ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1— 2012

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

ISO/IEC 15408-1:2009
Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

(IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»), Федеральным государственным унитарным предприятием «Ситуационно-кризисный Центр Федерального агентства по атомной энергии» (ФГУП «СКЦ Росатома»)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 814-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-1:2009 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (ISO/IEC 15408-1:2009 «Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model»).

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

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 15408-1—2008

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

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

Содержание

1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
3.1 Термины и определения, общие для всех частей ИСО/МЭК 15408 . . . 2
3.2 Термины и определения, относящиеся к классу ADV . . . 6
3.3 Термины и определения, относящиеся к классу AGD . . . 9
3.4 Термины и определения, относящиеся к классу ALC . . . 9
3.5 Термины и определения, относящиеся к классу AVA . . . 13
3.6 Термины и определения, относящиеся к классу ACO . . . 13
4 Сокращения . . . 13
5 Краткий обзор . . . 14
5.1 Общая информация . . . 14
5.2 Объект оценки . . . 14
5.3 Пользователи ИСО/МЭК 15408 . . . 15
5.4 Части ИСО/МЭК 15408 . . . 16
5.5 Контекст оценки . . . 17
6 Общая модель . . . 17
6.1 Введение к общей модели . . . 17
6.2 Активы и контрмеры . . . 18
6.3 Оценка . . . 21
7 Доработка требований безопасности для конкретного применения . . . 21
7.1 Операции . . . 21
7.2 Зависимости между компонентами . . . 23
7.3 Расширенные компоненты . . . 24
8 Профили защиты и пакеты . . . 24
8.1 Введение . . . 24
8.2 Пакеты . . . 24
8.3 Профили защиты . . . 25
8.4 Использование ПЗ и пакетов . . . 26
8.5 Многократное использование профилей защиты . . . 26
9 Результаты оценки . . . 27
9.1 Введение . . . 27
9.2 Результаты оценки ПЗ . . . 28
9.3 Результаты оценки ЗБ/ОО . . . 28
9.4 Утверждение о соответствии . . . 28
9.5 Использование результатов оценки ЗБ/ОО . . . 29
Приложение А (справочное) Спецификация заданий по безопасности . . . 30
Приложение В (справочное) Спецификация профилей защиты . . . 41
Приложение С (справочное) Руководство по выполнению операций . . . 45
Приложение D (справочное) Соответствие ПЗ . . . 47
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 48
Библиография . . . 49

Введение

Настоящая часть ИСО/МЭК 15408 обеспечивает сопоставимость результатов независимых оценок безопасности. В ИСО/МЭК 15408 это достигается предоставлением единого набора требований к функциональным возможностям безопасности продуктов ИТ и к мерам доверия, применяемым к этим продуктам ИТ при оценке безопасности. Данные продукты ИТ могут быть реализованы в виде аппаратного, программно-аппаратного или программного обеспечения.

В процессе оценки достигается определенный уровень уверенности в том, что функциональные возможности безопасности таких продуктов ИТ, а также меры доверия, предпринятые по отношению к таким продуктам ИТ, отвечают предъявляемым требованиям. Результаты оценки могут помочь потребителям решить, отвечают ли продукты ИТ их потребностям в безопасности.

ИСО/МЭК 15408 (здесь и далее, если не указывается конкретная часть стандарта, то ссылка относится ко всем частям стандарта) полезен в качестве руководства при разработке, оценке и/или приобретении продуктов ИТ с функциональными возможностями безопасности.

В ИСО/МЭК 15408 предусмотрена гибкость, допускающая применение множества методов оценки по отношению к множеству свойств безопасности множества продуктов ИТ. Поэтому пользователи настоящего стандарта должны исключить возможность неправильного использования указанной гибкости стандарта. Например, использование ИСО/МЭК 15408 в сочетании с неподходящими методами оценки, неприменимыми свойствами безопасности или ненадлежащими продуктами ИТ может привести к незначимым результатам оценки.

Следовательно, тот факт, что продукт ИТ был оценен, имеет значимость только в контексте свойств безопасности, которые были оценены, и методов оценки, которые использовались. Органам оценки рекомендуется тщательно проверить продукты, свойства и методы, чтобы сделать заключение, что оценка обеспечивает значимые результаты. Кроме того, покупателям оцененных продуктов рекомендуется тщательно рассмотреть этот контекст, чтобы сделать заключение, является ли оцененный продукт соответствующим и применимым для их конкретной ситуации и потребностей.

ИСО/МЭК 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. ИСО/МЭК 15408 может быть также применим к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. ИСО/МЭК 15408 применим к рискам, возникающим в результате действий человека (злоумышленных или иных), и к рискам, возникающим не в результате действий человека. Кроме области безопасности ИТ, ИСО/МЭК 15408 может быть применим и в других областях ИТ, но в нем не утверждается о применимости в этих областях.

Некоторые вопросы рассматриваются как лежащие вне области действия ИСО/МЭК 15408, поскольку они требуют привлечения специальных методов или являются смежными по отношению к безопасности ИТ. Часть из них перечислена ниже:

a) ИСО/МЭК 15408 не содержит критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к функциональным возможностям безопасности ИТ. Известно, однако, что безопасность в значительной степени может быть достигнута или поддерживаться административными мерами, такими как организационные меры, меры управления персоналом, меры управления физической защитой и процедурные меры.

b) Оценка некоторых специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ИСО/МЭК 15408 применимы и в этой области.

c) В ИСО/МЭК 15408 не рассматривается методология оценки, в рамках которой могут применяться конкретные критерии. Данная методология приведена в ИСО/МЭК 18045.

d) В ИСО/МЭК 15408 не рассматривается административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ожидается, что ИСО/МЭК 15408 будет использоваться для целей оценки в контексте такой структуры.

e) Процедуры использования результатов оценки при аттестации находятся вне области действия ИСО/МЭК 15408. Аттестация является административным процессом, посредством которого предоставляются полномочия на использование продукта ИТ (или их совокупности) в конкретной среде функционирования, включая все его части, не связанные с ИТ. Результаты процесса оценки являются исходными данными для процесса аттестации. Однако, поскольку для оценки не связанных с ИТ свойств,

а также их соотнесения с аспектами безопасности ИТ более приемлемы другие способы, аттестующим следует предусмотреть для этих аспектов особый подход.

f) Критерии для оценки специфических качеств криптографических алгоритмов не входят в ИСО/МЭК 15408. Если требуется независимая оценка математических свойств криптографии, то в системе оценки, в рамках которой применяют ИСО/МЭК 15408, должен быть предусмотрен порядок проведения таких оценок.

Терминология ИСО, такая как «может» (can), «справочный» (informative), «должен» (shall) и «следует» (should), используемая в настоящем стандарте, определена в Директивах ИСО/МЭК, часть 2. У термина «следует» (should) имеется дополнительное значение, применимое при использовании настоящего стандарта. См. примечание ниже. Для использования в ИСО/МЭК 15408 дано следующее определение термина «следует» (should).

«следует» (should): В пределах нормативного текста «следует» (should) указывает, что «среди нескольких возможностей одна рекомендована в качестве наиболее подходящей, без упоминания или исключения других, или что определенный способ действия является предпочтительным, но не обязательно требуемым» (Директивы ИСО/МЭК, часть 2).

Примечание — ИСО/МЭК 15408 интерпретирует «не обязательно требуемый» для отражения того, что выбор другой возможности требует логического обоснования, почему не была выбрана предпочтительная возможность.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

Information technology. Security techniques. Evaluation criteria for IT security.
Part 1. Introduction and general model

Дата введения — 2013—12—01

1 Область применения

Настоящий стандарт устанавливает основные понятия и принципы оценки безопасности ИТ, а также определяет общую модель оценки, которой посвящены различные части стандарта, предназначенного в целом для использования в качестве основы при оценке характеристик безопасности продуктов ИТ.

В данном стандарте представлен краткий обзор и описание всех частей ИСО/МЭК 15408; определены термины и сокращения, используемые во всех частях ИСО/МЭК 15408; установлено основное понятие объекта оценки (ОО), контекста оценки, описана целевая аудитория, которой адресованы критерии оценки. Представлены основные положения, необходимые для оценки продуктов ИТ.

В данном стандарте определяются различные операции, посредством которых функциональные компоненты и компоненты доверия, приведенные в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, могут быть доработаны для конкретного применения путем использования разрешенных операций.

В данном стандарте определяются ключевые понятия профилей защиты (ПЗ), пакетов требований безопасности, а также рассматриваются вопросы, связанные с утверждениями о соответствии; описываются выводы и результаты оценки. В данном стандарте даны инструкции по спецификации заданий по безопасности (ЗБ) и описание структуры компонентов в рамках всей модели. Также дана общая информация о методологии оценки, приведенной в ИСО/МЭК 18045, и области действия системы оценки.

2 Нормативные ссылки

Следующие нормативные документы необходимы для применения настоящего стандарта. Для датированных ссылок применяется только то издание, на которое дается ссылка. Для недатированных ссылок применяется самое последнее издание нормативного ссылочного документа (включая любые изменения).

ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

Издание официальное

3 Термины и определения

Применительно к настоящему документу используются следующие термины и определения.

Примечание — Данный раздел содержит только те термины, которые используются во всем тексте ИСО/МЭК 15408. Некоторые комбинации общих терминов, используемые в ИСО/МЭК 15408 и не вошедшие в данный раздел, поясняются непосредственно в тексте по месту использования.

3.1 Термины и определения, общие для всех частей ИСО/МЭК 15408

3.1.1 **негативные действия** (adverse actions): Действия, выполняемые источником угрозы по отношению к активам.

3.1.2 **активы** (assets): Сущности, предположительно представляющие ценность для владельца ОО.

3.1.3 **назначение** (assignment): Спецификация определенного параметра в компоненте или требовании.

3.1.4 **доверие** (assurance): Основание для уверенности в том, что ОО отвечает конкретным ФТБ.

3.1.5 **потенциал нападения** (attack potential): Мера усилий, затрачиваемых при атаке на ОО, выраженная в показателях компетентности, ресурсов и мотивации нарушителя.

3.1.6 **усиление** (augmentation): Добавление одного или нескольких требований к пакету.

3.1.7 **аутентификационные данные** (authentication data): Информация, используемая для верификации предъявленного идентификатора пользователя.

3.1.8 **уполномоченный пользователь** (authorised user): Пользователь ОО, которому в соответствии с ФТБ разрешено выполнять некоторую операцию.

3.1.9 **класс** (class): Совокупность семейств, объединенных общим назначением.

3.1.10 **четкий** (coherent): Логически упорядоченный и имеющий понятное значение.

Примечание — В случае с документацией это относится как к имеющемуся тексту, так и к структуре документа в том смысле, понятен ли он его целевой аудитории.

3.1.11 **полный** (complete): Свойство, обеспеченное наличием всех необходимых частей некоторой сущности.

Примечание — По отношению к документации это означает, что вся необходимая информация отражена в документации на уровне детализации, не требующем на данном уровне абстракции дальнейших пояснений.

3.1.12 **компонент** (component): Наименьшая выбираемая совокупность элементов, на которой могут основываться требования.

3.1.13 **составной пакет доверия** (composed assurance package): Пакет доверия, представляющий некоторое положение на предопределенной составной шкале доверия.

3.1.14 **подтвердить** (confirm): Декларировать, что что-то детально проверено с независимым определением достаточности.

Примечание — Требуемый уровень строгости зависит от типа рассматриваемого предмета. Данный термин применим только к действиям оценщика.

3.1.15 **внешняя связность** (connectivity): Свойство ОО, позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО.

Примечание — Это взаимодействие включает обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

3.1.16 **непротиворечивый** (consistent): Характеризует связь между двумя или более сущностями, указывая, что между этими сущностями нет никаких явных противоречий.

3.1.17 **противостоять** (counter): Характеризует противостояние некоторому нападению, при котором негативные последствия реализации некоторой конкретной угрозы уменьшаются, но не обязательно полностью ликвидируются.

3.1.18 **демонстрируемое соответствие** (demonstrable conformance): Связь между ЗБ и ПЗ, при которой ЗБ обеспечивает решение общей проблемы безопасности, определенной в ПЗ.

Примечание — ПЗ и ЗБ могут содержать совершенно разные утверждения, относящиеся к разным сущностям, использующие разные понятия и т.д. Демонстрируемое соответствие также является подходящим для типа ОО, для которого уже существует несколько сходных ПЗ, позволяя разработчику ЗБ утверждать о соответствии одновременно всем этим ПЗ и, таким образом, экономить трудозатраты.

3.1.19 **демонстрировать** (demonstrate): Предоставить заключение, полученное в процессе анализа, который является менее строгим, чем «доказательство» («proof»).

3.1.20 **зависимость** (dependency): Соотношение между компонентами, при котором, если некоторое требование, основанное на зависимом компоненте, включается в ПЗ, ЗБ или пакет, то и требование, основанное на компоненте, от которого зависит указанный выше компонент, должно быть, как правило, включено в ПЗ, ЗБ или пакет.

3.1.21 **описывать** (describe): Представить конкретные подробности о некоторой сущности.

3.1.22 **делать заключение** (determine): Подтвердить некоторое заключение, основанное на независимом анализе для достижения этого заключения.

Примечание — Использование данного термина подразумевает выполнение действительно независимого анализа, обычно в условиях отсутствия какого бы то ни было предшествующего анализа. Термин «делать заключение» отличается от терминов «подтверждать» («confirm») или «верифицировать» («verify»), которые предполагают необходимость проверки ранее выполненного анализа.

3.1.23 **среда разработки** (development environment): Среда, в которой осуществляется разработка ОО.

3.1.24 **элемент** (element): Неделимое изложение некоторой потребности в безопасности.

3.1.25 **обеспечивать** (ensure): Гарантировать сильную причинно-следственную связь между некоторым действием и его последствиями.

Примечание — Когда этому термину предшествует термин «способствовать», то это указывает, что одно данное действие не полностью определяет последствия.

3.1.26 **оценка** (evaluation): Оценивание ПЗ, ЗБ или ОО по определенным критериям.

3.1.27 **оценочный уровень доверия** (evaluation assurance level): Набор требований доверия, представляющий некоторое положение на предопределенной шкале доверия и составляющий пакет доверия.

3.1.28 **орган оценки** (evaluation authority): Организация, устанавливающая стандарты и контролирующая качество оценок, проводимых организациями в пределах определенного сообщества, и обеспечивающая реализацию ИСО/МЭК 15408 для данного сообщества посредством системы оценки.

3.1.29 **система оценки** (evaluation scheme): Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ИСО/МЭК 15408.

3.1.30 **исчерпывающий** (exhaustive): Характеристика методического подхода, используемого применительно к проведению анализа или деятельности в соответствии с точно изложенным планом.

Примечание — Этот термин используют применительно к проведению анализа или другой деятельности. Аналогичен термину «систематический» («systematic»), но более строгий, так как указывает не только на то, что в соответствии с некоторым точно изложенным планом проведения анализа или другой деятельности был применен методический подход, но также и на то, что этот план достаточен для обеспечения проведения исследования по всем возможным направлениям.

3.1.31 **объяснять** (explain): Предоставить аргументы, содержащие основания для выбора хода предпринимаемых действий.

Примечание — Данный термин отличается от терминов «описывать» («describe») и «демонстрировать» («demonstrate»). Предназначен для ответа на вопрос «Почему?» без попытки аргументировать, что ход предпринимаемых действий обязательно оптимален.

3.1.32 **расширение** (extension): Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в ИСО/МЭК 15408-2, и/или требований доверия, не содержащихся в ИСО/МЭК 15408-3.

3.1.33 внешняя сущность (external entity): Человек или ИТ-сущность, взаимодействующие с ОО из-за пределов границ ОО.

Примечание — В качестве внешней сущности может также рассматриваться пользователь ОО.

3.1.34 **семейство** (family): Совокупность компонентов, которые направлены на достижение сходной цели, но отличаются акцентами или строгостью.

3.1.35 **формальный** (formal): Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях.

3.1.36 **документация руководств** (guidance documentation): Документация, описывающая поставку, установку, конфигурирование, эксплуатацию, управление и/или использование ОО.

3.1.37 **идентификатор** (identity): Представление, однозначно идентифицирующее сущность (например, пользователя, процесс или диск) в контексте конкретного ОО.

Примечание — Примером такого представления может быть строка символов. Для человека-пользователя таким представлением может быть полное или сокращенное имя или (также уникальный) псевдоним.

3.1.38 **неформальный** (informal): Выраженный на естественном языке.

3.1.39 **передача между ФБО** (inter TSF transfers): Передача данных между ОО и функциональными возможностями безопасности других доверенных продуктов ИТ.

3.1.40 **внутренний канал связи** (internal communication channel): Канал связи между разделенными частями ОО.

3.1.41 **передача в пределах ОО** (internal TOE transfer): Передача данных между разделенными частями ОО.

3.1.42 **внутренне непротиворечивый** (internally consistent): Характеризует отсутствие очевидных противоречий между любыми аспектами сущности.

Примечание — Применительно к документации это означает, что в ней не может быть изложено что-либо, воспринимаемое как противоречащее чему-то другому.

3.1.43 **итерация** (iteration): Использование компонента для выражения двух или более отдельных требований.

3.1.44 **логическое обоснование** (justification): Анализ, приводящий к получению заключения.

Примечание — Термин «логическое обоснование» является более строгим, чем термин «демонстрация». Этот термин требует точных и подробных объяснений каждого шага логических суждений.

3.1.45 **объект** (object): Пассивная сущность в пределах ОО, которая содержит или получает информацию и над которой субъекты выполняют операции.

3.1.46 **операция** (над компонентом) (operation): Модификация или повторное использование компонента.

Примечание — Разрешенными операциями над компонентами являются назначение, итерация, уточнение и выбор.

3.1.47 **операция** (над объектом) (operation): Определенный тип действия, выполняемого субъектом по отношению к объекту.

3.1.48 **среда функционирования** (operation environment): Среда, в которой функционирует ОО.

3.1.49 **политика безопасности организации** (organisational security policies): Совокупность правил, процедур или руководящих принципов в области безопасности для некоторой организации.

Примечание — Политика может быть также отнесена к какой-либо определенной среде функционирования.

3.1.50 **пакет** (package): Именованная совокупность функциональных требований безопасности или требований доверия к безопасности.

Примечание — Примером пакета может служить «ОУДЗ».

3.1.51 **оценка профиля защиты** (protection profile evaluation): Оценивание ПЗ по определенным критериям.

3.1.52 **профиль защиты** (protection profile): Независимое от реализации изложение потребностей в безопасности для некоторого типа ОО.

3.1.53 **доказывать** (prove): Демонстрировать соответствие посредством формального анализа в математическом смысле.

Примечание — Доказательство должно быть полностью строгим во всех отношениях. Обычно термин «доказывать» используют, когда необходимо показать соответствие между двумя представлениями ФБО на высоком уровне строгости.

3.1.54 **уточнение** (refinement): Добавление деталей в компонент.

3.1.55 **роль** (role): Предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО.

3.1.56 **секрет** (secret): Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной ПФБ.

3.1.57 **безопасное состояние** (secure state): Состояние, при котором данные ФБО являются непротиворечивыми и ФБО продолжают корректно реализовывать ФТБ.

3.1.58 **атрибут безопасности** (security attribute): Характеристика субъектов, пользователей (включая внешние продукты ИТ), объектов, информации, сеансов и/или ресурсов, которые используются при определении ФТБ, и значения которых используются при осуществлении ФТБ.

3.1.59 **политика функции безопасности** (security function policy): Совокупность правил, описывающих конкретный режим безопасности, реализуемый ФБО, и выраженных в виде совокупности ФТБ.

3.1.60 **цель безопасности** (security objective): Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и/или предположениям.

3.1.61 **проблема безопасности** (security problem): Изложение, которое в формализованном виде определяет характер и масштабы безопасности, которую должен обеспечивать ОО.

Примечание — Данное изложение содержит сочетание:
- угроз, которым должно быть обеспечено противостояние со стороны ОО;
- ПБОр, осуществляемых ОО, и
- предположений, которые определены для ОО и его среды функционирования.

3.1.62 **требование безопасности** (security requirement): Требование, изложенное на стандартизованном языке и направленное на достижение целей безопасности для ОО.

3.1.63 **задание по безопасности** (security target): Зависимое от реализации изложение потребностей в безопасности для конкретного идентифицированного ОО.

3.1.64 **выбор** (selection): Выделение одного или нескольких пунктов из перечня в компоненте.

3.1.65 **полуформальный** (semiformal): Выраженный на языке с ограниченным синтаксисом и определенной семантикой.

3.1.66 **специфицировать** (specify): Предоставить конкретные подробности о некоторой сущности в строгой и точной форме.

3.1.67 **строгое соответствие** (strict conformance): Иерархическая связь между ПЗ и ЗБ, когда все требования из ПЗ также присутствуют в ЗБ.

Примечание — Эта связь может быть определена как «ЗБ должен содержать все утверждения, которые присутствуют в ПЗ, но может содержать больше». Предполагается, что строгое соответствие будет применяться для обязательных требований, которые могут быть выполнены единственным способом.

3.1.68 **оценка задания по безопасности** (security target evaluation): Оценивание ЗБ по определенным критериям.

3.1.69 **субъект** (subject): Активная сущность в ОО, выполняющая операции над объектами.

3.1.70 **объект оценки** (target of evaluation): Совокупность программного, программно-аппаратного и/или аппаратного обеспечения, возможно сопровождаемая руководствами.

