подход к анализу, что «все спецификации интерфейса, представленные в функциональной спецификации и проекте ОО, будут проанализированы для формулирования потенциальных уязвимостей», и перейти к объяснению методов, используемых в гипотезе.

Этот метод идентификации представит план нападения ОО, который бы выполнялся оценщиком при завершении тестирования на проникновение потенциальных уязвимостей в ОО. Обоснование метода идентификации представило бы свидетельства по охвату и глубине определения эксплуатации, которые бы выполнялись на ОО.

Б.3. Когда используется потенциал нападения

Б.3.1 Разработчик

Потенциал нападения используется автором ПЗ / ЗБ в ходе разработки ПЗ / ЗБ, принимая во внимание угрозы среды и отбор компонентов доверия. Это может быть просто независимое заключение, что потенциал нападения, которым обладает предполагаемый злоумышленник ОО, типично характеризуется как основной, повышенный основной, умеренный или высокий. С другой стороны, ПЗ/ЗБ, возможно, пожелает уточнить особенности уровней отдельных предполагаемых факторов, которыми обладает злоумышленник (например, злоумышленники, как предполагается, являются экспертами в типе технологии ОО, с доступом к специализированному оборудованию.)

Автор ПЗ / ЗБ считает, что угроза профиля была разработана в ходе оценки рисков (вне области применения СТ РК ИСО / МЭК 15408, но используется в качестве ввода в разработку ПЗ / ЗБ с точки зрения определения проблем безопасности или в случае низкого доверия ЗБ). Рассмотрение этого профиля угрозы с точки зрения одного из подходов, рассмотренных в следующих подпунктах, позволит спецификации потенциала нападения ОО противостоять.

Б.3.2 Оценщик

Потенциал нападения особенно рассматриваться оценщиком в двух различных направлениях в ходе оценки ЗБ и уязвимостей.

Потенциал нападения используется оценщиком при проведении анализа уязвимостей под - деятельности, чтобы определить, является или нет ОО устойчивым, к нападениям, предполагающим конкретный потенциал нападения злоумышленника. Если оценщики считают, что потенциальная уязвимость используется в ОО, то они должны подтвердить, что она используется с учетом всех аспектов предполагаемой среды, в том числе в предполагаемом потенциале нападения злоумышленника.

Таким образом, используя информацию, изложенную в формулировке угрозы безопасности ЗБ, оценщик определяет минимальный потенциал нападения, который требуется злоумышленнику, чтобы произвести атаку, и приходит к некоторым выводам о сопротивления ОО нападениям. Таблица Б.1 демонстрирует взаимосвязь между этим анализом и потенциалом нападения.

Таблица Б.1 Тестирование уязвимости и потенциала нападения

Компонент уязвимости	**Устойчивость ОО злоумышленнику с потенциалом нападения:**	**Остаточные уязвимости, используемые только злоумышленником с потенциалом нападения:**
VAN.5	Высокий	Сверх высокий
VAN .4	Умеренный	Высокий
VAN.3	Основной повышенный	Умеренный
VAN .2	Основной	Основной повышенный
VAN.1	Основной	Основной повышенный

«Сверх высокий» потенциал нападения в колонке остаточных уязвимостей, приведенной выше таблицы, представляет те потенциальные уязвимости, которые бы потребовали от злоумышленника иметь более высокий потенциал нападения, чем просто «высокий», чтобы надлежащим образом эксплуатировать потенциальные уязвимости. Уязвимость, классифицируемая как остаточная в данном случае, отражает тот факт, что существуют известные слабости в ОО, но в нынешней операционной среде, с предполагаемым потенциалом нападения, слабые места не могут быть использованы.

На любом уровне потенциала нападения, потенциальная уязвимость может считаться «невозможной» из-за контрмера в операционной среде, который предотвращает уязвимость от эксплуатации.

Анализ уязвимости применяется ко всем ИФБО, включая те, которым доступны вероятностные или пермутационные механизмы. Предположений относительно правильности разработки и реализации ИФБО не было сделано, так же как и ограничений на метод нападения или взаимодействие злоумышленника с ОО - в случае, если нападение возможно, то оно должно

быть рассмотрено в ходе анализа уязвимости. Как показано в таблице В.1, успешная оценка против уязвимости компонентов доверия отражает то, что ФБО разработаны и реализованы для защиты от требуемого уровня угрозы.

Для оценщика не обязательно выполнять подсчет потенциала нападения для каждой потенциальной уязвимости. В некоторых случаях, очевидно, при разработке метода нападения, требуется или нет потенциалу нападения, разработка и запуск метода нападения, соразмерно предположить о том, что злоумышленник в операционной среде. Для любых уязвимостей, эксплуатация которых определена, оценщик осуществляет подсчет потенциала нападения для определения того, что эксплуатация соответствует уровню потенциала нападения предполагаемого злоумышленника.

Подход, описанный ниже, должен применяться, когда необходимо рассчитать потенциал нападения, за исключением если орган оценки предоставляет обязательное указание о применении альтернативного подхода. Значения, приведенные в таблицах Б.2 и Б.3 ниже, математически не подтверждены. Таким образом, значения, указанные в примере этих таблиц, возможно, необходимо будет скорректировать в зависимости от типа технологии и конкретной среды. Оценщик должен справляться о руководстве у органов оценки.

Б.4 Подсчет потенциала нападения

Б.4.1 Применение потенциала нападения

Потенциал нападения является функцией опыта, ресурсов и мотивации. Существует множество методов, представляющих и подсчитывающих эти факторы. Кроме того, могут существовать и другие факторы, которые могут применяться для определенных типов ОО.

Б.4.1.1 Интерпретация мотивации

Мотивация является фактором потенциала нападения, который может быть использован для описания ряда аспектов, связанных со злоумышленником и его желаний. Во-первых, мотивация может подразумевать вероятность нападения - из угрозы, охарактеризованной как высоко мотивированная, можно сделать вывод, что нападение является неизбежным, или что ни одно нападение не ожидается не мотивированной угрозы. Однако, за исключением двух крайних уровней мотивации, трудно получить вероятность нападения, происходящей от мотивации.

Во-вторых, мотивация может подразумевать значение ресурса, денежное или иное, либо злоумышленника либо владельца ресурса. Ресурс более высокой значимости, скорее всего, будет более мотивировать нападения по сравнению с ресурсами, с менее высокой значимостью. Тем не менее, в другом, а не в общем виде, трудно отнести значение ресурса к мотивации, поскольку значение ресурса является субъективным - оно в значительной мере зависит от значения для владельца ресурса.

В-третьих, мотивация может означать, опыт и ресурсы, на которые злоумышленник готов осуществить нападение.

Можно сделать вывод о том, что высоко мотивированный злоумышленник может приобрести достаточный опыт и ресурсы для поражения мер защиты ресурсов. И наоборот, можно сделать вывод о том, что злоумышленник со значительным опытом и ресурсами, не желает осуществить нападение, используя их, если мотивация злоумышленника находится на низком уровне.

В ходе подготовки и проведения оценки, все три аспекта мотивации в какой – то мере учитываются. Первым аспектом вероятности нападения, является то, что может вдохновить разработчика на проведение оценки. Если разработчик считает, что злоумышленники достаточно мотивированы на нападение, то оценка может обеспечить уверенность в способности ОО помешать усилиям злоумышленника. В тех случаях, когда операционная среда вполне определенна, например, в системе оценки, уровень мотивации к нападению может быть известен, и будет влиять на выбор контрмер.

Учитывая второй аспект, владелец ресурса может полагать, что значимость ресурсов (однако измеренная) достаточна, чтобы мотивировать на них нападения. Если оценка считается необходимой, мотивация злоумышленника учитывается, для определения методов нападения, которые могут быть предприняты, также как опыт и ресурсы, используемые в этих нападениях. После проверки, разработчик имеет возможность выбрать соответствующий уровень доверия, в частности, требование AVA компонентов, соизмеримый с потенциалом нападения для угрозы. В ходе оценки, в качестве результата завершения оценки уязвимости, оценщик определяет, является ли действие ОО в своей операционной среде, достаточным, чтобы помешать злоумышленникам, с выявленными опытом и ресурсами.

Для автора ПЗ может быть возможным, подсчитать мотивации злоумышленника, так как автор ПЗ имеет большие знания в области операционной среды, в которой помещен ОО (в соответствии с требованиями ПЗ). Таким образом, мотивация могла бы формировать точные части выражения потенциала нападения в ПЗ, а также необходимые методы и меры, направленные на количественную оценку мотивации.