3.1.71 **источник угрозы** (threat agent): Сущность, которая негативно воздействует на активы.

3.1.72 **оценка ОО** (TOE evaluation): Оценивание ОО по определенным критериям.

3.1.73 **ресурс ОО** (TOE resource): Все, что может быть использовано или потреблено ОО.

3.1.74 **функциональные возможности безопасности ОО** (TOE security functionality): Совокупность функциональных возможностей всего аппаратного, программного и программно-аппаратного обеспечения ОО, которые необходимо использовать для корректной реализации ФТБ.

3.1.75 **прослеживать или сопоставлять** (trace): Выполнять неформальный анализ соответствия между двумя сущностями с минимальным уровнем строгости.

3.1.76 **передача за пределы ОО** (transfers outside TOE): Опосредованная ФБО передача данных сущностям, не контролируемым ФБО.

3.1.77 **трансляция** (translation): Описание процесса изложения требований безопасности на стандартизованном языке.

Примечание — Использование термина «трансляция» не является буквальным и не подразумевает, что каждое ФТБ, выраженное на стандартизованном языке, может быть также обратно транслировано к целям безопасности.

3.1.78 **доверенный канал** (trusted channel): Средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую для этого степень уверенности в безопасности.

3.1.79 **доверенный продукт ИТ** (trusted IT product): Продукт ИТ, отличный от ОО, для которого имеются свои функциональные требования, организационно скоординированные с ОО, и который, как предполагается, реализует свои функциональные требования корректно.

Примечание — Примером доверенного продукта ИТ является продукт, который был отдельно оценен.

3.1.80 **доверенный маршрут** (trusted path): Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую для этого степень уверенности в безопасности.

3.1.81 **данные ФБО** (TSF data): Данные, необходимые для функционирования ОО, на основе которых осуществляется реализация ФТБ.

3.1.82 **интерфейс ФБО** (TSF interface): Средства, через которые внешние сущности (или субъект в ОО, но за пределами ФБО) передают данные к ФБО, получают данные от ФБО и обращаются к сервисам ФБО.

3.1.83 **данные пользователя** (user data): Данные для пользователя, не влияющие на выполнение ФБО.

3.1.84 **верифицировать** (verify): Провести строгую детальную проверку с независимым определением ее достаточности.

Примечание — См. также термин «подтверждать» (3.1.14). Термин «верифицировать» имеет более глубокий смысл. Он используется в контексте действий оценщика, когда требуются независимые усилия оценщика.

3.2 Термины и определения, относящиеся к классу ADV

Примечание — Приведенные ниже термины используются в формулировках требований для отражения внутренней структуризации программного обеспечения. Некоторые из них взяты из IEEE Std 610.12—1990 «Стандартный глоссарий терминологии по проектированию программного обеспечения», Институт инженеров по электротехнике и электронике.

3.2.1 **администратор** (administrator): Сущность, которая имеет некоторый уровень доверия в отношении всех политик, реализуемых ФБО.

Примечание — Не все ПЗ или ЗБ предполагают одинаковый уровень доверия к администраторам. Обычно предполагается, что администраторы всегда придерживаются политик, изложенных в ЗБ для ОО. Некоторые из этих политик могут быть связаны с функциональными возможностями ОО, другие — со средой функционирования.

3.2.2 **дерево вызовов** (call tree): Идентифицирует модули в системе в виде диаграммы, показывающей, какие модули вызывают другие модули.

Примечание — Адаптированный термин IEEE Std 610.12—1990.

3.2.3 **связность** (cohesion): Прочность (плотность) модуля, способ и степень, с которыми задачи, выполняемые единичным программным модулем, связаны между собой.

[IEEE Std 610.12—1990]

Примечание — Виды связности включают: случайную, коммуникационную, функциональную, логическую, последовательную и временную. Эти типы связности описывают путем введения соответствующих терминов.

3.2.4 **случайная связность** (coincidental cohesion): Связность модуля, характеризуемая выполнением несвязанных или слабо связанных действий.

[IEEE Std 610.12—1990]

Примечание — См. также «связность» (3.2.3).

3.2.5 **коммуникационная связность** (commuication cohesion): Характеристика модуля, включающего функции, которые осуществляют выдачу выходных результатов другим функциям или используют выходные результаты от других функций.

[IEEE Std 610.12—1990]

Примечание 1 — См. также «связность» (3.2.3).

Примечание 2 — Примером коммуникационно-связанного модуля является модуль контроля доступа, который включает мандатный, дискреционный контроль и контроль полномочий.

3.2.6 **сложность** (complexity): Мера того, насколько трудным для понимания и, соответственно, для анализа, тестирования и поддержки является программное обеспечение.

[IEEE Std 610.12—1990]

Примечание — Уменьшение сложности является основной целью декомпозиции, распределения по уровням и минимизации модулей. Контроль сопряжения и связности значительно способствуют достижению этой цели.

В сфере разработки программного обеспечения были потрачены значительные усилия, связанные с попытками разработать метрики для измерения сложности исходного текста. Большинство из этих метрик использует легко вычисляемые характеристики исходного текста, такие как число операторов и операндов, сложность графа управления потоками (цикломатическая сложность), число строк исходного текста, коэффициент покрытия ком-

ментариями выполняемых операторов и подобные единицы измерений. Стандарты программирования являются полезным инструментарием при генерации кода, который является более простым для понимания.

Семейство «Внутренняя структура ФБО» (ADV_INT) требует проведения анализа сложности всех компонентов. Ожидается, что разработчик обеспечит основание для утверждений о достаточном сокращении сложности. Это основание может включать стандарты программирования, используемые разработчиком, и свидетельство того, что все модули удовлетворяют конкретному стандарту (или, что имеются некоторые исключения, которые логически обоснованы аргументами разработки программного обеспечения). Оно также может включать результаты использования инструментария для определения характеристик исходного текста, или может включать другие основания, которые разработчик находит соответствующими.

3.2.7 **связанность** (coupling): Способ и степень взаимозависимости программных модулей. [IEEE Std 610.12—1990]

Примечание — Типы связанности включают: связанность по вызову, связанность по общей области, связанность по содержимому. Эти типы связанности охарактеризованы ниже.

3.2.8 **связанность по вызову** (call coupling): Взаимосвязь между двумя модулями, взаимодействующими строго через вызовы их документированных функций.

Примечание — Примерами связанности по вызову являются связанность по данным, связанность по образцу, связанность по управлению.

3.2.9 **связанность по вызову (по данным)** (call coupling <data>): Взаимосвязь между двумя модулями, взаимодействующими строго через вызовы параметров, которые представляют собой отдельные элементы данных.

Примечание — См. также «связанность по вызову» (3.2.8).

3.2.10 **связанность по вызову (по образцу)** (call coupling <stamp>): Взаимосвязь между двумя модулями, взаимодействующими через вызовы параметров, которые включают в себя составные поля или имеют значительную внутреннюю структуру.

Примечание — См. также «связанность по вызову» (3.2.8).

3.2.11 **связанность по вызову (по управлению)** (call coupling <control>): Взаимосвязь между двумя модулями, когда один передает информацию, предназначенную для воздействия на внутреннюю логику другого.

Примечание — См. также «связанность по вызову» (3.2.8).

3.2.12 **связанность по общей области** (common coupling): Взаимосвязь между двумя модулями, разделяющими общую область данных или другой общий ресурс системы.

Примечание — Наличие глобальных переменных указывает на то, что модули, использующие эти глобальные переменные, связаны по общей области. Связанность по общей области через глобальные переменные в целом допускается, но в ограниченном объеме.

Например, переменные, помещенные в область глобальных переменных, но используемые только одним модулем, размещены ненадлежащим образом и их следует перенести.

Другими факторами, которые необходимо рассматривать при оценивании приемлемости глобальных переменных, являются следующие:

Количество модулей, которые модифицируют некоторую глобальную переменную. В большинстве случаев возможность управления значениями глобальной переменной следует предусмотреть только для одного модуля, но могут быть ситуации, при которых эта возможность может быть предоставлена и некоторому второму модулю; в этом случае должно быть предоставлено достаточное логическое обоснование. Недопустимо, чтобы такая возможность была предусмотрена более чем для двух модулей. (В процессе оценивания следует обратить внимание на определение модуля, действительно ответственного за значения конкретной переменной; например, если некоторую отдельную подпрограмму используют для модификации переменной, но при этом эта подпрограмма просто выполняет модификацию по запросу некоторого модуля, то именно этот модуль и является ответственным за модификацию; при этом может быть более чем один подобный модуль). Кроме того, в качестве составной части определения сложности, когда два модуля отвечают за значения некоторой глобальной переменной, следует четко показать, как действия по модификации координируются между этими модулями.

Количество модулей, которые обращаются к некоторой глобальной переменной: хотя в большинстве случаев нет ограничений на количество модулей, которые обращаются к глобальной переменной: случаи, при которых много модулей выполняют такие обращения, следует проверять на обоснованность и необходимость.

3.2.13 **связанность по содержимому** (content coupling): Взаимосвязь между двумя модулями, когда один модуль напрямую обращается к внутреннему содержанию другого модуля.

Примечание — Примерами такой связи являются модификация кода или обращение к внутренним меткам другого модуля. В результате часть или все содержимое одного модуля фактически включается в состав другого модуля. Связанность по содержимому можно рассматривать как использование необъявленного интерфейса модуля; это в противоположность связанности, которая использует только объявленные интерфейсы модуля.

3.2.14 **разделение доменов** (domain separation): Характеристика архитектуры безопасности, при которой ФБО определяют отдельные домены безопасности для каждого пользователя и ФБО и обеспечивают, что никакие процессы пользователя не могут повлиять на содержимое домена безопасности другого пользователя или ФБО.

3.2.15 **функциональная связность** (functional cohesion): Функциональная характеристика модуля, который выполняет действия, связанные с одной единственной задачей.

[IEEE Std 610.12—1990]

Примечание — Функционально связный модуль преобразует единственный тип входных данных в единственный тип выходных данных, например модуль управления стеком или модуль управления очередью. См. также «связность» (3.2.3).

3.2.16 **взаимодействие** (interaction): Общие, основанные на коммуникации действия между сущностями.

3.2.17 **интерфейс** (interface): Средства взаимодействия с компонентом или модулем.

3.2.18 **разделение на уровни** (layering): Метод проектирования, при котором отдельные группы модулей (уровни) иерархически организованы таким образом, чтобы один уровень зависел только от уровней, которые ниже его в иерархии сервисов, и предоставлял свои сервисы только уровням, которые выше его в иерархии.

Примечание — Строгое разделение на уровни накладывает дополнительное ограничение, заключающееся в том, что каждый уровень получает сервисы только от уровней, непосредственно ниже его, и предоставляет сервисы только для уровня, непосредственно выше его.

3.2.19 **логическая связность** (logical cohesion), процедурная связность (procedural cohesion): Характеристики модуля, выполняющего сходные виды действий по отношению к различным структурам данных.

Примечание 1 — Модуль демонстрирует логическую связность, если его функции выполняют связанные, но разные операции по отношению к разным входным данным.

Примечание 2 — См. также «связность» (3.2.3).

3.2.20 **модульная декомпозиция** (modular decomposition): Процесс разбиения системы на компоненты для упрощения проектирования, разработки и оценки.

[IEEE Std 610.12—1990]

3.2.21 **невозможность обхода** (ФБО) (non-bypassability <of TSF>): Свойство архитектуры безопасности, при котором все действия, связанные с ФТБ, производятся через ФБО.

3.2.22 **домен безопасности** (security domain): Набор ресурсов, по отношению к которым некоторая активная сущность имеет права на доступ.

3.2.23 **последовательная связность** (sequential cohesion): Характеристика модуля, который включает функции, выходные данные каждой из которых являются входными данными для последующей функции в этом модуле.

[IEEE Std 610.12—1990]

Примечание — Примером последовательно связного модуля является модуль, который включает функции по ведению записей аудита и по поддержке счетчика числа зарегистрированных нарушений некоторого конкретного типа.

3.2.24 **разработка программного обеспечения** (software engineering): Применение систематического, упорядоченного, измеримого подхода к разработке и сопровождению программного обеспечения, т. е. применение методов разработки по отношению к программному обеспечению.

[IEEE Std 610.12—1990]

Примечание — Как в отношении технических методов в целом, при применении принципов разработки программного обеспечения должен использоваться некоторый объем экспертных суждений. На выбор влияет много факторов, а не только применение мер модульной декомпозиции, разделения на уровни и минимизации. Например, разработчик может спроектировать некоторую систему, ориентируясь на будущие приложения, которые первоначально не будут реализовываться. Разработчик может определить некоторую логику по управлению этими

будущими приложениями без их полной реализации; в дальнейшем разработчик может реализовать некоторые вызовы пока еще не реализованных модулей, оставляя программные «заглушки» вызовов. Сделанное разработчиком логическое обоснование таких отклонений от хорошей структуризации программ должно быть оценено с использованием экспертных суждений, так же как должно быть оценено использование надлежащего порядка разработки программного обеспечения.

3.2.25 **временная связность** (temporal cohesion): Характеристика модуля, включающего функции, которые необходимо выполнять примерно в одно и то же время.

Примечание 1 — Адаптированный термин IEEE Std 610.12—1990.

Примечание 2 — Примерами модулей с временной связностью являются модули инициализации, восстановления и завершения работы.

3.2.26 **собственная защита ФБО** (TSF self-protection): Свойство архитектуры безопасности, при которой ФБО не могут быть нарушены не относящимися к ФБО кодом или сущностями.

3.3 Термины и определения, относящиеся к классу AGD

3.3.1 **установка** (installation): Процедура, выполняемая человеком-пользователем, по внедрению ОО в его среду функционирования и приведению его в рабочее состояние.

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

3.3.2 **функционирование (эксплуатация)** (operation): Стадия использования ОО, включающая «обычное использование», администрирование и поддержку (сопровождение) ОО после поставки и подготовки.

3.3.3 **подготовка** (preparation): Вид деятельности на стадии жизненного цикла некоторого продукта, включающий приемку потребителем поставленного ОО и его установку, которая может включать такие действия как загрузка, инициализация и приведение ОО в состояние готовности к функционированию.

3.4 Термины и определения, относящиеся к классу ALC

3.4.1 **критерии приемки** (acceptance criteria): Критерии, применяемые при выполнении процедур приемки (например, успешная проверка документации или успешное тестирование в случае с программным, программно-аппаратным или аппаратным обеспечением).

3.4.2 **процедуры приемки** (acceptance procedures): Процедуры, которым следуют в целях приемки вновь созданных или модифицированных элементов конфигурации как частей ОО или для перевода их на следующий этап жизненного цикла.

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

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

a) первоначальная приемка элемента под управление системы управления конфигурацией, в частности включение в ОО компонентов программного, программно-аппаратного и аппаратного обеспечения разных производителей («интеграция»);

b) перевод элементов конфигурации на следующую стадию жизненного цикла на каждом этапе создания ОО (например, модуль, подсистема, контроль качества конечного ОО);

c) приемка после перемещения элементов конфигурации (например, частей ОО или «заготовок» продуктов) между различными местами разработки;

d) приемка после поставки ОО потребителю.

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

Примечание — Адаптированный термин IEEE Std 610.12—1990.

3.4.4 **документация УК** (CM documentation): Вся документация УК, включая входные данные УК, список УК (список конфигурации), записи системы УК, план УК и документацию по применению УК.

3.4.5 **свидетельство управления конфигурацией** (configuration management evidence): Все, что может быть использовано для приобретения уверенности в правильности функционирования системы УК.

Примечание — Например, выходные данные УК, обоснования, предоставленные разработчиком, результаты контроля, испытаний и интервьюирования, полученные оценщиком в процессе непосредственного посещения места разработки.

3.4.6 **элемент конфигурации** (configuration item): Объект, находящийся под управлением системы УК в течение разработки ОО.

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

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

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

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

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

3.4.9 **план управления конфигурацией** (configuration management plan): Описание порядка использования системы управления конфигурацией для конкретного ОО.

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

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

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

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

Примечание — Примерами записей системы управления конфигурацией являются формы контроля изменений элементов конфигурации или формы санкционирования доступа к элементам конфигурации.

3.4.12 **инструментальные средства управления конфигурацией** (configuration management tools): Управляемые вручную или автоматизированные инструментальные средства, реализующие или поддерживающие систему управления конфигурацией.

Примечание — Например, инструментальные средства управления версиями частей ОО.

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

3.4.14 **поставка** (delivery): Передача завершенного ОО из производственной среды потребителю.

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

3.4.15 **разработчик** (developer): Организация, ответственная за разработку ОО.

3.4.16 **разработка** (development): Стадия жизненного цикла продукта, связанная с созданием представления реализации ОО.

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

3.4.17 **инструментальные средства разработки** (development tools): Инструментальные средства (включая программные средства тестирования, если применимы), поддерживающие разработку и производство ОО.

Примечание — Например, для программного ОО инструментальными средствами разработки обычно являются определенные языки программирования, компиляторы, компоновщики и инструментальные средства генерации.

3.4.18 **представление реализации** (implementation representation): Наименее абстрактное представление ФБО, а именно то, которое используется для создания собственно ФБО без дальнейшего уточнения проекта.

Примечание — Исходный текст (код), который затем компилируется, или схемы аппаратных средств, которые используются при построении реальных аппаратных средств, являются примерами частей представления реализации.

3.4.19 **жизненный цикл** (life-cycle): Последовательность стадий существования объекта (например, некоторого продукта или системы) во времени.

3.4.20 **определение жизненного цикла** (life-cycle definition): Определение модели жизненного цикла.

3.4.21 **модель жизненного цикла** (life-cycle model): Описание стадий (этапов) и их связей друг с другом, которые используются при управлении жизненным циклом определенного объекта, а также описание последовательности этих стадий (этапов) и их высокоуровневых характеристик.

Примечание — См. также рисунок 1.

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

Примечание 1 — Эта стадия может включать изготовление, интеграцию, генерацию, внутреннюю транспортировку, хранение и маркировку ОО.

Примечание 2 — См. также рисунок 1.

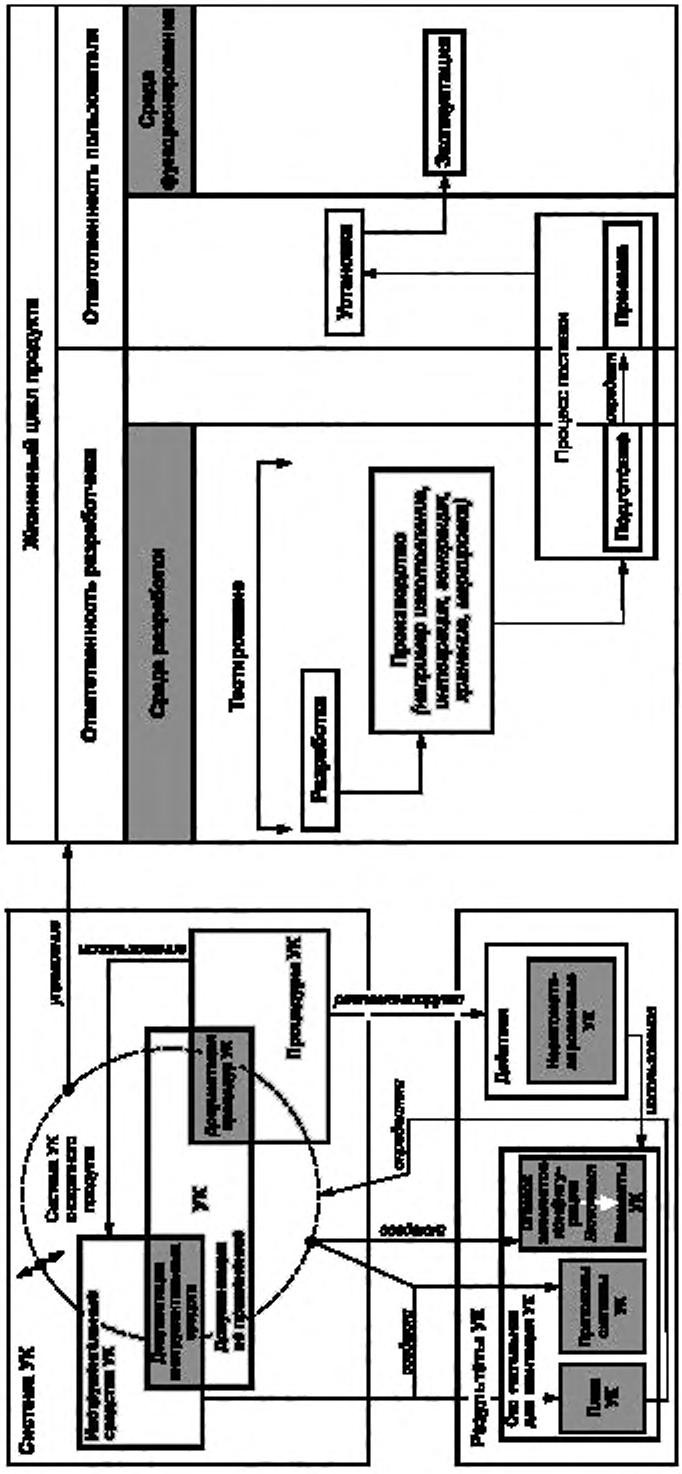

Рисунок 1 — Терминология, связанная с УК и жизненным циклом продукта

3.5 Термины и определения, относящиеся к классу AVA

3.5.1 **скрытый канал** (covert channel): Специально созданный несанкционированный канал передачи сигналов, который позволяет пользователю скрытно нарушать многоуровневую политику разграничения доступа и требования подконтрольности использования ОО.