Б.4.2 Определение потенциала нападения

Этот подпункт рассматривает факторы, которые определяют потенциал нападения, и содержит некоторые руководства, чтобы помочь устранить некоторые субъективности из этого аспекта процесса оценки.

Б.4.2.1 Определение потенциала нападения

Определение потенциала нападения для нападения соответствует идентификации усилий, необходимых для совершения нападения, а также для демонстрации, что оно может успешно применяться для ОО (в том числе

о создании или строительстве любого необходимого испытательного оборудования), тем самым используя уязвимость в ОО. Демонстрация того, что нападение может быть успешно применено, требует учитывать какие-либо трудности в расширении результатов, показанных в лабораторных условиях, чтобы создать полезное нападение. Например, если эксперимент показывает некоторые биты или байты конфиденциальных данных предмета (например, ключ), то необходимо подумать о том, как можно было бы получить остальную часть данного предмета (в данном примере, некоторые биты могут быть измерены непосредственно дальнейшими экспериментами, в то время как другие могут быть найдены с помощью различных способов, таких как исчерпывающий поиск). Возможно, нет необходимости проводить все эксперименты для выявления всего нападения, если становится ясно, что нападение доказывает, что доступ к ресурсам ОО был получен, и что полное нападение, могло реально осуществляться в эксплуатации в соответствии с компонентом нападения AVA_VAN. В некоторых случаях единственным способом доказать, что нападение может быть реально осуществляться в эксплуатации в соответствии с компонентом нападения AVA_VAN состоит в том, чтобы полностью выполнить нападение, а затем оценить исходя из требуемых ресурсов. Одним из выходов из идентификации потенциальных уязвимостей считается скрипт, который дает пошаговое описание того, каким образом проводить нападения, которые могут быть использованы при эксплуатации уязвимости другого примера ОО.

Во многих случаях оценщики оценивают параметры эксплуатации, а не выполнение полной эксплуатации. Оценки и их обоснование документируются в техническом отчете оценки.

Б.4.2.2 Учитываемые факторы

Следующие факторы должны учитываться в ходе анализа потенциала нападений, необходимых для эксплуатации уязвимостей:

а) время, потраченное для выявления и эксплуатации (истекшее время);

б) требуемый технический опыт специалиста (опыт специалиста);

в) знание проекта ОО и эксплуатации (знание ОО);

г) окно возможностей;

д) ИТ – оборудование и (или) программное обеспечение или другое оборудование, необходимое для эксплуатации.

Во многих случаях эти факторы являются зависимыми, но различной степени могут быть заменены друг другом.

Например, опыт или аппаратно-программное обеспечение может быть заменой времени. Подробное описание этих факторов следует.

Если это случается, то менее "дорогая" комбинация учитывается на этапе эксплуатации.

Истекшее время – это общее количество времени, потраченное злоумышленником, чтобы определить, что конкретная потенциальная

уязвимость может существовать в ОО, для разработки метода нападения и поддерживания усилий, необходимых для монтирования нападения на ОО. Рассмотрение этого фактора, в худшем случае используется для оценки затрат времени. Выявленное количество времени, выглядит следующим образом:

а) меньше, чем за один день;

б) от одного дня до одной недели;

в) от одной до двух недель

г) от двух недель, до одного месяца;

д) каждый дополнительный месяц до 6 месяцев, приводит к увеличению значения;

е) более чем 6 месяцев.

Опыт специалиста указывает на общий уровень знаний об основополагающих принципах типа продукта или метода нападения (например, интернет - протоколов, операционных систем Unix, переполнение буфера). Выявленные уровни являются следующими:

а) не специалистами являются, не имеющие знания по сравнению с экспертами или лица, не владеющие особым опытом;

б) специалисты, осведомлены в том, что они знакомы с областью применения безопасности продукта или типа системы;

в) эксперты знакомы с основными алгоритмами, протоколами, оборудованием, структурами, областью применения безопасности, принципами и концепциями работающих безопасности, методами и инструментами для определения новых нападений, криптографией, классическими нападениями для типов продукта, методами нападения и т.д. реализованными в продукте или типе системы;

г) уровень «Многократный эксперт» введен для того, чтобы обеспечить ситуацию, где необходимы знания различных областей на уровне экспертов для различных этапов нападения.