3.5.2 **обнаруженные потенциальные уязвимости** (encountered potential vulnerabilities): Потенциально слабые места ОО, идентифицированные оценщиком при выполнении видов деятельности по оценке, которые могли бы быть использованы для нарушения ФТБ.

3.5.3 **пригодная для использования уязвимость** (exploitable vulnerability): Слабое место ОО, которое может быть использовано для нарушения ФТБ в среде функционирования ОО.

3.5.4 **мониторинговые атаки** (monitoring attacks): Характерная категория методов нападения, которая включает пассивные методы и средства анализа, направленные на раскрытие чувствительных внутренних данных ОО в условиях его функционирования в соответствии с руководствами.

3.5.5 **потенциальная уязвимость** (potential vulnerability): Предполагаемая, но не подтвержденная слабость ОО.

Примечание — Предположение основывают на теоретически допустимой схеме нападения для нарушения ФТБ.

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

3.5.7 **уязвимость** (vulnerability): Слабое место ОО, которое может быть использовано для нарушения ФТБ в некоторой среде.

3.6 Термины и определения, относящиеся к классу ACO

3.6.1 **базовый компонент** (base component): Сущность в составном ОО, которая сама была предметом оценки, предоставляющая сервисы и ресурсы зависимому компоненту.

3.6.2 **совместимые** (компоненты) (compatible <components>): Свойство компонента, способного предоставлять сервисы, требуемые другим компонентом, через соответствующий интерфейс каждого компонента в согласованной среде функционирования.

3.6.3 **ОО-компонент** (component TOE): Успешно оцененный ОО, который является частью другого составного ОО.

3.6.4 **составной ОО** (composed TOE): ОО, состоящий из двух или более компонентов, которые были успешно оценены.

3.6.5 **зависимый компонент** (dependent component): Сущность в составном ОО, которая сама является предметом оценки, зависящая от предоставления сервисов базовым компонентом.

3.6.6 **функциональный интерфейс** (functional interface): Внешний интерфейс, предоставляющий пользователю доступ к функциональным возможностям ОО, которые напрямую не участвуют в выполнении функциональных требований безопасности.

Примечание — В составном ОО — это интерфейсы, предоставляемые базовым компонентом и требуемые зависимым компонентом для поддержки функционирования составного ОО.

4 Сокращения

В настоящем стандарте[1)] используются следующие сокращения:

ВЧС (VPN) — виртуальная частная сеть;
ГГц (GHz) — гигагерц;
ГИП (GUI) — графический интерфейс пользователя;
ДУД (DAC) — дискреционное управление доступом;
ЗБ (ST) — задание по безопасности;
ИОК (PKI) — инфраструктура открытых ключей;

[1)] Данные сокращения используются в одной или нескольких частях ИСО/МЭК 15408.

ИС (IC) — интегральная схема;
ИТ (IT) — информационная технология;
ИФБО (TSFI) — интерфейс ФБО;
IP — протокол Интернета;
Мб (MB) — мегабайт;
ОО (TOE) — объект оценки;
ОП (RAM) — оперативная память;
ОПБ (SPD) — определение проблемы безопасности;
ОС (OS) — операционная система;
ОУД (EAL) — оценочный уровень доверия;
ПБОр (OSP) — политика безопасности организации;
ПЗ (PP) — профиль защиты;
ПК (PC) — персональный компьютер;
ППИ (API) — прикладной программный интерфейс;
ПФБ (SFP) — политика функции безопасности;
PCI — шина взаимодействия с периферийными компонентами (интерфейс PCI);
СоПД (CAP) — составной пакет доверия;
ТДБ (SAR) — требование доверия к безопасности;
TCP — протокол управления передачей (протокол TCP);
УВВ (IOCTL) — управление вводом-выводом;
УВП (RPC) — удаленный вызов процедуры;
УК (CM) — управление конфигурацией;
ФБО (TSF) — функциональные возможности безопасности ОО;
ФТБ (SFR) — функциональное требование безопасности.

5 Краткий обзор

5.1 Общая информация

В этом разделе представлены основные концептуальные положения ИСО/МЭК 15408. В нем определены понятие «ОО», категории пользователей ИСО/МЭК 15408, контекст оценки и принятый подход к дальнейшему представлению материала в ИСО/МЭК 15408.

5.2 Объект оценки

ИСО/МЭК 15408 является гибким в отношении того, что оценивается и, таким образом, не привязывается, как это обычно понималось, к границам только продуктов ИТ.

Таким образом, в контексте оценки в ИСО/МЭК 15408 используется термин «ОО» (объект оценки).

ОО определяется как набор программных, программно-аппаратных и/или аппаратных средств, возможно сопровождаемых руководствами.

Хотя бывают случаи, что ОО представляет собой продукт ИТ, это не всегда так. ОО может быть продуктом ИТ, частью продукта ИТ, набором продуктов ИТ, уникальной технологией, которая может быть никогда не будет реализована в виде продукта, или сочетанием указанных вариантов.

Относительно ИСО/МЭК 15408 четкое соотношение между ОО и любыми продуктами ИТ является важным только в одном аспекте: оценку ОО, содержащего часть продукта ИТ, не следует ошибочно представлять как оценку продукта ИТ в целом.

Примерами ОО являются:

- прикладная программа;
- операционная система;
- прикладная программа в сочетании с операционной системой;
- прикладная программа в сочетании с операционной системой и рабочей станцией;
- операционная система в сочетании с рабочей станцией;
- интегральная схема смарт-карты;
- локальная вычислительная сеть, включая все терминалы, серверы, сетевое оборудование и программные средства;
- приложение базы данных за исключением программных средств удаленного клиента, обычно ассоциируемых с приложением базы данных.

5.2.1 Различные представления ОО

В ИСО/МЭК 15408 ОО может встречаться в нескольких представлениях, таких как (для программного ОО):

- список файлов в системе управления конфигурацией;
- отдельная мастер-копия, которая была только что скомпилирована;
- коробка, содержащая компакт-диск и руководства, готовая для поставки потребителю;
- установленная и функционирующая версия.

Все из перечисленного считается ОО: где в дальнейшем в ИСО/МЭК 15408 используется термин «ОО», его конкретное представление определяется из контекста.

5.2.2 Различные конфигурации ОО

Обычно продукты ИТ могут быть сконфигурированы различными способами путем включения или отключения различных опций при инсталляции. Так как в процессе оценки по ИСО/МЭК 15408 будет определяться, удовлетворяет ли ОО определенным требованиям, данная гибкость конфигурации может привести к проблемам, так как все возможные конфигурации ОО должны удовлетворять этим требованиям. По этим причинам частыми являются случаи, когда руководства как часть ОО строго ограничивают возможные конфигурации ОО. Таким образом, руководства ОО могут отличаться от общих руководств для продукта ИТ.

Примером является продукт ИТ «Операционная система». Этот продукт может быть сконфигурирован различными способами (например, типы пользователей, количество пользователей, типы разрешенных/неразрешенных внешних подключений, включение/отключение опций и др.)

Если такой продукт ИТ должен быть ОО и оценен на соответствие обоснованному набору требований, его конфигурацию следует намного более тщательно контролировать, так как многие опции (например, разрешение всех типов внешних подключений или отсутствие необходимости аутентификации администратора системы) приведут к тому, что ОО не будет удовлетворять требованиям.

По этой причине нормальным бы являлось дифференциация руководств для продукта ИТ (допускающих много конфигураций) и руководств для ОО (допускающих только одну конфигурацию или только те конфигурации, которые не отличаются относительно способов обеспечения безопасности).

Если руководства ОО допускают более одной конфигурации, то все эти конфигурации вместе именуются «ОО», и каждая такая конфигурация должна удовлетворять требованиям, предъявляемым к ОО.

5.3 Пользователи ИСО/МЭК 15408

В оценке характеристик безопасности ОО заинтересованы в основном три группы пользователей: потребители, разработчики и оценщики. Критерии, представленные в настоящем документе, структурированы в интересах этих групп, потому что именно они рассматриваются как основные пользователи ИСО/МЭК 15408. Далее объясняется, какую пользу могут принести критерии каждой из этих групп.

5.3.1 Потребители

ИСО/МЭК 15408 разработан, чтобы обеспечить посредством оценки удовлетворение запросов потребителей, поскольку это является основной целью и логическим обоснованием процесса оценки.

Результаты оценки помогают потребителям решить, удовлетворяет ли ОО их потребности в безопасности. Эти потребности обычно определяются как следствие анализа рисков, а также направленности политики безопасности. Потребители могут также использовать результаты оценки для сравнения различных ОО. Иерархическое представление требований доверия способствует этому.

ИСО/МЭК 15408 предоставляет потребителям, особенно входящим в группы и сообщества с едиными интересами, независимую от реализации структуру, называемую профилем защиты (ПЗ), для однозначного выражения их требований безопасности.

5.3.2 Разработчики

ИСО/МЭК 15408 предназначен для поддержки разработчиков при подготовке к оценке своих ОО и содействии в ее проведении, а также при установлении требований безопасности, которым должны удовлетворять эти ОО. Данные требования содержатся в зависимой от реализации конструкции, называемой заданием по безопасности (ЗБ). Эти ЗБ могут базироваться на одном или нескольких ПЗ, чтобы показать, что ЗБ соответствуют требованиям безопасности, предъявленных потребителями, которые установлены в данных ПЗ.

ИСО/МЭК 15408 можно использовать для определения обязанностей и действий по предоставлению свидетельств, необходимых при проведении оценки ОО по этим требованиям. Он также определяет содержание и представление таких свидетельств.

5.3.3 Оценщики

В ИСО/МЭК 15408 содержатся критерии, предназначенные для использования оценщиками ОО при формировании заключения о соответствии объектов оценки предъявленным к ним требованиям безопасности. В ИСО/МЭК 15408 дается описание совокупности основных действий, выполняемых оценщиком. При этом в ИСО/МЭК 15408 не определены процедуры, которых следует придерживаться при выполнении этих действий. Дальнейшая информация по этим процедурам приведена в 5.5.

5.3.4 Прочие

Хотя ИСО/МЭК 15408 ориентирован на определение и оценку характеристик безопасности ИТ для объектов оценки, он также может служить справочным материалом для всех, кто интересуется вопросами безопасности ИТ или несет ответственность за них. Среди них можно выделить, например, следующие группы, представители которых смогут извлечь пользу из информации, приведенной в ИСО/МЭК 15408:

a) лица, ответственные за техническое состояние оборудования, и сотрудники служб безопасности, ответственные за определение и выполнение политики и требований безопасности организации в области ИТ;

b) аудиторы как внутренние, так и внешние, ответственные за оценку адекватности безопасности ИТ-решения (которое может состоять из ОО или включать ОО);

c) проектировщики систем безопасности, ответственные за характеристики безопасности продуктов ИТ;

d) аттестующие, ответственные за приемку ИТ-решения в эксплуатацию в конкретной среде;

e) заявители, заказывающие оценку и обеспечивающие ее проведение;

f) органы оценки, ответственные за руководство и надзор за программами проведения оценок безопасности ИТ.

5.4 Части ИСО/МЭК 15408

ИСО/МЭК 15408 состоит из нескольких отдельных, но взаимосвязанных частей, перечисленных ниже. Термины, используемые при описании отдельных частей ИСО/МЭК 15408, приведены в разделе 6.

a) **Часть 1 «Введение и общая модель»** является введением в ИСО/МЭК 15408. В ней определяются общие понятия и принципы оценки безопасности ИТ и приводится общая модель оценки.

b) **Часть 2 «Функциональные компоненты безопасности»** устанавливает совокупность функциональных компонентов, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать функциональные требования к ОО. ИСО/МЭК 15408-2 содержит каталог функциональных компонентов, систематизированных по семействам и классам.

c) **Часть 3 «Компоненты доверия к безопасности»** устанавливает совокупность компонентов доверия, предназначенных для использования в качестве стандартных шаблонов, на основе которых следует устанавливать требования доверия к ОО. ИСО/МЭК 15408-3 содержит каталог компонентов доверия, систематизированных по семействам и классам. Кроме того, в ИСО/МЭК 15408-3 определены критерии оценки профилей защиты и заданий по безопасности и представлены семь предопределенных пакетов доверия, которые названы оценочными уровнями доверия (ОУД).

В поддержку трех частей ИСО/МЭК 15408, перечисленных выше, опубликованы и другие документы. Например, ИСО/МЭК 18045 предоставляет методологию оценки безопасности ИТ, используя ИСО/МЭК 15408 как основу. Предполагается, что будут опубликованы и другие документы, включая нормативно-методические материалы и руководства.

В таблице 1 показано, в каком качестве различные части ИСО/МЭК 15408 будут представлять интерес для каждой из трех основных групп пользователей ИСО/МЭК 15408.

Таблица 1 — Использование частей ИСО/МЭК 15408 основными группами пользователей

Часть ИСО/МЭК 15408	Потребители	Разработчики	Оценщики
1	Используют для получения общих сведений и должны использовать в качестве справочного руководства и руководства по структуре профилей защиты	Используют для получения общих сведений и в качестве справочного руководства. Должны использовать при разработке спецификаций безопасности для объектов оценки	Должны использовать в качестве справочного руководства и руководства по структуре профилей защиты и заданий по безопасности

Окончание таблицы 1

Часть ИСО/МЭК 15408	Потребители	Разработчики	Оценщики
2	Используют в качестве руководства и справочника при формулировании требований для ОО	Должны использовать в качестве справочника при интерпретации изложения функциональных требований и формулировании функциональных спецификаций для объектов оценки	Должны использовать в качестве справочного руководства при интерпретации изложения функциональных требований
3	Используют в качестве руководства при определении требуемых уровней доверия	Используют в качестве справочника при интерпретации изложения требований доверия и определении подходов к установлению доверия к объектам оценки	Используют в качестве справочного руководства при интерпретации изложения требований доверия

5.5 Контекст оценки

Для достижения большей сравнимости результатов оценок их следует проводить в рамках официальной системы оценки, которая устанавливает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться организациям, проводящим оценку, и самим оценщикам.

В ИСО/МЭК 15408 (во всех частях) не излагаются требования к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок.

Второе направление достижения большей сравнимости результатов оценок заключается в использовании общей методологии получения этих результатов. Для всех частей ИСО/МЭК 15408 такая методология приведена в ИСО/МЭК 18045.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие из критериев оценки требуют привлечения экспертных решений и базовых знаний, добиться согласованности которых бывает нелегко. Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертификацию.

Процесс сертификации представляет собой независимую экспертизу результатов оценки, которая завершается их утверждением или выдачей сертификата. Сведения о сертификатах обычно публикуются и являются общедоступными. Сертификация является средством обеспечения большей согласованности в применении критериев безопасности ИТ.

Системы оценки и процессы сертификации находятся в ведении органов оценки, управляющих системами и процессами оценки, и не входят в область действия ИСО/МЭК 15408 (всех частей).

6 Общая модель

6.1 Введение к общей модели

В этом разделе представлены общие понятия, используемые во всех частях ИСО/МЭК 15408, включая контекст использования этих понятий, и подход ИСО/МЭК 15408 к их применению. ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, к которым должны обращаться пользователи ИСО/МЭК 15408-1, развивают эти понятия в рамках описанного подхода. Кроме того, тем пользователям ИСО/МЭК 15408-1, которые собираются выполнять виды деятельности по оценке, необходим ИСО/МЭК 18045. Данный раздел предполагает наличие определенных знаний по безопасности ИТ и не предназначен для использования в качестве учебного пособия в этой области.

Безопасность в ИСО/МЭК 15408 (во всех частях) рассмотрена с использованием совокупности понятий безопасности и терминологии. Их понимание является предпосылкой эффективного использования ИСО/МЭК 15408 (всех частей). Однако сами по себе эти понятия имеют самый общий характер и не предназначены для ограничения класса проблем безопасности ИТ, к которым применим ИСО/МЭК 15408.

6.2 Активы и контрмеры

Безопасность связана с защитой активов. Активы — это сущности, представляющие ценность для кого-либо. Примеры активов включают:

- содержание файла или сервера;
- подлинность голосов, поданных на выборах;
- доступность процесса электронной коммерции;
- возможность использовать дорогостоящий принтер;
- доступ к средствам ограниченного доступа.

Но так как ценность — это весьма субъективное понятие, то почти все, что угодно, может рассматриваться в качестве активов.

Среда, в которой размещаются эти активы, называется средой функционирования. Примерами (аспектами) среды функционирования являются:

- компьютерное помещение в банке;
- компьютерная сеть, подключенная к Интернету;
- локальная вычислительная сеть (ЛВС);
- обычная офисная среда.

Многие активы представлены в виде информации, которая хранится, обрабатывается и передается продуктами ИТ таким образом, чтобы удовлетворить требования владельцев этой информации. Владельцы информации вправе требовать, чтобы доступность, распространение и модификация любой такой информации строго контролировались и активы были защищены от угроз контрмерами. Рисунок 2 иллюстрирует высокоуровневые понятия безопасности и их взаимосвязь.



Рисунок 2 — Понятия безопасности и их взаимосвязь

За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Примерами источников угрозы являются хакеры, злонамеренные пользователи, незлонамеренные пользователи (которые иногда делают ошибки), компьютерные процессы и сбои.

Владельцы активов будут воспринимать такие угрозы как потенциальную возможность нанесения такого ущерба активам, при котором ценность активов для владельцев уменьшилась бы. Специфичный для безопасности ущерб обычно состоит в следующем (но не ограничивается этим): потеря конфиденциальности активов, потеря целостности активов или потеря доступности активов.

Таким образом, эти угрозы увеличивают риски для активов, зависящие от вероятности реализации угрозы и ущерба активам при реализации рассматриваемой угрозы. Для того чтобы уменьшить риски для активов, реализуются контрмеры. Эти контрмеры могут включать ИТ-контрмеры (такие как межсетевые экран и смарт-карты) и не-ИТ-контрмеры (такие как охрана и процедуры). Более широкое рассмотрение контрмер (мер безопасности), а также способов их реализации и управления ими представлено в ИСО/МЭК 27001 и ИСО/МЭК 27002.

Поскольку за активы могут нести (несут) ответственность их владельцы, то им следует иметь возможность отстаивать принятое решение о приемлемости риска для активов, создаваемого угрозами.

При отстаивании этого решения должна иметься возможность продемонстрировать два важных момента, что:

- контрмеры являются достаточными, если контрмеры выполняют то, что заявлено, и угрозам, направленным на активы, обеспечивается противостояние;
- контрмеры являются корректными, если контрмеры выполняют то, что заявлено.

Многие владельцы активов не имеют знаний, опыта или ресурсов, необходимых для вынесения суждения о достаточности и корректности контрмер, и при этом они могут не захотеть полагаться исключительно на утверждения разработчиков этих контрмер. Вследствие этого данные потребители могут захотеть повысить свою уверенность в достаточности и корректности некоторых или всех контрмер путем заказа оценки этих контрмер.

Рисунок 3 иллюстрирует понятия, используемые при оценке, и их взаимосвязь.

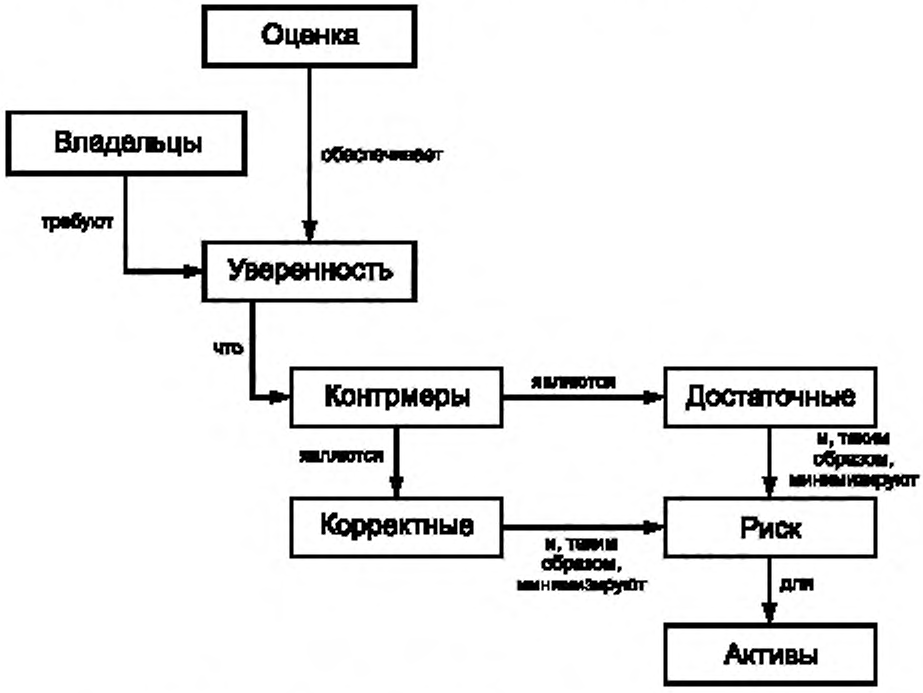

Рисунок 3 — Понятия, используемые при оценке, и их взаимосвязь

6.2.1 Достаточность контрмер

При оценке достаточность контрмер анализируется через конструкцию, называемую заданием по безопасности. В данном пункте представлен упрощенный обзор этой конструкции: более детальное и полное описание можно найти в приложении А.