Может случиться, что требуются знания из нескольких областей. По умолчанию, выбран самый высокий из различных факторов опыта. В конкретных случаях уровень "многократного эксперта" мог бы использоваться, но следует отметить, что знания должны затрагивать те области, которые являются сугубо разными, как, например однополупериодная манипуляция и криптография.

Знания ОО относится к конкретному опыту относительно ОО. Это отличается от общего опыты, но не связано с ним. Выявленные уровни являются следующими:

а) общественная информация относительно ОО (как, например, полученная из интернета);

б) ограниченная информация о ОО (например, информация, которая находится под контролем организации разработчика и совместно с другими организациями в рамках соглашения о неразглашении);

в) чувствительная информация ОО (например, знания, которые распределяются между дискретной группой внутри организации разработчиков, доступ к которой ограничен только для членов указанной группы);

г) критическая информация ОО (например, информация, которая известна всего лишь нескольким лицам, доступ к которой очень жестко контролируется на основе строгой необходимости знать и индивидуальной обязанности).

Информация ОО может быть выпущена в соответствии с абстракцией проекта, хотя это может быть сделано только на ОО на основе ОО. Некоторые проекты ОО могут быть общедоступными (или в значительной степени основанными на общественной доступности), и поэтому даже предоставление проекта было бы классифицировано как общественное или более ограниченное, в то время как представление реализации для других ОО очень внимательно контролируется, поскольку это бы дало злоумышленнику информацию, которая будет способствовать нападению, и поэтому считается чувствительной или даже критической.

Может случиться, что требуются знания из нескольких областей. По умолчанию, выбран самый высокий из различных факторов опыта.

Окно возможностей (возможность) также является важным фактором, и имеет отношение к фактору истекшего времени. Выявление или эксплуатация уязвимости может потребовать значительного количества доступов к ОО, что может повысить вероятность обнаружения. Некоторые методы нападения могут потребовать значительных усилий в автономном режиме, и лишь быстрый доступ к ОО для эксплуатации. Может так же потребоваться, чтобы доступ был непрерывным, или оставался на протяжении нескольких сессий.

Для некоторых ОО окно возможностей может приравняться к числу образцов ОО, которое хакер может добыть. Это очень важный момент, где попытки проникнуть в ОО и разрушить функции требований безопасности могут последовать предотвращению использования ОО и образцов его дальнейших испытаний, например, аппаратные устройства. Часто в этих случаях распределение ОО контролируется, и хакер должен применить усилия, чтобы приобрести дальнейшие образцы ОО.

Целями этого обсуждения являются:

а) излишний/неограниченный доступ имеет в виду, что нападение не нуждается в возможности быть реализованным, потому что нет никакого риска в том, чтобы быть обнаруженным в течение доступа к ОО, и нет проблем в том, чтобы допустить число образцов ОО к нападению;

б) легкость означает, что доступ требуется не больше чем на день, и что число образцов ОО, требуемых выполнить нападение, меньше чем десять;

в) изменение означает, что доступ требуется не больше чем на месяц, и что число образцов ОО, требуемых выполнить нападение, меньше чем сто;

г) трудность означает, что доступ требуется, в меньшей степени, месяц, или что число образцов ОО, требуемых выполнить нападение, в меньше степени, сто;

д) «ни один» означает, что окно возможностей не является достаточным для выполнения нападения (длина, для которой активы доступны или надежны, меньше, чем длина возможности, необходимая для выполнения нападения - например, если ключ активов меняется каждую неделю, а нападение проводится в течение двух недель); другой случай- это когда достаточному числу образцов ОО необходимо выполнить нападение, но хакеру это не доступно - например, если ОО является аппаратом и возможность разрушить ОО в течение нападения вместо того, чтобы быть успешным, очень высока, то хакер имеет доступ только к одному образцу ОО.

Обсуждение этого фактора может быть следствием определения того, что завершение использования, подлежащее требованиям для времени доступности, что лучше, чем времени возможности, является не возможным.