Задание по безопасности начинается с описания активов и угроз этим активам. Затем в задании по безопасности описываются контрмеры (в форме целей безопасности) и демонстрируется, что данные контрмеры являются достаточными, чтобы противостоять описанным угрозам: если контрмеры осуществляют то, что заявлено по отношению к ним, то обеспечено противостояние угрозам

Далее в задании по безопасности контрмеры делятся на две группы:

a) цели безопасности для ОО: они описывают контрмеры, корректность которых будет определяться при оценке;

b) цели безопасности для среды функционирования: они описывают контрмеры, корректность которых не будет определяться при оценке.

Причинами данного разделения являются:

- ИСО/МЭК 15408 применим только для оценивания корректности контрмер ИТ. Следовательно, не-ИТ-контрмеры (например, сотрудники службы безопасности, процедуры) всегда относят к среде функционирования;

- оценивание корректности контрмер требует затрат времени и денег, возможно делая неосуществимой оценку корректности всех контрмер ИТ;

- корректность некоторых контрмер ИТ может быть уже оценена в ходе другой оценки. Следовательно, экономически неэффективно проводить их повторную оценку.

В задании по безопасности для ОО (корректность контрмер ИТ которого будут оценивать в процессе оценки) требуется дальнейшая детализация целей безопасности для ОО в функциональных требованиях безопасности (ФТБ). Эти ФТБ формулируют на стандартном языке (описанном в ИСО/МЭК 15408-2), чтобы обеспечить точность и облегчить сопоставимость.

Таким образом, в задании по безопасности демонстрируется, что:

- ФТБ удовлетворяют целям безопасности для ОО;
- цели безопасности для ОО и цели безопасности для среды функционирования противостоят угрозам;
- и следовательно ФТБ и цели безопасности для среды функционирования противостоят угрозам.

Из этого следует, что корректный ОО (удовлетворяющий ФТБ) в сочетании с корректной средой функционирования (удовлетворяющей целям безопасности для среды функционирования) будет противостоять угрозам. Ниже отдельно рассматриваются корректность ОО и корректность среды функционирования.

6.2.2 Корректность ОО

Объект оценки может быть неправильно спроектирован и реализован и может, таким образом, содержать ошибки, которые ведут к уязвимостям. Посредством использования этих уязвимостей, нарушители могут причинить ущерб и/или несанкционированно использовать активы.

Эти уязвимости могут являться результатом случайных ошибок, сделанных в течение разработки, ненадлежащего проектирования, преднамеренного внедрения вредоносного кода, ненадлежащего тестирования и др.

Для определения корректности ОО могут выполняться различные виды деятельности, такие как:

- тестирование ОО;
- исследование различных проектных представлений ОО;
- исследование физической безопасности среды разработки ОО.

Задание по безопасности обеспечивает структурированное описание этих видов деятельности для определения корректности в форме требований доверия к безопасности (ТДБ). Эти ТДБ формулируются на стандартном языке (описанном в ИСО/МЭК 15408-3), чтобы обеспечить точность и облегчить сопоставимость.

Если ТДБ удовлетворяются, то существует доверие к корректности ОО, и, таким образом, меньше вероятность, что ОО содержит уязвимости, которые могут быть использованы нарушителем. Величина доверия, которое существует по отношению к корректности ОО, определяется самими ТДБ: несколько «слабых» ТДБ приведут к малому доверию, большое число «сильных» ТДБ приведет к большему доверию.

6.2.3 Корректность среды функционирования

Среда функционирования также может быть неправильно спроектирована и реализована и может, таким образом, содержать ошибки, которые ведут к уязвимостям. Посредством использования этих уязвимостей, нарушители могут причинить ущерб и/или несанкционированно использовать активы.

Однако в ИСО/МЭК 15408 доверие не приобретается при рассмотрении корректности среды функционирования. Или, другими словами, среда функционирования не оценивается (см. 6.3).

Что касается оценки, то предполагается, что среда функционирования является на 100 % правильным отражением целей безопасности для среды функционирования.

Это не мешает потребителю ОО использовать другие методы определения корректности конкретной среды функционирования, такие как:

- если для ОО типа «ОС» установлены цели безопасности для среды функционирования: «Среда функционирования должна обеспечить, что сущности из недоверенной сети (например, Интернета) могут осуществлять доступ к ОО только по ftp», то потребитель мог бы выбрать оцененный межсетевой экран и настроить его так, чтобы к ОО был разрешен доступ только по ftp;
- если для ОО установлены цели безопасности для среды функционирования: «Среда функционирования должна обеспечить, что никто из всего административного персонала не будет вести себя злонамеренно», то потребитель мог бы адаптировать свои контракты с административным персоналом для включения штрафных санкций за злонамеренное поведение, но это решение не является частью оценки в соответствии с ИСО/МЭК 15408.

6.3 Оценка

По стандарту ИСО/МЭК 15408 признают два типа оценки: оценка ЗБ/ОО, которая описывается ниже, и оценка ПЗ, которая определяется в ИСО/МЭК 15408-3. Много раз в ИСО/МЭК 15408 использован термин «оценка» (без уточнений) для ссылки на оценку ЗБ/ОО.

По ИСО/МЭК 15408 оценка ЗБ/ОО проходит в два этапа:

a) оценка ЗБ: на этом этапе определяют достаточность ОО и среды функционирования;

b) оценка ОО: на этом этапе определяют корректность ОО; как отмечалось ранее, оценка ОО не включает оценку корректности среды функционирования.

Оценку ЗБ выполняют путем применения критериев оценки заданий по безопасности (которые определены в разделе ASE ИСО/МЭК 15408-3). Конкретный способ применения критериев ASE определяется используемой методологией оценки.

Оценка ОО является более комплексной. Основные исходные данные для оценки ОО: свидетельства оценки, которые включают ОО и ЗБ, а также, как правило, исходные данные, получаемые из среды разработки, такие как проектная документация или результаты тестирования разработчиком.

Оценка ОО заключается в применении ТДБ (из задания по безопасности) к свидетельствам оценки. Конкретный способ применения конкретного ТДБ определяется используемой методологией оценки.

Как документировать результаты применения ТДБ, какие отчеты необходимо генерировать и в какой степени детализации — определяется в соответствии с используемой методологией оценки и в соответствии с требованиями системы оценки, в рамках которой выполняется оценка.

Результатом процесса оценки ОО будет:

- либо утверждение, что не все ТДБ удовлетворены, и поэтому не достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ;
- либо утверждение, что все ТДБ удовлетворены, и поэтому достигнут заданный уровень доверия к тому, что ОО удовлетворяет ФТБ, которые изложены в ЗБ.

Оценка ОО может быть выполнена после завершения разработки ОО или параллельно с разработкой ОО.

Способ изложения результатов оценки ЗБ/ОО описан в разделе 9. В этих результатах также идентифицируют ПЗ и пакет(ы), по отношению к которым заявлено соответствие ОО; эти конструкции описаны в разделе 8.

7 Доработка требований безопасности для конкретного применения

7.1 Операции

Функциональные компоненты и компоненты доверия из ИСО/МЭК 15408 можно использовать точно так, как они сформулированы в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, или же можно их конкретизировать, применяя разрешенные операции. При использовании операций разработчик ПЗ/ЗБ должен также отследить, чтобы зависимости других требований, которые зависят от данного требования, были удовлетворены. Разрешенные операции выбирают из следующей совокупности:

a) итерация (iteration): позволяет неоднократно использовать компонент при различном выполнении в нем операций;

b) назначение (assignment): позволяет определять параметры;

c) выбор (selection): позволяет выбирать один или более пунктов из перечня;

d) уточнение (refinement): позволяет осуществлять детализацию.

Операции «назначение» и «выбор» разрешены только в тех местах компонента, где они специально обозначены. Операции «назначение» и «выбор» разрешены для всех компонентов. Ниже операции описаны более детально.

Приложения ИСО/МЭК 15408-2 предоставляют руководство по допустимому выполнению операций выбора и назначения. Это руководство предоставляет нормативные инструкции по тому, как выполнять операции, и этим инструкциям необходимо следовать, если разработчик ПЗ/ЗБ логически не обоснует отклонение от этих инструкций:

a) «Нет» допускается как вариант выполнения выбора только если он явным образом предусмотрен.

Списки, предусмотренные для выполнения операций выбора, не должны быть пустыми. Если выбран вариант «Нет», не могут быть выбраны никакие другие дополнительные варианты. Если «Нет» не предусмотрено в качестве варианта выбора, допускается сочетание вариантов в операции выбора с союзами «и» и «или», если в операции выбора в явном виде не определено «выбрать одно из».

Операции выбора при необходимости можно сочетать с итерацией. В этом случае применение выбранного варианта для каждой итерации не должно пересекаться с предметом другой итерации выбора, так как они должны быть уникальными.

b) По отношению к выполнению операций назначения необходимо обратиться к приложениям ИСО/МЭК 15408-2, чтобы определить, когда «Нет» является допустимым выполнением.

7.1.1 Операция «итерация»

Операция «итерация» может быть выполнена по отношению к любому компоненту. Разработчик ПЗ/ЗБ выполняет операцию «итерация» путем включения в ПЗ/ЗБ нескольких требований, основанных на одном и том же компоненте. Каждая итерация компонента должна отличаться от всех других итераций этого компонента, что реализуется завершением по-другому операций «назначение» и «выбор» или применением по-другому операции «уточнение».

Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям.

В ряде случаев операция «итерация» может быть выполнена по отношению к компоненту, для которого вместо его итерации можно было бы выполнить операцию «назначение», указав диапазон или список значений. В этом случае разработчик ПЗ/ЗБ может выбрать наиболее подходящую альтернативу, решив с учетом всех обстоятельств, есть ли потребность предоставления единого обоснования для всего диапазона значений или необходимо иметь отдельное обоснование для каждого из значений. Разработчику также следует обратить внимание на то, требуется ли отдельное прослеживание для этих значений.

7.1.2 Операция «назначение»

Операцию «назначение» осуществляют тогда, когда рассматриваемый компонент включает элемент с некоторым параметром, значение которого может быть установлено разработчиком ПЗ/ЗБ. Параметром может быть ничем не ограниченная переменная или правило, которое ограничивает переменную конкретным диапазоном значений.

Каждый раз, когда элемент в ПЗ предусматривает операцию «назначение», разработчик ПЗ должен выполнить одно из четырех действий:

a) оставить операцию «назначение» полностью невыполненной. Разработчик ПЗ, например, мог бы включить в ПЗ FIA_AFL.1.2 «При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*]";

b) полностью выполнить операцию «назначение». Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.2 «При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны **предотвращать в дальнейшем привязку соответствующей внешней сущности к какому-либо субъекту**»;

c) ограничить операцию «назначение», чтобы в дальнейшем ограничить диапазон допустимых значений. Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.1 «ФБО должны **обнаружить, когда произойдет [назначение: положительное целое число от 4 до 9] неуспешных попыток аутентификации ...**»;

d) преобразовать «назначение» в «выбор», ограничивая таким образом «назначение». Например, разработчик ПЗ мог бы включить в ПЗ FIA_AFL.1.2 «При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны **[выбор: предотвращать в дальнейшем привязку соответствующего пользователя к какому-либо субъекту, уведомлять администратора»]**.

Каждый раз, когда элемент в ЗБ предусматривает операцию «назначение», разработчик ЗБ должен завершить выполнение этой операции «назначение», как указано выше в варианте b). Варианты a), c) и d) для ЗБ не допускаются.

Значения, определенные в вариантах b), c) и d), должны соответствовать указанному типу значений, требуемому для данного «назначения».

Когда «назначение» должно быть завершено определением некоторой совокупности, например субъектов, в «назначении» можно перечислить совокупность этих субъектов, но также можно привести некоторое описание этой совокупности, на основе которого могут быть определены элементы совокупности, такое как:

- все субъекты;
- все субъекты типа X;
- все субъекты, кроме субъекта A,

при условии, что понятно, какие субъекты имеются в виду.

7.1.3 Операция «выбор»

Операцию «выбор» осуществляют тогда, когда рассматриваемый компонент включает элемент, в котором разработчиком ПЗ/ЗБ должен быть сделан выбор из нескольких пунктов.

Каждый раз, когда элемент в ПЗ предусматривает операцию «выбор», разработчик ПЗ может выполнить одно из трех действий:

a) оставить операцию «выбор» полностью невыполненной;

b) полностью выполнить операцию «выбор» путем выбора одного или более пунктов;

c) ограничить операцию «выбор», удалив некоторые из вариантов, но оставив два или более.

Каждый раз, когда элемент в ЗБ предусматривает операцию «выбор», разработчик ЗБ должен завершить выполнение этой операции «выбор», как указано выше в варианте b). Варианты a) и c) для ЗБ не допускаются.

Пункт или пункты, выбранные при выполнении действий по вариантам b) и c), должны быть взяты из пунктов, предоставленных для выбора.

7.1.4 Операция «уточнение»

Операция «уточнение» может быть выполнена по отношению к любому требованию. Разработчик ПЗ/ЗБ выполняет уточнение путем изменения требования. Первое правило по отношению к уточнению состоит в том, чтобы ОО, удовлетворяющий уточненному требованию, также удовлетворял неуточненному требованию в контексте ПЗ/ЗБ (т. е. уточненное требование должно быть «более строгим», чем исходное требование). Если уточнение не удовлетворяет этому правилу, то результирующее уточненное требование считается расширенным требованием и будет рассматриваться как таковое.

Единственное исключение из этого правила состоит в том, что допускается, чтобы разработчик ПЗ/ЗБ уточнил ФТБ для его применения по отношению к некоторым, но не ко всем субъектам, объектам, операциям, атрибутам безопасности и/или внешним сущностям.

Однако это исключение не относится к уточнению ФТБ, которые взяты из ПЗ, о соответствии которым заявлено; эти ФТБ не могут быть уточнены таким образом, чтобы относиться к меньшему количеству субъектов, объектов, операций, атрибутов безопасности и/или внешних сущностей, чем ФТБ в ПЗ.

Второе правило по отношению к уточнению состоит в том, что уточнение должно быть связано с исходным компонентом.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, такие как перефразирование предложения, чтобы сделать его более понятным читателю. Не допускается, чтобы эти изменения каким-либо образом изменяли смысл требования.

7.2 Зависимости между компонентами

Между компонентами могут существовать зависимости. Зависимости возникают, когда компонент не самодостаточен и предполагает наличие другого компонента для обеспечения функциональных возможностей безопасности или доверия к безопасности.

Функциональные компоненты в ИСО/МЭК 15408-2 обычно имеют зависимости от других функциональных компонентов, также как некоторые компоненты доверия в ИСО/МЭК 15408-3 могут иметь зависимости от других компонентов ИСО/МЭК 15408-3. Могут быть также определены зависимости компонентов из ИСО/МЭК 15408-2 от компонентов из ИСО/МЭК 15408-3. Не исключено также наличие зависимостей расширенных функциональных компонентов от компонентов доверия или наоборот.

Описание зависимостей компонентов определяется с учетом определений компонентов в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3. Чтобы обеспечить полноту требований к ОО, следует удов-

летворить зависимости компонентов при включении в ПЗ и ЗБ требований, основанных на компонентах, имеющих зависимости. Зависимости следует также учитывать при формировании пакетов.

Другими словами, если компонент А имеет зависимость от компонента Б, это означает, что когда ПЗ/ЗБ содержит требование безопасности, основанное на компоненте А, ПЗ/ЗБ должен также содержать одно из следующего:

a) требование безопасности, основанное на компоненте Б;

b) требование безопасности, основанное на компоненте, более высоком по иерархии по отношению к Б;

c) обоснование, почему ПЗ/ЗБ не содержит требования безопасности, основанного на компоненте Б.

В случаях a) и b), когда требование безопасности включено вследствие наличия зависимости, может быть необходимым выполнить операции (назначение, итерация, уточнение, выбор) по отношению к этому требованию безопасности таким образом, чтобы обеспечить уверенность в том, что оно действительно удовлетворяет зависимость.

В случае c) в обосновании невключения требования следует отражать:

- либо почему нет необходимости в зависимости;
- либо, что зависимость учтена средой функционирования ОО; в данном случае в обосновании следует описать, каким образом в целях безопасности для среды функционирования учтена эта зависимость;
- либо, что зависимость учтена другими ФТБ некоторым другим способом (расширенные ФТБ, сочетание ФТБ и др.).

7.3 Расширенные компоненты

Согласно ИСО/МЭК 15408 необходимо, чтобы требования основывались на компонентах из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3 с двумя исключениями:

a) существуют цели безопасности для ОО, которые не могут быть преобразованы в ФТБ из ИСО/МЭК 15408-2, или существуют требования «третьей стороны» (например, законы, стандарты), которые не могут быть преобразованы в ТДБ из ИСО/МЭК 15408-3 (например, относящиеся к оценке криптографии);

b) цели безопасности могут быть выражены на основе компонентов из ИСО/МЭК 15408-2 и/или ИСО/МЭК 15408-3, но только с большими трудностями и/или сложностями.

В обоих случаях от разработчика ПЗ/ЗБ требуется определить собственные компоненты. Эти вновь определенные компоненты называются расширенными компонентами. Точно определенный расширенный компонент необходим для обеспечения контекста и значения расширенных ФТБ или ТДБ, основанных на этом компоненте.

После корректного определения новых компонентов разработчик ПЗ/ЗБ может затем базировать одно или более ФТБ или ТДБ на этих вновь определенных расширенных компонентах и использовать их таким же образом, как и другие ФТБ и ТДБ. С этого момента не существует каких-либо различий между ФТБ и ТДБ, основанными на ИСО/МЭК 15408, и ФТБ и ТДБ, основанными на расширенных компонентах. Дополнительные требования к расширенным компонентам изложены в семействах «Определение расширенных компонентов» (APE_ECD) и «Определение расширенных компонентов» (ASE_ECD) ИСО/МЭК 15408-3.

8 Профили защиты и пакеты

8.1 Введение

Чтобы дать возможность заинтересованным группам или сообществам потребителей выражать свои потребности безопасности и облегчить разработку ЗБ, данная часть ИСО/МЭК 15408 предоставляет две специальные конструкции: пакеты и профили защиты (ПЗ). В 8.2 и 8.3 эти конструкции описаны более подробно. В 8.4 объясняется, как эти конструкции могут быть использованы.

8.2 Пакеты

Пакет — это именованный набор требований безопасности. Пакеты делятся на:

- функциональные пакеты, включающие только ФТБ;
- пакеты доверия, включающие только ТДБ.

Смешанные пакеты, включающие как ФТБ, так и ТДБ, не допустимы.

Пакет может быть определен какой-либо стороной и предназначен для многократного использования. Для этой цели он должен включать требования, которые в сочетании являются полезными и эффективными.

Пакеты могут использоваться при создании более крупных пакетов, ПЗ и ЗБ. В настоящее время не существует критериев оценки пакетов, поэтому любой набор ФТБ или ТДБ может быть пакетом.

Примерами пакетов доверия являются оценочные уровни доверия (ОУД), определенные в ИСО/МЭК 15408-3.

8.3 Профили защиты

В то время как ЗБ всегда описывает конкретный ОО (например, межсетевой экран X-2, версия 3.1), ПЗ предназначен для описания типа ОО (например, межсетевые экраны прикладного уровня). Поэтому один и тот же ПЗ можно использовать в качестве шаблона для множества различных ЗБ, которые будут использовать в различных оценках. Подробное описание ПЗ приведено в приложении В.

Обычно ЗБ описывает требования для ОО и его формирует разработчик ОО, в то время как ПЗ описывает общие требования для некоторого типа ОО и поэтому обычно разрабатывается:

- сообществом пользователей, стремящихся прийти к консенсусу относительно требований для данного типа ОО;
- разработчиком ОО или группой разработчиков подобных ОО, желающих установить минимальный базис для конкретного типа ОО;
- правительственной организацией или крупной корпорацией, определяющими свои требования как часть процесса закупки.

ПЗ определяет допустимый тип соответствия ЗБ профилю защиты. То есть в ПЗ устанавливают (в разделе ПЗ «Утверждение о соответствии», см. В.5), какие типы соответствия являются допустимыми для ЗБ, а именно:

- если в ПЗ установлено, что требуется «строгое соответствие», то ЗБ должно в строгой форме соответствовать ПЗ;
- если в ПЗ установлено, что требуется «демонстрируемое соответствие», то ЗБ должно либо строго соответствовать ПЗ, либо его соответствие ПЗ может быть продемонстрировано.

Иными словами, для ЗБ допускается «демонстрируемое соответствие» ПЗ, только если ПЗ в явном виде это разрешает.

Если в ЗБ заявляют о соответствии нескольким ПЗ, то оно должно соответствовать (как описано выше) каждому из этих ПЗ в такой форме, как это предписано в этом ПЗ. Это подразумевает, что ЗБ может строго соответствовать одним ПЗ и демонстрируемо соответствовать другим ПЗ.

Задание по безопасности либо соответствует рассматриваемому ПЗ, либо не соответствует. ИСО/МЭК 15408 не признает «частичное» соответствие. Поэтому обязанность разработчика ПЗ — обеспечить, чтобы ПЗ не был чрезмерно перегруженным и не создавал бы, таким образом, препятствий разработчикам ПЗ/ЗБ при заявлении о соответствии ПЗ.

ЗБ эквивалентно ПЗ либо является более ограничительным, если:

- ОО, который удовлетворяет ЗБ, также удовлетворяет ПЗ;
- все среды функционирования, которые удовлетворяют ПЗ, также удовлетворяют ЗБ.

Проще говоря, ЗБ должен наложить те же самые или большие ограничения на ОО и те же самые или меньшие ограничения на среду функционирования ОО.

Это общее утверждение может быть более конкретизировано для различных подразделов ЗБ:

Определение проблемы безопасности: обоснование соответствия в ЗБ должно продемонстрировать, что определение проблемы безопасности в ЗБ является эквивалентным (или более ограничительным) по отношению к определению проблемы безопасности в ПЗ. Это означает, что:

- ОО, который бы отвечал определению проблемы безопасности в ЗБ, также отвечал бы определению проблемы безопасности в ПЗ;
- все среды функционирования, которые отвечали бы определению проблемы безопасности в ПЗ, также отвечали бы определению проблемы безопасности в ЗБ.

Цели безопасности: обоснование соответствия в ЗБ должно продемонстрировать, что цели безопасности в ЗБ являются эквивалентными (или более ограничительными) по отношению к целям безопасности в ПЗ. Это означает что:

- ОО, который бы отвечал целям безопасности для ОО в ЗБ, также отвечал бы целям безопасности для ОО в ПЗ;
- все среды функционирования, которые отвечали бы целям безопасности для среды функционирования в ПЗ, также отвечали бы целям безопасности для среды функционирования в ЗБ.

Если определено строгое соответствие профилям защиты, то применяют следующие требования:

a) Определение проблемы безопасности: ЗБ должно включать определение проблемы безопасности из ПЗ, может определять дополнительные угрозы и ПБОр, но не может определять дополнительные предположения;

b) Цели безопасности: ЗБ:

- должно включать все цели безопасности для ОО из ПЗ, но может определять дополнительные цели безопасности для ОО;
- должно включать все цели безопасности для среды функционирования (за одним исключением, указанным в следующем пункте данного перечисления), но не может определять дополнительные цели безопасности для среды функционирования;
- может определить, что определенные цели для среды функционирования из ПЗ являются целями безопасности для ОО в ЗБ. Это называется переназначением цели безопасности. Если цель безопасности переназначена для ОО, то обоснование целей безопасности должно четко показать, какое предположение или часть предположения больше не требуются.

c) Требования безопасности: ЗБ должно включать все ФТБ и ТДБ из ПЗ, но может определять дополнительные или иерархичные, более строгие ФТБ и ТДБ. Выполнение операций в ЗБ должно быть согласовано с выполнением операций в ПЗ; либо выполнение операций в ЗБ будет таким же, как и в ПЗ, либо приведет к более ограничивающим требованиям (при применении правил уточнения).

Если определено «демонстрируемое соответствие» профилям защиты, то применяют следующие требования:

- ЗБ должно включать обоснование того, почему ЗБ рассматривается как «эквивалентное или более ограничительное» по отношению к ПЗ;
- демонстрируемое соответствие позволяет разработчику ПЗ описать общую проблему безопасности, которая должна быть решена, и обеспечить общее руководство по требованиям, необходимым для ее решения, с пониманием того, что, вероятно, существует более чем один способ ее решения.

Оценка ПЗ является необязательной. Оценка выполняется с применением к нему критериев класса APE, перечисленных в ИСО/МЭК 15408-3. Цель такой оценки состоит в том, чтобы продемонстрировать, что ПЗ полный, непротиворечивый, технически правильный и, таким образом, подходящий для использования в качестве шаблона для формирования других ПЗ или ЗБ.

Базирование ПЗ/ЗБ на оцененном ПЗ имеет два преимущества:

- существует намного меньше риска, что в ПЗ есть ошибки, неясности или пропуски. Если какие-либо проблемы с ПЗ (которые были бы выявлены при оценке этого ПЗ) обнаружат во время разработки или оценки нового ЗБ, то может пройти значительное время прежде, чем ПЗ будет исправлен;
- при оценке новых ПЗ/ЗБ часто могут быть повторно использованы результаты оценки оцененного ПЗ, что обеспечивает уменьшение усилий по оценке новых ПЗ/ЗБ.

Взаимосвязь между содержанием ПЗ, ЗБ и ОО продемонстрирована на рисунке 4.

8.4 Использование ПЗ и пакетов

Если в ЗБ утверждается о соответствии одному или более пакету и/или профилю защиты, оценка данного ЗБ будет (среди других характеристик данного ЗБ) демонстрировать, что ЗБ действительно соответствует этим пакетам и/или ПЗ, по отношению к которым утверждается о соответствии. Подробности этого определения соответствия можно найти в приложении А.

Это делает возможным следующий процесс:

a) организация, заинтересованная в приобретении конкретного типа продукта безопасности ИТ, излагает свои потребности в безопасности в ПЗ, затем обеспечивает его оценку и выпуск;

b) разработчик получает этот ПЗ, разрабатывает ЗБ, которое содержит утверждение о соответствии данному ПЗ, и обеспечивает оценку этого ЗБ;

c) затем разработчик создает ОО (или использует существующий) и обеспечивает его оценку на соответствие ЗБ.

В результате разработчик может доказать, что его ОО удовлетворяет потребностям в безопасности организации: поэтому организация может закупить этот ОО. Аналогичный порядок может применяться в отношении пакетов.

8.5 Многократное использование профилей защиты

ИСО/МЭК 15408 также допускает соответствие профилей защиты другим ПЗ, предусматривая создание цепочек профилей защиты, в которых каждый последующий ПЗ базируется на предыдущем (предыдущих) ПЗ.

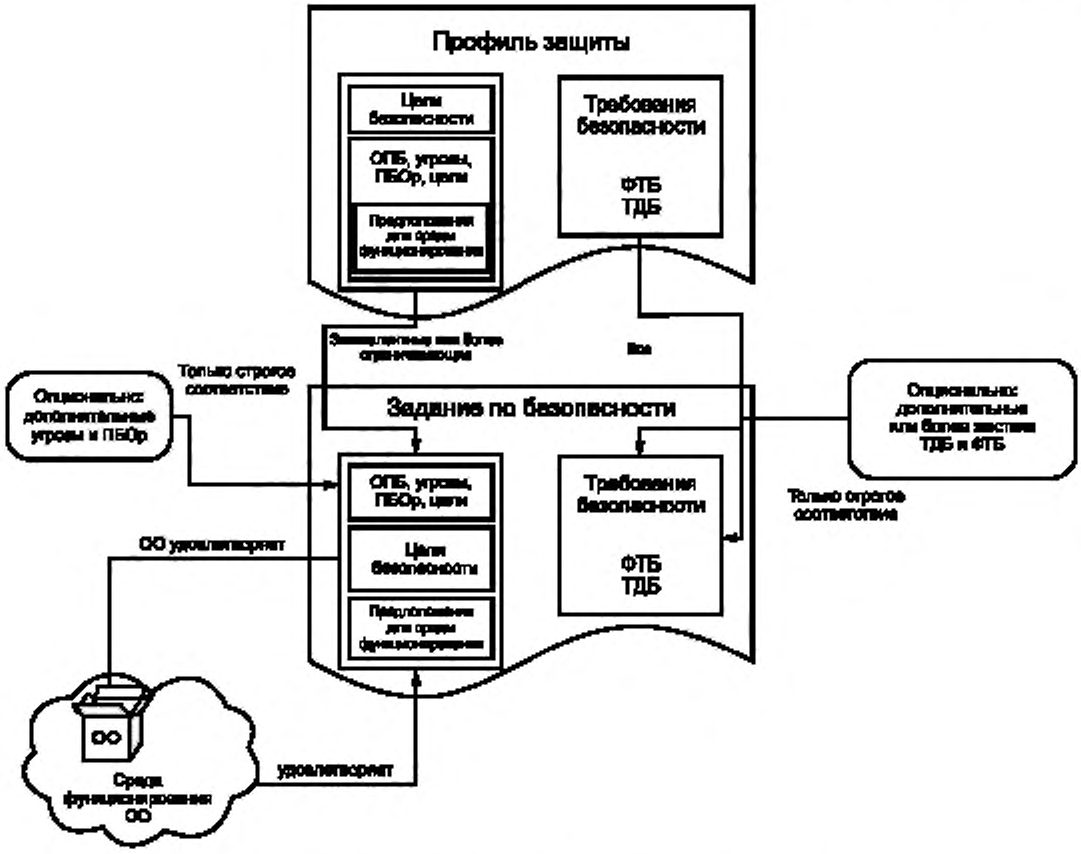

Рисунок 4 — Взаимосвязь между содержанием ПЗ, ЗБ и ОО

Например, можно было бы взять ПЗ для интегральной схемы и ПЗ для ОС смарт-карты и использовать их для разработки ПЗ для смарт-карты (ИС и ОС), в котором утверждается о соответствии двум исходным ПЗ. Затем можно было бы разработать ПЗ для смарт-карт для общественного транспорта, базируясь на ПЗ для смарт-карт и ПЗ для загружаемого в них приложения. В конечном счете, разработчик мог бы затем разработать ЗБ, базируясь на этом ПЗ для смарт-карт для общественного транспорта.

9 Результаты оценки

9.1 Введение

В этом разделе представлены ожидаемые результаты оценки ПЗ и ЗБ/ОО, выполненной в соответствии с ИСО/МЭК 18045:

- оценки профилей защиты позволяют создавать каталоги (реестры) оцененных ПЗ;
- оценка ЗБ дает промежуточные результаты, которые затем используются при оценке ОО;
- оценки ЗБ/ОО позволяют создавать каталоги (реестры) оцененных ОО. Во многих случаях эти каталоги будут ссылаться на продукты ИТ, на основе которых определены эти ОО, а не на конкретные ОО. Следовательно, наличие продукта ИТ в каталоге не должно интерпретироваться как признак того, что весь продукт ИТ прошел оценку; реальный объем оценки ЗБ/ОО определяется ЗБ. Ссылка на портал с примерами таких каталогов приведена в разделе «Библиография».

На рисунке 5 продемонстрированы ожидаемые результаты оценки ПЗ и ЗБ/ОО.

ЗБ могут базироваться на пакетах, оцененных ПЗ, неоцененных ПЗ; тем не менее, совсем не обязательно, чтобы ЗБ на чем-то базировались.

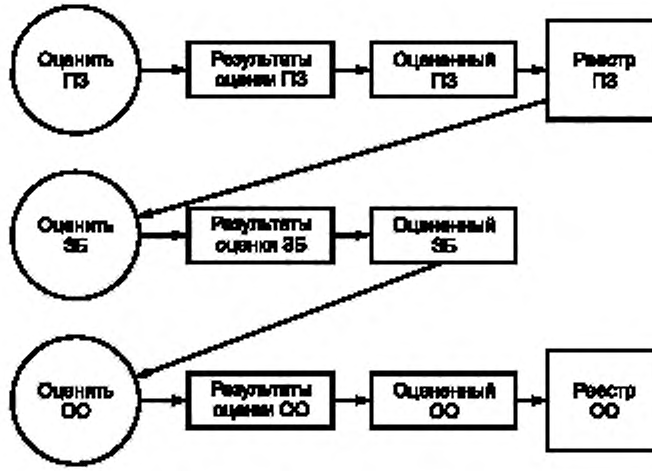

Рисунок 5 — Результаты оценки

Необходимо, чтобы оценка приводила к объективным и повторяемым результатам, на которые затем можно ссылаться как на свидетельство даже при отсутствии абсолютно объективной шкалы для представления результатов оценки безопасности ИТ. Наличие совокупности критериев оценки является необходимым предварительным условием для того, чтобы оценка приводила к значимому результату, предоставляя техническую основу для взаимного признания результатов оценки различными органами оценки.

Результат оценки представляет собой итоговые данные специфического типа исследования характеристик безопасности ОО. Такой результат не гарантирует пригодность к использованию в какой-либо конкретной среде применения. Решение о приемке ОО к использованию в конкретной среде применения основывается на учете многих аспектов безопасности, включая и выводы оценки.

9.2 Результаты оценки ПЗ

ИСО/МЭК 15408-3 содержит критерии оценки, которые оценщику необходимо принять во внимание для того, чтобы установить, является ли ПЗ полным, непротиворечивым, технически правильным и, следовательно, пригодным для использования при разработке ЗБ.

Результаты оценки должны также включать «Утверждение о соответствии» (см. 9.4).

9.3 Результаты оценки ЗБ/ОО

ИСО/МЭК 15408-3 содержит критерии оценки, которые оценщику необходимо принять во внимание для того, чтобы установить, существует ли достаточное доверие к тому, что ОО удовлетворяет ФТБ из ЗБ.

Результат оценки ОО должен формулироваться как «соответствие/несоответствие» по отношению к ЗБ. Если и для ЗБ, и для ОО результат оценки — «соответствует», то соответствующий продукт получает право включения в реестр. Результаты оценки должны также включать «Утверждение о соответствии», как определено в 9.4.

Возможно, результаты оценки в дальнейшем будут использованы в процессе сертификации, но этот процесс находится за рамками ИСО/МЭК 15408.

9.4 Утверждение о соответствии

Утверждение о соответствии указывает источник совокупности требований, которым удовлетворяет ПЗ или ЗБ, проходящие оценку. Это утверждение о соответствии содержит утверждение о соответствии ИСО/МЭК 15408, которое:

a) описывает ту версию ИСО/МЭК 15408, о соответствии которой заявлено в ПЗ или ЗБ;

b) описывает соответствие ИСО/МЭК 15408-2 (функциональные требования безопасности), включающее одно из следующего:

- «соответствие ИСО/МЭК 15408-2» — ПЗ или ЗБ соответствует ИСО/МЭК 15408-2, если все ФТБ в данном ПЗ или ЗБ основаны только на функциональных компонентах из ИСО/МЭК 15408-2;

- «расширение ИСО/МЭК 15408-2» — ПЗ или ЗБ является расширенным по отношению к ИСО/МЭК 15408-2, если как минимум одно ФТБ в данном ПЗ или ЗБ не основано на функциональных компонентах из ИСО/МЭК 15408-2;

c) описывает соответствие ИСО/МЭК 15408-3 (требования доверия к безопасности), включающее одно из следующего:

- «соответствие ИСО/МЭК 15408-3» — ПЗ или ЗБ соответствует ИСО/МЭК 15408-3, если все ТДБ в данном ПЗ или ЗБ основаны только на компонентах доверия из ИСО/МЭК 15408-3;

- «расширение ИСО/МЭК 15408-3» — ПЗ или ЗБ является расширенным по отношению к ИСО/МЭК 15408-3, если как минимум одно ТДБ в данном ПЗ или ЗБ не основано на компонентах доверия из ИСО/МЭК 15408-3.

Кроме того, утверждение о соответствии может включать утверждение, сделанное относительно пакетов требований; в данном случае оно включает одно из следующего:

- «соответствие именованному пакету» — ПЗ или ЗБ соответствует предопределенному именованному пакету (например, ОУД), если:

ФТБ в ПЗ или ЗБ идентичны ФТБ в пакете или ТДБ в ПЗ или ЗБ идентичны ТДБ в пакете;

- «усиление именованного пакета» — ПЗ или ЗБ является усилением предопределенного именованного пакета, если:

ФТБ в ПЗ или ЗБ включают все ФТБ из пакета, а также содержат как минимум одно дополнительное ФТБ или ФТБ, которое является иерархичным по отношению к некоторому ФТБ из пакета;

ТДБ в ПЗ или ЗБ включают все ТДБ из пакета, а также содержат как минимум одно дополнительное ТДБ или ТДБ, которое является иерархичным по отношению к некоторому ТДБ из пакета.

При успешном прохождении ОО оценки на соответствие ЗБ, любые утверждения о соответствии задания по безопасности также относятся и к ОО. Таким образом, ОО также, например, может соответствовать ИСО/МЭК 15408-2.

И наконец, утверждение о соответствии может также включать два утверждения относительно профилей защиты:

a) «соответствие ПЗ» — ПЗ или ОО удовлетворяет конкретному(ым) профилю (ям) защиты, который(ые) перечислен(ы) как часть утверждения о соответствии;

b) «изложение соответствия» (только для профилей защиты) — В данном изложении описывается способ, которым должно быть обеспечено соответствие профилей защиты или заданий по безопасности рассматриваемому ПЗ: строгое или демонстрируемое. Более подробная информация по вопросу «изложения соответствия» приведена в приложении В.

9.5 Использование результатов оценки ЗБ/ОО

После оценки ЗБ и ОО у владельцев активов имеется доверие (как определено в ЗБ) к тому, что ОО вместе со средой функционирования противостоят конкретным угрозам. Результаты оценки могут быть использованы владельцем активов при принятии решения о принятии риска, связанного с подверженностью активов воздействию конкретных угроз.

При этом владелец активов должен тщательно проверить следующее:

- соответствует ли определение проблемы безопасности в ЗБ конкретной проблеме безопасности владельца активов;

- соответствует ли среда функционирования у владельца активов (или может ли быть обеспечено ее соответствие) целям безопасности для среды функционирования, описанным в ЗБ.

Если что-либо из перечисленного не выполняется, то ОО может оказаться непригодным с точки зрения целей владельца активов.

После ввода оцененного ОО в эксплуатацию сохраняется возможность проявления в ОО ранее неизвестных ошибок или уязвимостей. В этом случае разработчик может внести изменения в ОО (чтобы устранить уязвимости) или изменить ЗБ, чтобы исключить уязвимости из области оценки. В любом случае прежние результаты оценки могут оказаться уже недействительными.

Если окажется необходимым восстановить уверенность, то потребуется переоценка. Для переоценки может быть использован ИСО/МЭК 15408, однако подробные процедуры переоценки находятся вне области данной части ИСО/МЭК 15408.

Приложение А
(справочное)

Спецификация заданий по безопасности

А.1 Цель и структура данного приложения

Цель данного приложения состоит в изложении концепции задания по безопасности (ЗБ). В данном приложении не определены критерии класса ASE; соответствующее определение содержится в ИСО/МЭК 15408-3 и поддержано документами, приведенными в разделе «Библиография».

Приложение А состоит из четырех основных частей:

a) Что должно содержать ЗБ. Краткая информация по этому вопросу изложена в А.2, более подробно в А.4—А.10. В указанных подразделах описано обязательное содержание ЗБ, взаимосвязи в рамках содержания ЗБ, а также представлены примеры.

b) Как следует использовать ЗБ. Краткая информация по этому вопросу изложена в А.3, более подробно — в А.11. В указанных разделах описано, каким образом следует использовать ЗБ, а также приведены вопросы, на которые могут быть даны ответы в ЗБ.

c) ЗБ для низкого уровня доверия (упрощенное ЗБ). ЗБ для низкого уровня доверия представляют собой ЗБ с сокращенным содержанием. Такие ЗБ описаны в А.12.

d) Утверждение о соответствии стандартам. В разделе А.13 описано, каким образом разработчик ЗБ может сделать утверждение, что ОО удовлетворяет некоторому конкретному стандарту.

А.2 Обязательное содержание ЗБ

На рисунке А.1 представлено содержание ЗБ, установленное в ИСО/МЭК 15408-3. Рисунок А.1 также можно использовать как структурную схему ЗБ, хотя допустимы и альтернативные структуры. Например, если обоснование требований безопасности является очень объемным, то оно может быть вынесено в приложение к ЗБ вместо включения в раздел «Требования безопасности». Разделы ЗБ и содержание этих разделов кратко рассмотрены ниже; в А.4—А.10 приведены более подробные пояснения. ЗБ обычно содержит:

a) раздел «Введение ЗБ», содержащий описание ОО на трех различных уровнях абстракции;

b) раздел «Утверждения о соответствии», указывающий, утверждается ли в ЗБ о соответствии каким-либо ПЗ и/или пакетам, и если «да», то каким ПЗ и/или пакетам;

c) раздел «Определение проблемы безопасности», в котором указываются угрозы, ПБОр и предположения;

d) раздел «Цели безопасности», показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;

e) раздел «Определение расширенных компонентов» (опционально), в котором могут быть определены новые компоненты (т. е. компоненты, не содержащиеся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;

f) раздел «Требования безопасности», в котором цели безопасности для ОО преобразованы в изложение на стандартизованном языке. Этот стандартизированный язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ;

g) раздел «Краткая спецификация ОО», показывающий, как ФТБ реализованы в ОО.

Существуют также ЗБ для низкого уровня доверия, имеющие сокращенное содержание; подробно такие ЗБ описаны в А.12. Все остальные части данного приложения предполагают ЗБ с полным содержанием.

А.3 Использование ЗБ

А.3.1 Как следует использовать ЗБ

Типовое ЗБ выполняет две роли:

Перед оценкой и в процессе оценки ЗБ определяет, «что должно быть оценено». В этой роли ЗБ служит основой для соглашения между разработчиком и оценщиком о точных характеристиках безопасности ОО и точной области оценки. Техническая правильность и полнота являются основными проблемными вопросами для этой роли. В разделе А.7 описано, каким образом следует использовать ЗБ в данной роли.

После оценки ЗБ определяет, «что было оценено». В этой роли ЗБ служит основанием для соглашения между разработчиком или поставщиком ОО и потенциальным потребителем ОО. ЗБ описывает точные характеристики безопасности ОО в краткой форме, и потенциальный потребитель может доверять этому описанию, так как ОО был оценен на предмет удовлетворения данному ЗБ. Удобство использования и понятность являются основными проблемными вопросами для этой роли. В разделе А.11 описано, каким образом следует использовать ЗБ в данной роли.