Аппаратное и (или) программное обеспечения ИТ или другие оборудования направляют на проверку для определения или использования уязвимости:

а) стандартное оборудование для хакера доступно с легкостью либо для определения уязвимости, либо для нападения. Это оборудование может быть частью ОО (например, отладочная программа в операционной системе), или может быть быстро приобретена.

ПРИМЕР Загрузки из Интернета, анализатор протокола или сценарии нападения.

б) специализированное оборудование не доступно для хакера столь же легко, но может быть приобретено без особого усилия. Оно может содержать умеренного количества оборудования (например, инструментарий для анализа потребляемой мощности, использование сотней ПК, вдоль и поперек связанных с Интернетом, относятся к этой категории), или развитие более огромных сценариев нападений и программ. Если разные испытательные стенды, состоящие из специализированного оборудования, требуются для особых операций нападения, это будет оценено как заказное;

в) заказное оборудование не доступно для общества, так как оно изготавливается по специальному заказу (например, сверхутонченное программное обеспечение), или потому что оборудование настолько специализировано, что его распространение контролируется, возможно даже ограничено. Или же оно может быть очень дорогое.

г) уровень «Составное заказное» внедрен, чтобы позволить ситуации, когда разные типы заказного оборудования требуются для особых операций нападения. Информация, требуемая для личностей для доступности в нападении на ОО, необходима для экспертизы специалистов и их знаний ОО. Между экспертизой хакера (где хакером может быть один или несколько человек с дополнительными сферами знаний) и способностью эффективно использовать оборудование в нападении существует скрытая взаимосвязь. Чем слабее экспертиза хакера, тем ниже потенциал использования оборудования (аппаратное/программное обеспечение ИТ или другие оборудования). Подобно этому, чем больше экспертиза, тем лучше используется потенциал для оборудования в нападении. Также скрытая, эта взаимосвязь между экспертизой и использованием оборудования не всегда применяется, например, когда меры по защите окружающей среды предотвращает хакером использования оборудования, или когда, посредством усилия других, инструментарий нападения, требуемый маленькой экспертизой для эффективного использования, производится и свободно распространяется (посредством Интернет).

Б.4.2.3 Вычисление потенциала нападения

Таблица Б.2 определяет факторы, обсужденные в предыдущем подпункте, и ассоциации числовых величин с суммарной величиной каждого фактора.

В местах, где фактор очень близок к границам диапазона, оценщик обдумывает использование промежуточной величины к тем, что в таблице. Например, если двадцать образцов требуются для выполнения нападения, то величина между первым и четвертым может быть выбрана для этого фактора, или если же схема основана на общедоступном плане, но разработчик внес некоторые изменения, то величина между нулем и тройкой должна быть выбрана оценщиком в соответствии с его просмотром взаимодействия их плановых изменений. Таблица предназначена быть руководством.

Обозначения в Таблице Б.2 с принятием во внимание «окна возможностей» не является естественной прогрессией от временных рамок, указанных в предшествующих диапазонах, связанных с этим фактором. Эта спецификация указывает на то, что в особом случае потенциальная уязвимость не может быть разработана в ОО с ее предназначенным операционным оборудованием. Например, доступ к ОО может быть обнаружен после определенного количества времени, проведенного в ОО с названным оборудованием (то есть в корпусе системы), где проводится регулярный осмотр, и взломщик не сможет добиться доступа к ОО за требуемые нераскрытые две недели. Однако, это будет неприменимо для ОО, связанного с компьютерной сетью, где возможен удаленный доступ, и где физическая среда для ОО неизвестно.

Таблица Б.2 Вычисление потенциала нападения

Фактор	Оценка
Время работы	
<= один день	0
<= одна неделя	1
<= две недели	2
<= один месяц	4
<= два месяца	7
<= три месяца	10
<= четыре месяца	13
<= пять месяцев	15
<= шесть месяцев	17
> шесть месяцев	19
Опыт	
Непрофессионал	0
Специалист	3*[1)]
Эксперт	6
Высококвалифицированный специалист	8
Знание ОО	
Общедоступное	0
Ограниченное	3
Чувствительное	7
Критическое	11
Окно возможностей	
Излишний / неограниченный доступ	0
Легкий	1
Умеренный	4
Трудный	10
Ни один	**[2)]

Оборудование	
Стандартное	0
Специализированное	4 [3)]
Заказное	7
Составное заказное	9

(1) - когда несколько специалистов требуются для выполнения хода наступления, результирующий уровень экспертизы все еще остается "опытным" (который ведет к показателю 3);

(2) - указывает, что ход атаки не используется как должное, по сравнению с остальными единицами в предназначенной операционной среде ОО;

(3) - если разные испытательные стенды, состоящие из специализированного оборудования, требуются для особых операций нападения, это должно быть расценено как заказное.