А.3.2 Как не следует использовать ЗБ

Две роли (из многих), для которых не следует использовать ЗБ:

- детальная спецификация: ЗБ разрабатывается в качестве спецификации безопасности на относительно высоком уровне абстракции. Обычно в ЗБ не следует включать детальные спецификации протоколов, детальное описание алгоритмов и/или механизмов, длинное описание детализированных операций и т. д.;



Рисунок А.1 — Содержание задания по безопасности

- полная спецификация: ЗБ разрабатывается в качестве спецификации безопасности, а не общей спецификации. Кроме относящихся к безопасности, другие характеристики, такие как возможности взаимодействия, физические размеры и масса, требуемое напряжение и т. д., не следует включать в ЗБ. Это означает, что в целом ЗБ может быть частью полной спецификации, но не полной спецификацией само по себе.

А.4 Введение ЗБ (ASE_INT)

В разделе «Введение ЗБ» описывают ОО в повествовательной форме на трех уровнях абстракции:

a) ссылка на ЗБ и ссылка на ОО, обеспечивающие идентификационные материалы для ЗБ и ОО, на который ссылается ЗБ;

b) аннотация ОО, в которой кратко описывается ОО;

c) описание ОО, в котором более подробно описывается ОО.

А.4.1 Ссылка на ЗБ и ссылка на ОО

ЗБ содержит четкую ссылку на ЗБ, которая идентифицирует данное ЗБ. Типичная ссылка на ЗБ состоит из наименования ЗБ, версии, разработчика и даты выпуска. Пример ссылки на ЗБ — «MauveRAM Database ST, version 1.3, MauveCorp Specification Team, 11 October 2002».

ЗБ также содержит ссылку на ОО, идентифицирующую ОО, для которого требуется соответствие ЗБ. Типичная ссылка на ОО состоит из наименования разработчика, наименования ОО и номера версии ОО. Пример ссылки на ОО — «MauveCorp MauveRAM Database v2.11». Поскольку один и тот же ОО может быть оценен несколько раз, например, по инициативе различных потребителей этого ОО, для него может существовать несколько ЗБ, и поэтому ссылка на ОО не обязательно является уникальной.

Если ОО сформирован на основе одного или более известных продуктов, то допускается отразить это в ссылке на ОО путем указания наименований этих продуктов. Однако это не должно вводить потребителей в заблуждение: ситуации, когда основные части или функциональные возможности безопасности не были рассмотрены в процессе оценке, но в ссылке на ОО это не отражено, являются недопустимыми.

Ссылка на ЗБ и ссылка на ОО облегчают индексацию и ссылку на ЗБ и ОО и их включение в состав сводной информации списков оцененных ОО/продуктов.

А.4.2 Аннотация ОО

Аннотация ОО нацелена на потенциальных потребителей ОО, просматривающих списки оцененных ОО/продуктов, чтобы найти ОО, которые могут удовлетворить их потребности в безопасности и поддерживаться их аппаратным, программным и программно-аппаратным обеспечением. Как правило, объем аннотации ОО — несколько параграфов.

В аннотации ОО кратко описывают использование ОО и его основные характеристики безопасности, идентифицируют тип ОО и все основные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО, но требуемые для ОО.

А.4.2.1 Использование и основные характеристики безопасности ОО

Описание использования и основных характеристик безопасности ОО предназначено, чтобы дать общее представление о возможностях ОО с точки зрения безопасности и о том, для чего можно использовать ОО в контексте безопасности. Это должно быть написано для (потенциальных) потребителей ОО с описанием использования и основных характеристик ОО в терминах бизнес-операций и на языке, понятном потребителям.

Пример такого описания: «The MauveCorp MauveRAM Database v2.11 является многопользовательской системой управления базами данных, предназначенной для использования в сетевой среде. Она предоставляет возможность одновременной работы до 1024 пользователей, возможность использовать аутентификацию, основанную на пароле/токене, а также — биометрическую аутентификацию; обеспечивает защиту от случайного повреждения данных и откат назад на десять тысяч транзакций. Существует возможность настройки механизмов аудита в широком диапазоне, позволяющая осуществлять детальный аудит по отношению к некоторым пользователям и транзакциям, обеспечивая при этом приватность для других пользователей и транзакций».

А.4.2.2 Тип ОО

В аннотации ОО идентифицируют общий тип ОО, такой как: межсетевой экран, шлюз виртуальной частной сети, смарт-карта, интранет, веб-сервер, система управления базами данных, веб-сервер вместе с системой управления базами данных, ЛВС, ЛВС с веб-сервером и системой управления базой данных и др.

Возможна ситуация, когда ОО не может быть легко отнесен к имеющемуся типу, при которой приемлемым является указание на то, что ОО не отнесен ни к одному типу.

В некоторых случаях тип ОО может ввести в заблуждение потребителей. Например:

- от ОО с учетом его типа могут ожидать определенные функциональные возможности, в то время как у данного ОО эти функциональные возможности отсутствуют. Например:

  ОО типа «АТМ-карта», который не поддерживает какие-либо функциональные возможности идентификации/аутентификации;

  ОО типа «межсетевой экран», который не поддерживает протоколы, используемые почти повсеместно;

  ОО типа «ИОК», у которого нет функциональных возможностей аннулирования сертификатов.

- от ОО с учетом его типа могут ожидать возможность функционирования в определенной среде, в то время как для данного ОО такая возможность отсутствует. Например:

  ОО типа «операционная система ПК», который не может безопасно функционировать при наличии у ПК сетевого подключения, накопителя на гибких дисках, CD/DVD-дисковода;

  межсетевой экран, который может безопасно функционировать только при условии, что все пользователи, которые могут подключаться через этот межсетевой экран, являются благонадежными.

А.4.2.3 Требуемые аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО

В то время как некоторые ОО не зависят от других ИТ, многие ОО (особенно программные ОО) зависят от дополнительных, не входящих в ОО, аппаратных средств/программного обеспечения и/или программно-аппаратных средств. В последнем случае в «Аннотации ОО» требуется идентифицировать соответствующие, не входящие в ОО, аппаратные средства/программное обеспечение и/или программно-аппаратные средства. Полная и абсолютно детальная идентификация дополнительных аппаратных средств/программного обеспечения и/или программно-аппаратных средств не требуется, но при этом необходима полнота и детализация идентификации, достаточная для определения потенциальными потребителями основных аппаратных средств, программного обеспечения и/или программно-аппаратных средств, необходимых для использования ОО.

Примеры идентификации аппаратных средств/программного обеспечения/программно-аппаратных средств:

- стандартный ПК с процессором 1ГГц или более и ОП 512 Мб или более, функционирующий под управлением операционной системы Yaiza версии 3.0 с установленным обновлением 6d, с или 7 или версии 4.0;
- стандартный ПК с процессором 1ГГц или более и ОП 512 Мб или более, функционирующий под управлением операционной системы Yaiza версии 3.0 с установленным обновлением 6d, с, установленной графической картой WonderMagic 1.0 с набором драйверов для WM версии 1.0;
- стандартный ПК с операционной системой Yaiza версии 3.0 (или выше);
- интегральная схема CleverCard SB2067;
- интегральная схема CleverCard SB2067 с установленной операционной системой для смарт-карт QuickOS;

- локальная вычислительная сеть департамента транспорта по состоянию на декабрь 2002 года.

А.4.3 Описание ОО

«Описание ОО» представляет собой описание ОО в повествовательной форме, возможно в объеме нескольких страниц. Описание ОО должно обеспечить оценщикам и потенциальным потребителям общее понимание возможностей безопасности ОО с большей детализацией, чем в аннотации ОО. Описание ОО можно также использовать для описания более широкого прикладного контекста, для которого ОО будет подходящим.

В описании ОО рассматривают физические границы ОО: список всех аппаратных, программно-аппаратных, программных частей и руководства, которые составляют ОО. Этот список должен быть описан на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих частей.

В описании ОО следует также рассмотреть логические границы ОО: логические характеристики безопасности, обеспечиваемые ОО, на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих характеристик. Предполагается, что данное описание будет более подробным, чем описание общих характеристик безопасности в аннотации ОО.

Важная роль физических и логических границ заключается в том, что они описывают ОО способом, не оставляющим неясностей в том, входит ли определенная часть или характеристика в ОО или не входит. Это особенно важно, когда ОО интегрирован с сущностями, не входящими в ОО, и не может быть легко выделен из них.

Примеры, когда ОО интегрирован с сущностями, не входящими в ОО:

- ОО является ИС смарт-карты, за исключением криптографического сопроцессора;
- ОО является частью межсетевого экрана MinuteGap версии 18.5, связанной с трансляцией сетевых адресов.

А.5 Утверждения о соответствии (ASE_CCL)

В данном подразделе ЗБ описывается соответствие ЗБ:

- части 2 и части 3 настоящего стандарта;
- профилям защиты (если применимо);
- пакетам (если применимо).

Описание соответствия ЗБ ИСО/МЭК 15408 состоит из двух пунктов: ссылка на используемый ИСО/МЭК 15408 и указание на то, содержит ли ЗБ расширенные требования безопасности или не содержит (см. А.8).

Описание соответствия ЗБ профилям защиты предусматривает перечисление в ЗБ профилей защиты, по отношению к которым требуется соответствие. Пояснения см. в 9.4.

Описание соответствия ЗБ пакетам предусматривает перечисление в ЗБ пакетов, по отношению к которым требуется соответствие. Пояснения см. в 9.4.

А.6 Определение проблемы безопасности (ASE_SPD)

А.6.1 Введение

В разделе ЗБ «Определение проблемы безопасности» определяется проблема безопасности, которая должна быть решена. Определение проблемы безопасности относительно ИСО/МЭК 15408 является аксиоматическим. Таким образом, процесс установления определения проблемы безопасности находится вне области применения ИСО/МЭК 15408.

Однако полноценность результатов оценки в существенной степени зависит от ЗБ, а полноценность ЗБ в существенной степени зависит от качества определения проблемы безопасности. Поэтому зачастую необходимо потратить существенные ресурсы и использовать четкие процессы и процедуры анализа, чтобы получить надлежащее определение проблемы безопасности.

Согласно ИСО/МЭК 15408-3 не обязательно иметь изложение всех подразделов определения проблемы безопасности; ЗБ, в котором изложены угрозы, не обязательно должно содержать изложение ПБОр и наоборот. Кроме того, в ЗБ могут быть опущены предположения.

Когда ОО является физически распределенным, может оказаться предпочтительным рассмотреть соответствующие угрозы, ПБОр и предположения отдельно для различных областей (доменов) среды функционирования ОО.

А.6.2 Угрозы

Данный подраздел раздела «Определение проблемы безопасности» представляет угрозы, которым должен противостоять ОО, его среда функционирования или их сочетание.

Угроза определяется негативным действием, выполняемым источником угрозы по отношению к некоторому активу.

Негативные действия — действия, выполняемые источником угрозы по отношению к некоторому активу. Эти действия влияют на одну или более характеристик актива, которые связаны со значимостью данного актива.

Источники угроз могут быть описаны как отдельные сущности, но в некоторых случаях может оказаться предпочтительным описать их как типы сущностей, группы сущностей и т. п.

Примеры источников угроз — хакеры, пользователи, компьютерные процессы и инциденты. Далее источники угроз могут быть описаны через такие аспекты, как компетентность, доступные ресурсы, возможности и мотивация.

Примеры угроз:

- хакер (со значительной компетентностью, стандартным оборудованием и профинансированный для реализации угрозы), осуществляющий удаленное копирование конфиденциальных файлов из сети компании;
- компьютерный «червь», существенно снижающий производительность глобальной сети;
- системный администратор, нарушающий приватность пользователя;
- пользователь Интернета, прослушивающий трафик конфиденциального электронного обмена.

А.6.3 Политика безопасности организации (ПБОр)

Данный подраздел раздела «Определение проблемы безопасности» представляет ПБОр, которые должны быть реализованы ОО, его средой функционирования или их сочетанием.

ПБОр — правила безопасности, процедуры или руководящие принципы, предписанные (или предполагаемые быть предписанными) в настоящее время и/или в будущем фактической или гипотетической организацией в среде функционирования. ПБОр может быть установлена организацией, управляющей средой функционирования ОО, или может быть установлена законодательными или регулирующими органами. ПБОр может относиться к ОО и/или к среде функционирования ОО.

Примеры ПБОр:

- все продукты, которые используются государственными организациями, должны соответствовать национальным стандартам по генерации пароля и криптографии;
- только пользователям с привилегиями системного администратора и допуском секретного отдела должно быть разрешено управление файл-сервером Департамента.

А.6.4 Предположения

Данный подраздел раздела «Определение проблемы безопасности» представляет предположения, которые сделаны по отношению к среде функционирования ОО для обеспечения функциональных возможностей безопасности. Если ОО помещен в среду функционирования, которая не отвечает этим предположениям, то ОО, возможно, окажется уже не в состоянии обеспечить все свои функциональные возможности безопасности. Предположения могут быть по отношению к физическим аспектам, персоналу и внешней связности в среде функционирования.

Примеры предположений:

- предположения, связанные с физическими аспектами среды функционирования:
- предполагается, что ОО будет размещен в помещении, где выполнены работы по минимизации электромагнитных излучений;
- предполагается, что консоли администратора ОО будут помещены в зону ограниченного доступа.
- предположения, связанные с персоналом среды функционирования:
  - предполагается, что пользователи ОО будут в достаточной степени обученными, чтобы эксплуатировать ОО;
  - предполагается, что пользователи ОО допущены к информации ограниченного доступа;
  - предполагается, что пользователи ОО не будут записывать свои пароли.
  - предположения по отношению к аспектам связности среды функционирования:
  - предполагается, что на автоматизированном рабочем месте на базе ПК для работы ОО доступно как минимум 10 Гб дискового пространства;
  - предполагается, что ОО является единственным, кроме ОС, приложением, работающим на конкретной рабочей станции;
  - предполагается, что ОО не будет связан с недоверенной сетью.

В процессе оценки эти предположения считаются верными: они в любом случае не проверяются.

По этим причинам предположения могут быть сделаны только по отношению к среде функционирования. Предположения никогда не могут делаться по отношению к режиму функционирования ОО, потому что оценка состоит из оценки утверждений, сделанных по отношению к ОО, а не из предположений, что утверждения по отношению к ОО являются верными.

А.7 Цели безопасности (ASE_OBJ)

Цели безопасности — это краткое и абстрактное изложение предполагаемого решения проблемы, определенной в разделе ЗБ «Определение проблемы безопасности». У целей безопасности тройная роль:

- предоставить высокоуровневое на естественном языке описание решения проблемы;
- разделить данное решение на две части, отражающие, что различные сущности решают свою часть проблемы;
- продемонстрировать, что эти части решения формируют полное решение проблемы.

А.7.1 Высокоуровневое решение

Цели безопасности состоят из совокупности коротких и четких утверждений без чрезмерно больших подробностей, которые формируют высокоуровневое решение проблемы безопасности. Уровень абстракции целей безопасности должен быть таким, чтобы они были ясными и понятными для хорошо осведомленных потенциальных потребителей ОО. Цели безопасности излагаются на естественном языке.

А.7.2 Части решения проблемы

В ЗБ высокоуровневое решение проблемы, которое описывается целями безопасности, делится на две части. Эти части описания решения названы целями безопасности для ОО и целями безопасности для среды функционирования. Это отражает, что данные части решения обеспечиваются двумя различными сущностями: ОО и средой функционирования.

А.7.2.1 Цели безопасности для ОО

ОО обеспечивает функциональные возможности безопасности для решения некоторой части проблемы, определенной в разделе ЗБ «Определение проблемы безопасности». Данная часть решения названа целями безопасности для ОО и включает совокупность целей, которые должны быть достигнуты ОО, чтобы решить свою часть проблемы.

Примеры целей безопасности для ОО:

- ОО должен обеспечивать конфиденциальность содержания всех файлов, передаваемых между ним и сервером;
- ОО должен выполнять идентификацию и аутентификацию всех пользователей до предоставления им доступа к сервису передачи информации, предоставляемого ОО;
- ОО должен ограничить доступ пользователей к данным согласно политике доступа к данным, описанной в приложении к ЗБ.

Если ОО является физически распределенным, может оказаться предпочтительным разделить подраздел ЗБ, содержащий цели безопасности для ОО, на несколько пунктов, чтобы учесть это.

А.7.2.2 Цели безопасности для среды функционирования

В среде функционирования ОО применяются технические и процедурные меры для поддержки ОО в отношении корректной реализации его функциональных возможностей безопасности (которые определены целями безопасности для ОО). Данная часть решения проблемы названа целями безопасности для среды функционирования и включает совокупность утверждений, описывающих цели, которые должны быть достигнуты средой функционирования.

Примеры целей безопасности для среды функционирования:

- в среде функционирования должно быть предоставлено автоматизированное рабочее место с установленной ОС Inux версии 3.01b для функционирования ОО на его базе;
- в среде функционирования должно быть обеспечено, чтобы все люди — пользователи ОО были соответствующим образом обучены до того, как им будет разрешено работать с ОО;
- среда функционирования ОО должна ограничить физический доступ к ОО, разрешая такой доступ только персоналу, выполняющему функции администраторов, и персоналу технической поддержки в сопровождении администраторов;
- среда функционирования должна обеспечить конфиденциальность журналов аудита, сгенерированных ОО, до их отправки на центральный сервер аудита.

Если среда функционирования ОО состоит из нескольких областей, каждая из которых обладает разными характеристиками, может оказаться предпочтительным разделить подраздел ЗБ, содержащий цели безопасности для среды функционирования, на несколько пунктов, чтобы учесть это.

А.7.3 Взаимосвязь между целями безопасности и определением проблемы безопасности

ЗБ также содержит подраздел «Обоснование целей безопасности», включающий два пункта:

- прослеживание, показывающее, какие цели безопасности направлены на какие угрозы, ПБОр и предположения;
- совокупность логических обоснований, показывающих, что все угрозы, ПБОр и предположения надлежащим образом учтены в целях безопасности.

А.7.3.1 Прослеживание целей безопасности к определению проблемы безопасности

Прослеживание показывает, каким образом цели безопасности сопоставлены с угрозами, ПБОр и предположениям, приведенным в разделе «Определение проблемы безопасности», обеспечивая при этом следующее:

a) Отсутствие избыточных целей: каждая цель безопасности сопоставлена, по крайней мере, с одной угрозой, ПБОр или предположением.

b) Полноту по отношению к определению проблемы безопасности: для каждой угрозы, ПБОр и предположения имеется, по крайней мере, одна цель безопасности, сопоставленная с ними.

c) Корректность сопоставления: так как предположения всегда делаются по отношению к среде функционирования, то цели безопасности для ОО не сопоставляются с предположениями. Сопоставления, допустимые в соответствии с ИСО/МЭК 15408-3, представлены на рисунке А.2.



Рисунок А.2 — Сопоставление целей безопасности и определения проблемы безопасности

Несколько целей безопасности могут быть сопоставлены с одной и той же угрозой, указывая на то, что сочетание этих целей безопасности направлено на противостояние данной угрозе. Подобное утверждение справедливо для ПБОр и предположений.

А.7.3.2 Предоставление логического обоснования для сопоставления

Обоснование целей безопасности демонстрирует, что сопоставление является надлежащим: все определенные угрозы, ПБОр и предположения учтены (т.е., угрозам обеспечено противостояние, ПБОр осуществлена, предположения реализованы, если все цели безопасности, сопоставленные с конкретной угрозой, ПБОр или предположением, достигнуты).

Данная демонстрация содержит результаты анализа эффекта от достижения соответствующих целей безопасности по противостоянию угрозам, осуществлению ПБОр и реализации предположений и приводит к заключению, что это действительно так.

В некоторых случаях, когда элементы «Определения проблемы безопасности» являются очень близкими к изложению некоторых целей безопасности, демонстрация может быть очень простой. Пример: угроза «Т17: Источник угрозы Х читает конфиденциальную информацию при ее передаче между А и В», цель безопасности для ОО: «О12: ОО должен обеспечить сохранение конфиденциальности всей информации, передаваемой между А и В» и демонстрация: «Угрозе Т17 напрямую противостоит цель О12».

А.7.3.3 Предотвращаемые угрозы

Противостояние угрозе не обязательно означает устранение угрозы, а может означать достаточное уменьшение этой угрозы или достаточное смягчение последствий реализации этой угрозы.

Примеры устранения угрозы:

- устранение возможностей со стороны источника угрозы осуществлять нежелательное действие;
- перемещение, изменение или защита актива таким образом, что нежелательное действие становится более не применимым к нему;
- устранение источника угрозы (например, отключение от сети ПК, которые часто «рушат» эту сеть).

Примеры уменьшения угрозы:

- ограничение способности источника угрозы по выполнению нежелательных действий;
- ограничение возможности выполнить нежелательное действие источником угрозы;
- уменьшение вероятности успешного результата, выполненного нежелательного действия;
- снижение мотивации источника угрозы выполнить нежелательное действие путем сдерживания;
- требование от источника угрозы большей компетентности или больших ресурсов.

Примеры смягчения последствий реализации угрозы:

- частое создание резервных копий актива;
- приобретение дополнительных копий актива;
- страхование актива;
- обеспечение своевременного обнаружения успешных нежелательных действий, чтобы предпринять соответствующие ответные действия.

А.7.4 Цели безопасности: заключение

Основываясь на целях безопасности и обосновании целей безопасности, может быть сделано следующее заключение: если все цели безопасности достигнуты, то проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы.