Чтобы определить сопротивление ОО по отношению к идентифицированной потенциальной уязвимости, должны быть применены следующие операции:

а) определить возможные сценарии нападения {AS1, AS2, ..., ASn} на ОО в операционной среде;

б) для каждого сценария нападения, выполнять теоретический анализ и вычислять важные потенциальные нападения, используя Таблицу В.2;

в) для каждого сценария нападения, если необходимо, выполнять испытания на проникновение, чтобы подтвердить или опровергнуть теоретический анализ;

г) разделить все сценарии нападения {AS1, AS2, ..., ASn} на две группы:

1) успешные сценарии нападения (то есть те, которые успешно были использованы для разрушения Функциональных Требований Безопасности) и

2) сценарии нападения, потерпевшие неудачу.

д) для каждого сценария нападения, применить Таблицу В.3 и определить, есть ли противоречия между сопротивлением ОО и выбранным компонентом доверия AVA_VAN, смотрите последний столбец Таблицы В.3;

е) стоит найти одно противоречие, оценка уязвимости упадет, например, автор ЗБ выбирает компонент AVA_VAN.5, то сценарий нападения с потенциалом нападения в 21 очко (выше) взломал безопасность ОО. В этом случае ОО сопротивляется нападающему с помощью "Умеренного" потенциала нападения, это противоречит AVA_VAN.5, отсюда, доверие уязвимости слабеет.

«Ценности» столбца Таблицы Б.3 указывают на диапазон оценки потенциала нападения (вычисленный с помощью Таблицы В.2) в сценарии

нападения, что послужило разрушению Функциональных Требований Безопасности.

Таблица Б.3 Оценка уязвимости и сопротивления ОО

Оценки	Потенциал нападения, требуемый для сценария	Сопротивление ОО нападающему с потенциалом нападения:	Встречает компоненты доверия:	Провал компонентов:
0-9	Основной	Не оцененный	-	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA VAN.5
10-13	Повышенный -Основной	Основной	AVA_VAN.1, AVA_VAN.2	AVA_VAN.3, AVA_VAN.4, AVA VAN.5
14-19	Измененный	Повышенный-Основной	AVA_VAN.1, AVA_VAN.2, AVA VAN.3	AVA_VAN.4, AVA_VAN.5
20-24	Высокий	Измененный	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA VAN.4	AVA_VAN.5
=>25	Сверх высокий	Высокий	AVA_VAN.1, AVA_VAN.2, AVA_VAN.3, AVA_VAN.4, AVA VAN.5	-

Такой подход, как этот, не может учитывать каждое обстоятельство или фактор, но должен давать лучшего указания уровня сопротивления нападения, чтобы добиться стандартной оценки. Остальные факторы, такие как доверие, на маловероятные случайные происшествия, не включаются в основную модель, но могут быть использованы оценщиком как оправдание в определении цены других, по сравнению с теми, которые может указать основная модель.

Необходимо отметить, что, тогда как число уязвимостей, оцененных отдельно, может определить высокое сопротивление нападению, то комбинация уязвимостей, оцененных вместе, могут определить, что низшие оценки полностью применимы. Присутствие одной уязвимости может сделать использование другой легче.

Если автор ПЗ/ЗБ желает использовать таблицу потенциала нападения для определения уровня нападения, то ОО должен выдержать (выбор

компонента анализа уязвимости (AVA_VAN)), он должен исходить из следующего:

Для всех разных сценариев нападения (то есть для всех разных типов нападающего и (или) разных типов нападения, о которых думает автор), которые не должны нарушить ФТБ, несколько пробегов через Таблицу В.2 должны определить разные оценки потенциала нападения, придуманных для каждого неудачного сценария нападения. Автор ПЗ/ЗБ затем выбирает высшую оценку, чтобы определить уровень сопротивления ОО из Таблицы В.3: сопротивление ОО должно быть, в меньшей степени, ровно этой определенной высшей оценки. Например, высшая оценка потенциалов нападения всех сценариев нападения, которая не должна разрушить политику безопасности ОО, установленной по умеренному способу; отсюда, сопротивление ОО будет, в меньшей степени, умеренным (то есть умеренным или высоким); поэтому, автор ПЗ/ЗБ может выбрать либо AVA_VAN.4 (для умеренных), либо AVA_VAN.5 (для высоких), в качестве подходящего компонента доверия.

Б.5 Пример вычисления прямого нападения

Объектами механизмов для прямого нападения являются часто жизненно-важные элементы для безопасности системы и разработчики, часто усиливающие эти механизмы. Например, ОО может использовать простую очередь чисел аутентификационного механизма, что может быть преодолено нападающим в силу его возможности быстрого отгадывания другого набора чисел пользователя. Система может усилить этот механизм посредством ограничения набора чисел и их использования различными способами. В течение курса оценивания, анализ этого прямого нападения может проистекать следующим образом:

Информация, собранная с ЗБ и при раскрытии схем данных определяет и аутентифицирует обеспечение основы, которая управляет доступом к ресурсам сети широким распределенным терминалам. Физический доступ к терминалу не контролируется никакими эффективными средствами. Продолжительность доступа к терминалу также не контролируется никакими эффективными средствами. Авторизированные пользователи системы выбирают их собственные пароли, что зарегистрироваться для использования системы, и затем для входа под именем пользователя. Система ставит следующие ограничения для паролей, выбранных пользователями:

а) пароль должен быть не меньше четырех и не больше шести цифр длиной;

б) последовательность очередности чисел запрещается (такие как 7,6,5,4,3);

в) повтор цифр запрещается (каждая цифра должна быть единственной).

Руководство, обеспеченное для пользователей при выборе пароля,

говорит о том, что пароль должен быть настолько случаен, насколько это возможно, и не должен быть как-то связан с пользователем в некоторых случаях - дата рождения, например.

Область пароля вычисляется следующим образом:

а) образцы человеческих привычек - важная часть соображения, имеющая влияние на подход для раскрытия пароля. В худшем случае, сценарий и пользователь выбирают число, включающее только четыре цифры, числом при перестановке пароля при условии, что каждая цифра должна быть единственная, является:

$$7\ (8)\ (9)\ (10) = 5040$$

б) числом возможных возрастаний последовательности является семь, такая же цифра как и в убывании последовательности. Пароль после запрета последовательности будет:

$$5040 - 14 = 5026$$

Основанный на дальнейшей информации, собранной из схемы данных, механизм пароля спланирован с терминалом, связывающим особенности. После шести, проваленных попыток, терминал закрывается на час. Проваленные аутентификационные вычисления восстанавливаются после пяти минут, и хакер может в лучшей попытке вводить пять паролей каждые пять минут, или 60 паролей каждый час.

В среднем, хакер сможет ввести 2513 паролей, за 2513 минут, до того, как введет правильный пароль. Среднее успешное нападение, как результат, исчисляется меньшим, чем по Формуле (Б.1):

$$\frac{2513}{60\frac{\min}{hour}} \approx 42 hours \qquad (Б.1)$$

Используя подход вычисления потенциала нападения, описанный в предыдущем подпункте, установлено, что непрофессионал может раскрыть механизм в рамках дней (получив доступ к объекту оценки), используя при этом стандартное оборудование, и без особых знаний ОО, с оценкой 1. Данная полученная оценка, 1, потенциал нападения, требуемый для совершения успешного нападения, не оценивается, так как он падает вниз, что рассматривается как основа.

УДК 681.324 **МКС 35.040**

Ключевые слова: Альбрехт 1984, анализ функциональных точек (АФТ), границы, изменение, измерение функционального размера (ИФР), корректированный размер, корректировка технической сложности, логическая транзакция, объект, подсчет функциональных точек базовых уровней, подсчет функциональных точек приложения, подсчет функциональных точек разработки проекта, подсчет функциональных точек изменений по проекту, подсчет функциональных точек установленного, подтип объекта, пользователь, приложение, система, тип элементов данных (ТЭД), МГПФТ, КСИ

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074