А.8 Определение расширенных компонентов (ASE_ECD)

Во многих случаях требования безопасности в ЗБ (см. А.9) основаны на компонентах из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. Однако в некоторых случаях в ЗБ могут быть требования, которые не основаны на компонентах из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3. В этом случае новые компоненты (расширенные компоненты) должны быть определены, и такое определение следует сделать в разделе ЗБ «Определение расширенных компонентов». Дополнительная информация по данному вопросу приведена в С.4 (приложение С).

Данный раздел ЗБ предназначен для изложения только расширенных компонентов, а не расширенных требований (требований, основанных на расширенных компонентах). Расширенные требования следует включать в раздел ЗБ «Требования безопасности» (см. А.9), и их предназначение то же, что и у требований, основанных на компонентах из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3.

А.9 Требования безопасности (ASE_REQ)

Требования безопасности включают две группы требований:

a) функциональные требования безопасности (ФТБ): перевод целей безопасности для ОО на некоторый стандартизированный язык;

b) требования доверия к безопасности (ТДБ): описание того, каким образом должно быть получено доверие к тому, что ОО удовлетворяет ФТБ.

Эти две группы требований безопасности рассматриваются в 9.1 и 9.2.

А.9.1 Функциональные требования безопасности

ФТБ являются результатом преобразования целей безопасности для ОО. ФТБ обычно представлены на более детальном уровне абстракции, но они должны быть полным представлением (цели безопасности должны быть полностью учтены) и быть независимыми от любого конкретного технического решения (реализации). ИСО/МЭК 15408 требует их представления на некотором стандартизированном языке по следующим причинам:

- чтобы обеспечить точное описание того, что подлежит оценке. Поскольку цели безопасности для ОО обычно формулируются на естественном языке, перевод их на стандартизированный язык способствует более точному описанию функциональных возможностей ОО;
- чтобы обеспечить сопоставление двух ЗБ. В то время как различные разработчики ЗБ могут использовать различную терминологию при описании целей безопасности, стандартизированный язык обеспечивает использование единой терминологии и понятий при изложении требований безопасности. Это позволяет легко сравнивать ЗБ.

ИСО/МЭК 15408 не требует перевода на стандартизированный язык целей безопасности для среды функционирования, так как среда функционирования не оценивается и поэтому не требует описания, направленного на ее оценку. См. пункты раздела «Библиография», относящиеся к оценке безопасности автоматизированных систем.

Могут быть ситуации, когда части среды функционирования оценены в процессе другой оценки, но это — вне области действия текущей оценки. Например, для ОО «ОС» может потребоваться, чтобы в его среде функционирования присутствовал межсетевой экран. Межсетевой экран может быть оценен в рамках другой оценки, но такая оценка не имеет никакого отношения к оценке ОО «ОС».

А.9.1.1 Способы преобразования целей безопасности в требования безопасности, поддерживаемые ИСО/МЭК 15408

ИСО/МЭК 15408 поддерживает преобразование целей безопасности в требования безопасности тремя способами:

a) путем предоставления предопределенного «точного языка», разработанного в целях точного описания того, что подлежит оценке. Этот язык определяется как совокупность компонентов, определенных в ИСО/МЭК 15408-2. Использование этого языка для четкого преобразования целей безопасности для ОО в ФТБ является обязательным, хотя существуют некоторые исключения (см. 7.3);

b) путем предоставления операций — механизм, который позволяет разработчику ЗБ модифицировать ФТБ, чтобы обеспечить более точный учет целей безопасности для ОО. В данной части ИСО/МЭК 15408 определены четыре допустимые операции: назначение, выбор, итерация и уточнение. Дальнейшее их рассмотрение представлено в С.2 (приложение С);

c) путем определения зависимостей — механизм, который поддерживает более полное преобразование целей безопасности для ОО в ФТБ. На языке ИСО/МЭК 15408-2 ФТБ может иметь зависимости от других ФТБ. Это указывает, что если в ЗБ используется данное ФТБ, то в общем случае в ЗБ должны также быть использованы и ФТБ, от которых оно зависит. Это уменьшает для разработчика ЗБ возможность упустить включение в ЗБ необходимых ФТБ и таким образом улучшает полноту ЗБ. Дальнейшее рассмотрение зависимостей представлено в 7.2.

А.9.1.2 Взаимосвязь между ФТБ и целями безопасности

ЗБ также содержит «Обоснование требований безопасности», включающее два пункта, касающихся ФТБ:

- прослеживание, показывающее, какие ФТБ какие цели безопасности для ОО учитывают;
- совокупность логических обоснований, показывающих, что все цели безопасности для ОО надлежащим образом учтены в ФТБ.

А.9.1.2.1 Прослеживание ФТБ к целям безопасности для ОО

Прослеживание показывает, каким образом ФТБ сопоставлены с целями безопасности для ОО, обеспечивая при этом следующее:

a) Отсутствие избыточных ФТБ: каждое ФТБ сопоставлено, по крайней мере, с одной целью безопасности.

b) Полнота по отношению к целям безопасности для ОО: для каждой цели безопасности для ОО имеется, по крайней мере, одно ФТБ, сопоставленное с ней.

Несколько ФТБ могут быть сопоставлены с одной и той же целью безопасности для ОО, указывая на то, что сочетание этих требований безопасности удовлетворяет данную цель безопасности для ОО.

А.9.1.2.2 Предоставление логического обоснования для сопоставления

Обоснование требований безопасности демонстрирует, что сопоставление является надлежащим: если все ФТБ, сопоставленные с конкретной целью безопасности для ОО, удовлетворены, то эта цель безопасности для ОО достигнута.

Данная демонстрация должна содержать результаты анализа эффекта от удовлетворения соответствующего ФТБ при достижении конкретной цели безопасности для ОО и приводить к заключению, что это действительно так.

В случаях, когда ФТБ являются очень близкими к изложению целей безопасности для ОО, демонстрация может быть очень простой.

А.9.2 Требования доверия к безопасности (ТДБ)

ТДБ — описание того, каким образом должен быть оценен ОО. В данном описании используется стандартизированный язык по следующим причинам:

- чтобы обеспечить точное описание того, каким образом ОО должен быть оценен. Использование стандартизированного языка способствует точному описанию и исключению неоднозначности;
- чтобы обеспечить сопоставление двух ЗБ. В то время как различные разработчики ЗБ могут использовать различную терминологию, стандартизированный язык обеспечивает использование единой терминологии и понятий. Это позволяет легко сравнивать ЗБ.

Рассматриваемый стандартизированный язык определяется как совокупность компонентов, определенных в ИСО/МЭК 15408-3. Использование этого языка является обязательным, хотя существуют некоторые исключения. ИСО/МЭК 15408 (все части) усиливает этот язык по двум направлениям:

a) путем предоставления операций — механизм, который позволяет разработчику ЗБ модифицировать ТДБ. В данной части ИСО/МЭК 15408 определены четыре допустимые операции: назначение, выбор, итерация и уточнение. Дальнейшее их рассмотрение представлено в С.2 (приложение С);

b) путем определения зависимостей — механизм, который поддерживает более полное выражение ТДБ. На языке ИСО/МЭК 15408-3 ТДБ может иметь зависимости от других ТДБ. Это указывает, что если в ЗБ используется данное ТДБ, то в общем случае должны также использоваться и ТДБ, от которых оно зависит. Это уменьшает для разработчика ЗБ возможность упустить включение в ЗБ необходимых ТДБ и, таким образом, улучшает полноту ЗБ. Более подробное рассмотрение зависимостей представлено в 7.2.

А.9.3 ТДБ и обоснование требований безопасности

ЗБ также содержит обоснование требований безопасности, которое содержит аргументы, позволяющие считать конкретную совокупность ТДБ надлежащей. Каких-либо конкретных требований к такому обоснованию не предъявляется. Цель этого обоснования заключается в том, чтобы обеспечить пользователям ЗБ понимание причины выбора конкретной совокупности ТДБ.

Примером несогласованности является ситуация, когда в «Описании проблемы безопасности» присутствуют угрозы, источник которых (нарушитель) обладает достаточными возможностями, а в совокупность ТДБ включен младший компонент из семейства AVA_VAN или вообще не включен никакой компонент из данного семейства.

А.9.4 Требования безопасности: заключение

В ЗБ в «Определении проблемы безопасности» определяется проблема безопасности, которая включает угрозы, ПБОр и предположения. В разделе ЗБ «Цели безопасности» решение проблемы безопасности подразделяется на две части:

- цели безопасности для ОО;
- цели безопасности для среды функционирования.

Кроме того, приводится обоснование целей безопасности, показывающее, что если все цели безопасности достигнуты, то проблема безопасности решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы.

В разделе ЗБ «Требования безопасности» цели безопасности для ОО преобразуются в ФТБ и предоставляется обоснование требований безопасности, показывающее, что если все ФТБ удовлетворены, то все цели безопасности для ОО достигнуты.

Кроме того, здесь приводится совокупность ТДБ, чтобы показать, каким образом оценивается ОО, а также — пояснение выбора этих ТДБ.

Все вышеупомянутое может быть объединено в рамках следующего утверждения. Если все ФТБ и ТДБ удовлетворены и все цели безопасности для среды функционирования достигнуты, то имеется доверие к тому, что проблема безопасности, определенная в соответствии с ASE_SPD, решена: всем угрозам обеспечено противостояние, все ПБОр осуществлены и все предположения реализованы. Данное утверждение проиллюстрировано на рисунке А.3.

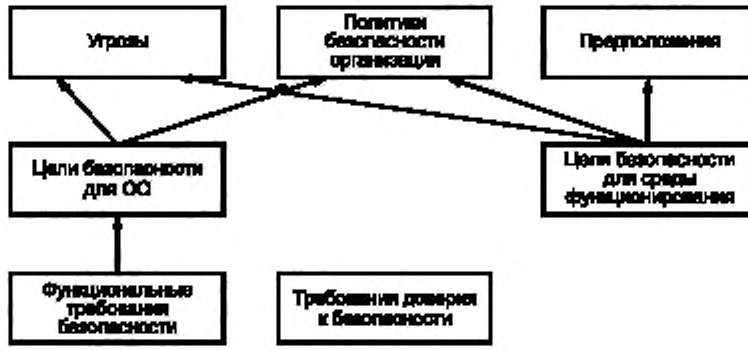

Рисунок А.3 — Взаимосвязь между определением проблемы безопасности, целями безопасности и требованиями безопасности

Объем приобретенного доверия определяется ТДБ, а достаточность этого объема доверия определяется пояснением выбора ТДБ.

А.10 Краткая спецификация ОО (ASE_TSS)

Цель «Краткой спецификации ОО» — предоставить потенциальным потребителям ОО описание того, каким образом ОО удовлетворяет все ФТБ. В разделе «Краткая спецификация ОО» следует привести описание основных технических механизмов, используемых ОО с этой целью. Уровень детализации данного описания должен быть достаточным, чтобы позволить потенциальным потребителям понять основной облик и реализацию ОО.

Например, если ОО является ПК, подключенным к Интернет, и ФТБ включают компонент FIA_UAU.1 для определения аутентификации, то в краткой спецификации ОО следует указать, каким образом выполняется аутентификация: посредством пароля, токена, сканирования радужной оболочки глаза и т. д.

Может быть также приведен больший объем информации, такой, например, как указание применимых стандартов, используемых в ОО для удовлетворения ФТБ, или более детальное описание.

А.11 Вопросы, на которые можно ответить с помощью ЗБ

По окончании оценки ЗБ определяет «что было оценено». В этой роли ЗБ служит основой для соглашения между разработчиком или поставщиком ОО и потенциальным потребителем ОО. Поэтому с помощью ЗБ можно ответить на следующие (а также и на другие) вопросы:

a) Как найти необходимые ЗБ/ОО из множества существующих ЗБ/ОО? Этот вопрос обращен к «Аннотации ОО», в которой дается краткое (несколько параграфов) описание ОО;

b) Согласован ли ОО с существующей инфраструктурой ИТ? Этот вопрос обращен к «Аннотации ОО», в которой идентифицируются основные элементы аппаратных средств/программно-аппаратных средств/программного обеспечения, под управлением которых должен функционировать ОО;

c) Согласован ли ОО с существующей средой функционирования? Этот вопрос обращен к «Целям безопасности для среды функционирования», где определяются все ограничения на размещение ОО в среде функционирования;

d) Что делает (возможности) ОО (заинтересованный пользователь)? Этот вопрос обращен к «Аннотации ОО», в которой дается краткое (несколько параграфов) описание ОО;

e) Что делает ОО (потенциальный потребитель)? Этот вопрос обращен к «Описанию ОО», в котором дается более подробное, чем в «Аннотации ОО», описание ОО (на несколько страниц);

f) Что делает ОО (технический специалист)? Этот вопрос обращен к «Краткой спецификации ОО», в которой приводится высокоуровневое описание механизмов, использованных в ОО;

g) Что делает ОО (эксперт)? Этот вопрос обращен к ФТБ, которые обеспечивают достаточно абстрактное техническое описание, и к «Краткой спецификации ОО», в которой приводятся дополнительные подробности;

h) Решает ли ОО проблему с учетом требований государства/организации? Если государство/организация определили пакеты и/или ПЗ, чтобы определить решение, то ответ на указанный вопрос может быть найден в разделе ЗБ «Утверждения о соответствии», в котором перечисляются все пакеты и ПЗ, которым соответствует ЗБ;

i) Отвечает ли ОО конкретной проблеме безопасности (эксперт)? Каким угрозам противостоит ОО? Какую политику безопасности организации реализует ОО? Какие предположения сделаны относительно среды функционирования? На эти вопросы отвечает «Определение проблемы безопасности»;

j) Каков объем доверия к ОО? Ответ на этот вопрос может быть найден в ТДБ в разделе ЗБ «Требования безопасности», в котором определен уровень доверия, использованный при оценке ОО, а следовательно — объем доверия к корректности ОО, обеспечиваемый в результате оценки.

А.12 Задания по безопасности для низкого уровня доверия

Написание ЗБ является нетривиальной задачей и может, особенно при оценках для низких уровней доверия, составлять основную часть общих усилий, затрачиваемых разработчиком и оценщиком в течение всей оценки. Поэтому приемлемо также разрабатывать упрощенное ЗБ для низкого уровня доверия.

ИСО/МЭК 15408 допускает использование упрощенного ЗБ для оценки по ОУД1, но не по ОУД2 и выше. В ЗБ для низкого уровня доверия может быть заявлено соответствие ПЗ для низкого уровня доверия (см. приложение В). В обычном ЗБ (т. е. ЗБ с полным содержанием) может быть заявлено соответствие ПЗ для низкого уровня доверия.

ЗБ для низкого уровня доверия имеет значительно сокращенное содержание по сравнению с обычным ЗБ:

- не требуется приводить определение проблемы безопасности;
- не требуется излагать цели безопасности для ОО. Но при этом цели безопасности для среды функционирования должны быть изложены;
- не требуется приводить обоснование целей безопасности, поскольку в ЗБ не приводится определение проблемы безопасности;
- в обосновании требований безопасности необходимо привести только обоснование неудовлетворения зависимостей, поскольку в ЗБ не приводятся цели безопасности для ОО.

Все, что остается в таком ЗБ, включает:

a) ссылки на ОО и ЗБ;

b) утверждение о соответствии;

c) различные описательные материалы:

1) аннотация ОО;
2) описание ОО;
3) краткая спецификация ОО;

d) цели безопасности для среды функционирования;

e) ФТБ и ТДБ (включая определение расширенных компонентов) и обоснование требований безопасности (только если конкретные зависимости не удовлетворены).

Сокращенное содержание ЗБ для низкого уровня доверия приведено на рисунке 4.

А.13 Ссылка в ЗБ на другие стандарты

В некоторых случаях разработчику ЗБ может потребоваться ссылка на какой-либо дополнительный стандарт, такой, например, как конкретный стандарт по криптографии или описание конкретного протокола. ИСО/МЭК 15408 позволяет сделать это тремя способами:

a) В качестве политики безопасности организации (или ее части).

Если, например, существует нормативный документ, определяющий, как выбираются пароли, это может быть изложено в ЗБ в качестве политики безопасности организации. На основе этого может быть изложена цель безопасности для среды функционирования (например, если пользователи ОО соответствующим образом должны выбирать пароли) или могут быть изложены цели безопасности для ОО, а затем — соответствующие ФТБ (вероятно, на основе класса FIA), если пароли генерирует ОО. В обоих случаях обоснование разработчика должно быть убедительным, что цели безопасности для ОО и ФТБ являются подходящими для реализации ПБОр. Оценщик должен определить, действительно ли это убедительно (и может изучить для этого упомянутый стандарт), действительно ли ПБОр реализована в ФТБ как приведено ниже.



Рисунок А.4 — Содержание задания по безопасности для низкого уровня доверия

b) В качестве стандарта (например, стандарта по криптографии), использованного при конкретизации ФТБ.

В этом случае соответствие конкретному стандарту является частью выполнения объектом оценки ФТБ и рассматривается, как будто полный текст стандарта является частью ФТБ. Далее соответствие конкретному стандарту определяется, как и любое другое соответствие ФТБ, при выполнении видов деятельности, предусмотренных классами ADV и ATE; соответствие определяется путем анализа проекта и тестирования на предмет того, что ФТБ полны и полностью реализованы ОО. Если необходима ссылка только на определенную часть стандарта, то эту часть следует однозначно указать при конкретизации ФТБ.

c) В качестве упоминания стандарта (например, стандарта по криптографии) в краткой спецификации ОО.

Краткая спецификация ОО рассматривается только в качестве пояснения того, как реализованы ФТБ, и не используется в качестве строгого требования к реализации, каковыми являются ФТБ или документы, поставляемые в соответствии с классом ADV. Таким образом, оценщик может обнаружить несогласованность, если в краткой спецификации ОО есть ссылка на некоторый стандарт, но это не отражено в документации, предусмотренной классом ADV, и не предусмотрено соответствующей деятельностью, чтобы проверить выполнение стандарта.

Приложение В
(справочное)

Спецификация профилей защиты

В.1 Цель и структура данного приложения

Цель данного приложения состоит в изложении концепции профиля защиты (ПЗ). В данном приложении не определены критерии класса APE; соответствующее определение содержится в ИСО/МЭК 15408-3 и поддержано документами, приведенными в разделе «Библиография».

Так как профили защиты и задания по безопасности имеют значительные совпадения, в данном приложении внимание сосредоточено на отличиях между ПЗ и ЗБ. Материал, который является идентичным для ЗБ и для ПЗ, изложен в приложении А.

Приложение В состоит из четырех основных частей:

a) Что должно содержать ПЗ. Краткая информация по этому вопросу изложена в В.2, более подробно в В.4—В.9. В указанных разделах описано обязательное содержание ПЗ, взаимосвязи в рамках содержания ПЗ, а также представлены примеры.

b) Как следует использовать ПЗ. Краткая информация по этому вопросу изложена в В.3.

c) ПЗ для низкого уровня доверия (упрощенный ПЗ). Упрощенные ПЗ представляют собой ПЗ с сокращенным содержанием. Такие ПЗ описаны в В.11.

d) Утверждение о соответствии стандартам. В разделе В.12 описано, каким образом разработчик ПЗ может сделать утверждение, что ОО должен удовлетворять некоторому конкретному стандарту.

В.2 Обязательное содержание ПЗ

На рисунке В.1 представлено содержание ПЗ, установленное в ИСО/МЭК 15408-3. Рисунок В.1 также можно использовать как структурную схему ПЗ, хотя допустимы и альтернативные структуры. Например, если обоснование требований безопасности является очень объемным, то оно может быть вынесено в приложение к ПЗ вместо включения в раздел «Требования безопасности». Разделы ПЗ и содержание этих разделов кратко рассмотрены ниже; в В.4 — В.9 приведены более подробные пояснения. ПЗ содержит:

a) раздел «Введение ПЗ», содержащий описание типа ОО;

b) раздел «Утверждения о соответствии», указывающий, утверждается ли в ПЗ о соответствии каким-либо ПЗ и/или пакетам, и если «да», то каким ПЗ и/или пакетам;

c) раздел «Определение проблемы безопасности», в котором указываются угрозы, ПБОр и предположения;

d) раздел «Цели безопасности», показывающий, каким образом решение проблемы безопасности распределено между целями безопасности для ОО и целями безопасности для среды функционирования ОО;

e) раздел «Определение расширенных компонентов» (опционально), в котором могут быть определены новые компоненты (т. е. компоненты, не содержащиеся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3). Эти новые компоненты необходимы, чтобы определить расширенные функциональные требования и расширенные требования доверия;

f) раздел «Требования безопасности», в котором цели безопасности для ОО преобразованы в изложение на стандартизованном языке. Этот стандартизированный язык представляет собой форму представления ФТБ. Кроме того, в рассматриваемом разделе определяют ТДБ.

Существуют также ПЗ для низкого уровня доверия (упрощенные ПЗ), имеющие сокращенное содержание; подробно такие ПЗ описаны в В.11. За этим исключением все остальные части данного приложения предполагают ПЗ с полным содержанием.

В.3 Использование ПЗ

В.3.1 Как следует использовать ПЗ

ПЗ представляет собой изложение потребностей в безопасности, в котором некоторое сообщество пользователей, регулирующий орган или группа разработчиков определяет общую совокупность потребностей в безопасности. ПЗ дает возможность потребителям ссылаться на эту совокупность и облегчает последующую оценку удовлетворения этих потребностей.

Поэтому ПЗ обычно используют в качестве:

- части спецификации требований конкретного потребителя или группы потребителей, которые будут рассматривать приобретение продукта ИТ некоторого конкретного типа, только если он удовлетворяет ПЗ;
- части нормативного регулирования со стороны регулирующего органа, который разрешает использование продукта ИТ некоторого конкретного типа, только если он удовлетворяет ПЗ;
- базовой линии некоторой группы разработчиков, которые договариваются, что все продукты ИТ данного типа, которые они будут производить, будут удовлетворять данной базовой линии,
- хотя это не исключает другого использования.

В.3.2 Как не следует использовать ПЗ

Три роли (из многих), для которых не следует использовать ПЗ:

- детальная спецификация: ПЗ разрабатывается в качестве спецификации безопасности на относительно высоком уровне абстракции. Обычно в ПЗ не следует включать детальные спецификации протоколов, детальное описание алгоритмов и/или механизмов, длинное описание детализированных операций и т. д.;

- полная спецификация: ПЗ разрабатывается в качестве спецификации безопасности, а не общей спецификации. Кроме относящихся к безопасности, другие характеристики, такие как возможности взаимодействия, физические размеры и масса, требуемое напряжение и т. д., не следует включать в ПЗ. Это означает, что в целом ПЗ может быть частью полной спецификации, но не полной спецификацией сам по себе.

- спецификация некоторого отдельно взятого продукта. В отличие от ЗБ, ПЗ разрабатывается для описания определенного типа продуктов ИТ, а не отдельно взятого продукта ИТ. При описании некоторого отдельно взятого продукта ИТ лучше использовать для этой цели ЗБ.



Рисунок В.1 — Содержание профиля защиты

В.4 Введение ПЗ (APE_INT)

В разделе «Введение ПЗ» описывают ОО в повествовательной форме на двух уровнях абстракции:

a) ссылка на ПЗ, обеспечивающая идентификационные материалы для ПЗ;

b) аннотация ОО, в которой кратко описывается ОО.

В.4.1 Ссылка на ПЗ

ПЗ содержит четкую ссылку на ПЗ, которая идентифицирует данный ПЗ. Типичная ссылка на ПЗ состоит из наименования ПЗ, версии, разработчика и даты выпуска. Ссылка должна быть уникальной, чтобы было возможно выделять различные ПЗ и различные версии одного и того же ПЗ.

Ссылка на ПЗ облегчает индексацию и ссылку на ПЗ и их включение в списки ПЗ.

В.4.2 Аннотация ОО

Аннотация ОО нацелена на потенциальных потребителей ОО, просматривающих списки оцененных продуктов, чтобы найти ОО, которые могут удовлетворить их потребности в безопасности и поддерживаться их аппаратным, программным и программно-аппаратным обеспечением.

Аннотация ОО также предназначена для разработчиков, которые могут использовать ПЗ при разработке ОО или адаптации существующих продуктов.

Как правило, объем аннотации ОО — несколько параграфов.

В аннотации ОО кратко описывают использование ОО и его основные характеристики безопасности, идентифицируют тип ОО и все основные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО, но доступные для ОО.

B.4.2.1 Использование и основные характеристики безопасности ОО

Описание использования и основных характеристик безопасности ОО предназначено, чтобы дать общее представление о возможностях ОО и о том, для чего можно использовать ОО. Это должно быть написано для (потенциальных) потребителей ОО с описанием использования и основных характеристик ОО в терминах бизнес-операций и на языке, понятном потребителям ОО.

B.4.2.2 Тип ОО

В аннотации ОО идентифицируют общий тип ОО, такой как: межсетевой экран, шлюз виртуальной частной сети, смарт-карта, интранет, веб-сервер, система управления базами данных, веб-сервер и система управления базами данных, ЛВС, ЛВС с веб-сервером и системой управления базой данных и др.

B.4.2.3 Доступные аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО

В то время как некоторые ОО не зависят от других ИТ, многие ОО (особенно программные ОО) зависят от дополнительных, не входящих в ОО, аппаратных средств/программного обеспечения и/или программно-аппаратных средств. В последнем случае в «Аннотации ОО» требуется идентифицировать не входящие в ОО аппаратные средства/программное обеспечение и/или программно-аппаратные средства.

Поскольку профиль защиты не разрабатывают для конкретного продукта, во многих случаях в нем может быть дано только общее представление о доступных аппаратных средствах/программном обеспечении/программно-аппаратных средствах. В некоторых других случаях, например, при спецификации требований для конкретного потребителя, когда платформа уже известна, может быть предоставлена более конкретная информация.

Примеры идентификации аппаратных средств/программного обеспечения/программно-аппаратных средств:

- «отсутствует» (для полностью автономного ОО);
- операционная система Yaiza версии 3.0, функционирующая на ПК;
- интегральная схема CleverCard SB2067;
- интегральная схема CleverCard SB2067 с установленной операционной системой для смарт-карт QuickOS;
- локальная вычислительная сеть департамента транспорта по состоянию на декабрь 2002 года.

B.5 Утверждения о соответствии (APE_CCL)

В данном разделе ПЗ описывают соответствие ПЗ другим ПЗ и пакетам. Это идентично разделу «Утверждения о соответствии» для ЗБ (см. А.5) за одним исключением: тип утверждения о соответствии.

В ПЗ в утверждении о соответствии излагается, каким образом ЗБ и/или другие ПЗ должны соответствовать данному ПЗ. Разработчик ПЗ выбирает, какой тип соответствия требуется: «строгое» соответствие или «демонстрируемое» соответствие. Более подробно этот вопрос рассмотрен в приложении D.

B.6 Определение проблемы безопасности (APE_SPD)

Данный раздел идентичен разделу ЗБ «Определение проблемы безопасности», рассмотренному в А.6.

B.7 Цели безопасности (APE_OBJ)

Данный раздел идентичен разделу ЗБ «Цели безопасности», рассмотренному в А.7.

B.8 Определение расширенных компонентов (APE_ECD)

Данный раздел идентичен разделу ЗБ «Определение расширенных компонентов», рассмотренному в А.8.

B.9 Требования безопасности (APE_REQ)

Данный раздел идентичен разделу ЗБ «Требования безопасности», рассмотренному в А.9.

Однако следует заметить, что правила выполнения операций в ПЗ немного отличаются от правил выполнения операций в ЗБ. Более подробно этот вопрос рассмотрен в 7.1.

B.10 Краткая спецификация ОО

ПЗ не содержит краткой спецификации ОО.

B.11 Профили защиты для низкого уровня доверия

ПЗ для низкого уровня доверия (упрощенное ПЗ) соотносится с обычным ПЗ (т. е. ПЗ с полным содержанием) так же, как и ЗБ для низкого уровня доверия (упрощенное ЗБ) соотносится с обычным ЗБ. Это означает, что упрощенное ПЗ включает:

a) введение ПЗ, включающее ссылку на ПЗ и аннотацию ОО;
b) утверждения о соответствии;
c) цели безопасности для среды функционирования;
d) ФТБ и ТДБ (включая определение расширенных компонентов), а также обоснование требований безопасности (только в случае неудовлетворения зависимостей).

В упрощенном ПЗ может присутствовать утверждение о соответствии только некоторому упрощенному ПЗ (см. В.5). В обычном ПЗ может также присутствовать утверждение о соответствии упрощенному ПЗ.

Сокращенное содержание упрощенного ПЗ приведено на рисунке В.2.



Рисунок В.2 — Содержание упрощенного ПЗ

В.12 Ссылка в ПЗ на другие стандарты

Этот раздел идентичен разделу А.13, посвященному ссылке на стандарты в ЗБ, за одним исключением: так как в ПЗ не содержится краткая спецификация ОО, то пункт с) раздела А.13 не применим по отношению к ПЗ.

Разработчику ПЗ необходимо учитывать, что ссылка в ФТБ на какой-либо стандарт может существенно добавить нагрузку на разработчика ОО, чтобы удовлетворить ПЗ (в зависимости от объема и сложности стандарта и требуемого уровня доверия); при этом может быть более приемлемым требовать использования альтернативных (не относящихся к частям стандарта ИСО/МЭК 15408) способов оценки соответствия стандарту, на который имеется ссылка в ПЗ.

Приложение С
(справочное)

Руководство по выполнению операций

С.1 Введение

Профили защиты и задания по безопасности содержат предопределенные требования безопасности: разработчикам ПЗ и ЗБ при некоторых обстоятельствах также предоставляется возможность расширить список компонентов требований безопасности.

С.2 Примеры операций

В 7.1 приведены четыре типа операций. Примеры выполнения различных операций рассмотрены ниже.

С.2.1 Операция «итерация»

Как описано в 7.1.1, операция «итерация» может быть выполнена по отношению к любому компоненту. Разработчик ПЗ/ЗБ выполняет операцию «итерация» путем включения нескольких требований, основанных на одном и том же компоненте. Каждая итерация компонента должна отличаться от всех других итераций этого компонента, что реализуется завершением по-другому операций «назначение» и «выбор» или применением по-другому операции «уточнение».

Различные итерации следует уникально идентифицировать, чтобы обеспечить четкое обоснование и прослеживаемость от или к этим требованиям.

Типичный пример выполнения итерации — повторение дважды компонента FCS_COP.1 для того, чтобы потребовать реализации двух различных криптографических алгоритмов. Пример уникальной идентификации каждой итерации:

- Криптографическая операция (FCS_COP.1(1));
- Криптографическая операция (FCS_COP.1(2)).

С.2.2 Операция «назначение»

Как описано в 7.1.2, операцию «назначение» осуществляют тогда, когда рассматриваемый компонент включает элемент с некоторым параметром, значение которого может быть установлено разработчиком ПЗ/ЗБ. Параметром может быть ничем не ограниченная переменная или правило, которое ограничивает переменную конкретным диапазоном значений.

Пример элемента требований с операцией «назначение»: FIA_AFL.1.2 «При достижении или превышении определенного числа неуспешных попыток аутентификации ФБО должны выполнить [назначение: *список действий*]".

С.2.3 Операция «выбор»

Как описано в 7.1.3, операцию «выбор» осуществляют тогда, когда рассматриваемый компонент включает элемент, в котором разработчиком ПЗ/ЗБ должен быть сделан выбор из нескольких пунктов.

Пример элемента требований с операцией «выбор»: FPT_TST.1.1 «ФБО должны выполнять пакет программ самотестирования [выбор: *при запуске, периодически в процессе нормального функционирования, по запросу уполномоченного пользователя, при условиях* [назначение: *условия, при которых следует предусмотреть самотестирование*]] для демонстрации правильного выполнения ...»

С.2.4 Операция «уточнение»

Как описано в 7.1.4, операция «уточнение» может быть выполнена по отношению к любому требованию. Разработчик ПЗ/ЗБ выполняет уточнение путем изменения требования.

Пример допустимого выполнения операции «уточнение»: FIA_UAU.2.1 «ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя» уточнен следующим образом — «ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован **на основе имени пользователя и пароля** до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя».

Первое правило по отношению к уточнению состоит в том, чтобы ОО, удовлетворяющий уточненному требованию, также удовлетворял неуточненному требованию в контексте ПЗ/ЗБ (т. е. уточненное требование должно быть «более строгим», чем исходное требование).

Единственное исключение из этого правила состоит в том, что допускается, чтобы разработчик ПЗ/ЗБ уточнил ФТБ для его применения по отношению к некоторым, но не ко всем субъектам, объектам, операциям, атрибутам безопасности и/или внешним сущностям.

Пример подобного исключения: FIA_UAU.2.1 «ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя» уточнен следующим образом «ФБО должны требовать, чтобы каждый пользователь **из Интернета** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя».

Второе правило по отношению к уточнению состоит в том, что уточнение должно быть связано с исходным компонентом. Например, уточнение компонента аудита путем добавления дополнительного элемента, связанного с предотвращением электромагнитного излучения, недопустимо.

Особым случаем уточнения является редакционное уточнение, когда в требование вносят небольшие изменения, такие как перефразирование предложения, чтобы сделать его более понятным читателю. Не допускается, чтобы эти изменения каким-либо образом изменяли смысл требования. Примеры редакционных уточнений:

ФТБ, основанное на компоненте FPT_FLS.1, «ФБО должны сохранить безопасное состояние при следующих типах сбоев: выход из строя одного процессора» могло бы быть уточнено следующим образом — FPT_FLS.1 «ФБО должны сохранить безопасное состояние при следующих типах сбоев: **выход одного процессора из строя**» или даже — FPT_FLS.1 «ФБО должны сохранить безопасное состояние при следующих типах сбоев: **один процессор вышел из строя**».

С.3 Организация компонентов

Компоненты в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 организованы в иерархические структуры:

классы, состоящие из
семейств, включающих
компоненты, состоящие из
элементов.

Данная организация иерархии «класс — семейство — компонент — элемент» помогает потребителям, разработчикам и оценщикам в поиске конкретных компонентов.

В ИСО/МЭК 15408 функциональные компоненты и компоненты доверия представлены в едином иерархическом стиле, по отношению к ним использована единая организация и терминология.

С.3.1 Класс

Примером класса является класс FIA, который направлен на идентификацию пользователей, аутентификацию пользователей и связывание пользователей и субъектов.

С.3.2 Семейство

Примером семейства является семейство «Аутентификация пользователя» (FIA_UAU), которое является частью класса FIA. Это семейство связано с аутентификацией пользователей.

С.3.3 Компонент

Примером компонента является компонент FIA_UAU.3 «Аутентификация, защищенная от подделок», который связан с аутентификацией, защищенной от подделок.

С.3.4 Элемент

Примером элемента является элемент FIA_UAU.3.2, который связан с предотвращением использования скопированных аутентификационных данных.

С.4 Расширенные компоненты

С.4.1 Определение расширенных компонентов

Всякий раз, когда разработчик ПЗ/ЗБ определяет расширенный компонент, это должно быть сделано способом, подобным существующим компонентам ИСО/МЭК 15408: четким, однозначным и оцениваемым (имеется возможность методично продемонстрировать выполнение требования, основанного на этом компоненте, для ОО). Расширенные компоненты должны использовать обозначение, способ выражения и уровень детализации, подобные существующим компонентам ИСО/МЭК 15408.

Разработчик ПЗ/ЗБ также должен убедиться, что все применимые зависимости расширенного компонента включены в определение этого расширенного компонента. Примерами возможных зависимостей являются следующие:

a) если расширенный компонент относится к аудиту, то, вероятно, придется включить зависимости от компонентов класса FAU;

b) если расширенный компонент связан с модификацией или доступом к данным, то, вероятно, придется включить зависимости от компонентов семейства FDP_ACC;

c) если расширенный компонент использует конкретное описание проекта, то, вероятно, придется включить зависимость от компонентов соответствующего семейства (например, «Функциональная спецификация») класса ADV.

В случае расширенного функционального компонента разработчик ПЗ/ЗБ также должен включить в определение компонента применимую информацию, связанную с аудитом и действиями по управлению, подобно тому, как это сделано для существующих компонентов ИСО/МЭК 15408-2. В случае расширенного компонента доверия разработчик ПЗ/ЗБ также должен предоставить соответствующую методологию оценки для данного компонента, подобную методологии, изложенной в ИСО/МЭК 18045.

Расширенные компоненты могут быть помещены в существующие семейства, в этом случае разработчик ПЗ/ЗБ должен показать, каким образом изменяются данные семейства. Если для новых компонентов не подходят существующие семейства, то они должны быть помещены в новое семейство. Новые семейства должны быть определены так же, как определены семейства в ИСО/МЭК 15408.

Новые семейства могут быть помещены в существующие классы, в этом случае разработчик ПЗ/ЗБ должен показать, каким образом изменяются данные классы. Если для новых семейств не подходят существующие классы, то они должны быть помещены в новый класс. Новые классы должны быть определены так же, как определены классы в ИСО/МЭК 15408.

Приложение D
(справочное)

Соответствие ПЗ

D.1 Введение

ПЗ предназначен для использования в качестве «шаблона» для ЗБ. То есть ПЗ описывает совокупность потребностей пользователя, в то время как ЗБ, который соответствует этому ПЗ, описывает ОО, который удовлетворяет данные потребности.

Также возможно использовать один ПЗ в качестве «шаблона» для другого ПЗ. То есть ПЗ может требовать соответствие другому ПЗ. Этот случай полностью аналогичен утверждению о соответствии ПЗ в ЗБ. Для ясности в данном приложении описывается только случай ЗБ/ПЗ, но приложение применимо и для случая ПЗ/ПЗ.

ИСО/МЭК 15408 не допускает любой формы частичного соответствия, таким образом, если в ПЗ или ЗБ заявлено о соответствии ПЗ, то данные ПЗ или ЗБ должны полностью соответствовать указанному (указанным) ПЗ, на которое (которые) имеется ссылка. Однако существуют два типа соответствия («строгое» и «демонстрируемое»), при этом допустимый тип соответствия определяется в ПЗ. Таким образом в ПЗ (в утверждении о соответствии ПЗ, см. В.5) устанавливаются допустимые типы соответствия для ЗБ. Данное отличие между строгим и демонстрируемым соответствием применимо на индивидуальной основе для каждого ПЗ, по отношению к которому в ЗБ утверждается о соответствии. Это может означать, что ЗБ «строго» соответствует одним ПЗ, а тип соответствия другим ПЗ — «демонстрируемое» соответствие. «Демонстрируемый» тип соответствия ПЗ допустим для ЗБ, только если в ПЗ это явно разрешено, в то же время ЗБ может «строго» соответствовать любому ПЗ.

Другими словами, для ЗБ является допустимым «демонстрируемое» соответствие ПЗ только, если ПЗ явно разрешает это.

Соответствие ПЗ означает, что ПЗ или ЗБ (а если для ЗБ имеется оцененный продукт, то и продукт также) отвечают всем требованиям данного ПЗ.

Выпущенные ПЗ обычно будут требовать «демонстрируемого» соответствия. Это означает, что ЗБ, в котором утверждается о соответствии подобному ПЗ, должно предлагать решение общей проблемы безопасности, описанной в ПЗ, но может это сделать любым способом, который является эквивалентным или более ограничительным, по отношению к описанному в ПЗ. «Эквивалентный или более ограничительный» способ подробно определен в рамках ИСО/МЭК 15408, но в принципе это означает, что ПЗ и ЗБ могут содержать полностью различные утверждения, в которых рассматриваются различные сущности, используются различные понятия и т. д., при условии, что в целом ЗБ налагает идентичные ПЗ или большие ограничения по отношению к ОО, а также — идентичные ПЗ или меньшие ограничения по отношению к среде функционирования ОО.

D.2 Строгое соответствие

Строгое соответствие ориентировано на разработчиков ПЗ, которым требуются свидетельства, что требования ПЗ удовлетворены, что ЗБ является примером реализации ПЗ, хотя при этом ЗБ может быть более широким, чем ПЗ. По существу ЗБ определяет ОО, который выполняет, по крайней мере, что определено в ПЗ, и среду функционирования, которая выполняет как максимум что определено в ПЗ.

Типичный пример использования строгого соответствия заключается в выборе для приобретения продукта, для которого ожидается точное соответствие требований безопасности требованиям, определенным в ПЗ.

ЗБ, подтверждающее строгое соответствие некоторому ПЗ, может вводить дополнительные ограничения по отношению к ПЗ.

D.3 Демонстрируемое соответствие

Демонстрируемое соответствие ориентировано на разработчиков ПЗ, которым требуются свидетельства, что ЗБ является надлежащим для решения характерной проблемы безопасности, описанной в ПЗ.

Если в случае строго соответствия между ПЗ и ЗБ имеется четкое соотношение типа «подмножество — надмножество», то в случае демонстрируемого соответствия это соотношение менее четко определено. ЗБ, в которых утверждается о соответствии ПЗ, должны предлагать решение характерной проблемы безопасности, описанной в ПЗ.

Однако утверждение о соответствии допустимо только в случае, когда ЗБ налагает идентичные ПЗ или большие ограничения по отношению к ОО, а также — идентичные ПЗ или меньшие ограничения по отношению к среде функционирования ОО.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 15408-2	IDT	ГОСТ Р ИСО/МЭК 15408-2—2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»
ИСО/МЭК 15408-3	IDT	ГОСТ Р ИСО/МЭК 15408-3—2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности»
ИСО/МЭК 18045	IDT	ГОСТ Р ИСО/МЭК 18045—2008 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 15443 (все части), Information technology — Security techniques — Security assurance framework

[2] ISO/IEC 15446 Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

[3] ISO/IEC 19790 Information technology — Security techniques — Security requirements for cryptographic modules

[4] ISO/IEC 19791 Information technology — Security techniques — Security assessment of operational systems

[5] ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements

[6] ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

[7] IEEE Std 610.12—1990 Institute of Electrical and Electronics Engineers, Standard Glossary of Software Engineering Terminology

[8] Портал Common Criteria, CCRA, gost.e-ecolog.ru

УДК 681.324:006.354 ОКС 35.040 П85 ОКСТУ 4002

Ключевые слова: информационная технология, критерии оценки безопасности, задание по безопасности, профиль защиты, объект оценки, функциональные возможности безопасности, доверие к безопасности

Редактор *Е.В. Вахрушева*
Технический редактор *А.И. Белов*
Корректор *Н.В. Каткова*
Компьютерная верстка *Е.Г. Жилиной*

Сдано в набор 07.04.2014. Подписано в печать 29.04.2014. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 5,07. Тираж 59 экз. Зак. 2129.

Набрано в Издательском доме «Вебстер»
gost.e-ecolog.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru gost.e-ecolog.ru