ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1— 2008

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

ISO/IEC 15408-1:2005
Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model
(IDT)

Издание официальное

БЗ 12—2007/455

Москва
Стандартинформ
2009

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»), Федеральным государственным учреждением «4 Центральный научно-исследовательский институт Министерства обороны России» (ФГУ «4 ЦНИИ Минобороны России»), Федеральным государственным унитарным предприятием «Научно-технический и сертификационный центр по комплексной защите информации» ФГУП Центр «Атомзащитаинформ», Федеральным государственным унитарным предприятием «Центральный научно-исследовательский институт управления, экономики и информации Росатома» (ФГУП «ЦНИИАТОМИНФОРМ») при участии экспертов Международной рабочей группы по общим критериям на основе собственного аутентичного перевода стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 519-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 15408-1:2005 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (ISO/IEC 15408-1:2005 «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 С

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 15408-1—2002

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «Национальные стандарты». Соответствующая информация, уведомления и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет

© Стандартинформ, 2009

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

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 2
3 Обозначения и сокращения . . . 5
4 Краткий обзор . . . 5
4.1 Введение . . . 5
4.2 Контекст оценки . . . 6
4.3 Структура ИСО/МЭК 15408 . . . 7
5 Общая модель . . . 8
5.1 Контекст безопасности . . . 8
5.2 Подход ИСО/МЭК 15408 . . . 10
5.3 Понятия безопасности . . . 12
5.4 Описательные возможности ИСО/МЭК 15408 . . . 15
6 Требования ИСО/МЭК 15408 и результаты оценки . . . 20
6.1 Введение . . . 20
6.2 Требования, включаемые в профиль защиты и задание по безопасности . . . 20
6.3 Требования к объекту оценки . . . 21
6.4 Результаты оценки соответствия . . . 21
6.5 Использование результатов оценки объекта оценки . . . 22
Приложение А (обязательное) Спецификация профилей защиты . . . 23
Приложение В (обязательное) Спецификация заданий по безопасности . . . 27
Приложение С (обязательное) Сведения о соответствии национальных стандартов ссылочным международным стандартам . . . 33
Библиография . . . 34

Введение

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

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

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

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

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

ИСО/МЭК 15408 дает возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности продуктов или систем ИТ и мерам доверия, применяемым к ним при оценке безопасности. В процессе оценки достигается определенный уровень уверенности в том, что функции безопасности таких продуктов или систем, а также предпринимаемые меры доверия отвечают предъявляемым требованиям. Результаты оценки могут помочь потребителям решить, являются ли продукты или системы ИТ достаточно безопасными для их предполагаемого применения и приемлемы ли прогнозируемые риски при их использовании.

ИСО/МЭК 15408 полезен в качестве руководства как при разработке продуктов или систем с функциями безопасности ИТ, так и при приобретении коммерческих продуктов или систем с функциями безопасности. При оценке продукт или систему ИТ с функциями безопасности называют объектом оценки (ОО). К таким ОО, например, относятся операционные системы, вычислительные сети, распределенные системы и приложения.

ИСО/МЭК 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Характеристики защищенности, относящиеся к данным 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 сосредоточен на угрозах информации, возникающих в результате действий человека как злоумышленных, так и иных, но возможно также применение ИСО/МЭК 15408 и для некоторых угроз, не связанных с человеческим фактором. Кроме того, ИСО/МЭК 15408 может быть применим и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

ИСО/МЭК 15408 применим к мерам безопасности ИТ, реализуемым аппаратными, программно-аппаратными и программными средствами. Если предполагается, что отдельные аспекты оценки применимы только для некоторых способов реализации, это будет отмечено при изложении соответствующих критериев.

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 — 2009—10—01

1 Область применения

ИСО/МЭК 15408 предназначен для использования в качестве основы при оценке характеристик безопасности продуктов или систем информационных технологий (ИТ). Устанавливая общую базу критериев, ИСО/МЭК 15408 позволяет сделать результаты оценки безопасности ИТ значимыми для более широкой аудитории.

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 мерам безопасности ИТ. Известно, что безопасность ОО в значительной степени может быть достигнута административными мерами, такими как организационные меры, меры управления персоналом, меры управления физической защитой и процедурные меры. Административные меры безопасности в среде эксплуатации ОО рассматриваются в качестве предположений о безопасном использовании там, где они влияют на способность мер безопасности ИТ противостоять установленным угрозам.

b) Оценка специальных физических аспектов безопасности ИТ, таких как контроль электромагнитного излучения, прямо не затрагивается, хотя многие концепции ИСО/МЭК 15408 применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО.

c) В ИСО/МЭК 15408 не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ИСО/МЭК 15408 может использоваться для целей оценки в контексте такой структуры и такой методологии.

d) Процедуры использования результатов оценки безопасности при аттестации продуктов и систем ИТ находятся вне области действия ИСО/МЭК 15408. Аттестация продукта или системы ИТ является административным процессом, посредством которого предоставляются полномочия на их использование в конкретной среде эксплуатации. Оценка концентрируется на тех аспектах безопасности продукта или системы ИТ и среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки безопасности являются, следовательно, важными исходными материалами для процесса аттестации. Однако, поскольку для оценки не связанных с ИТ характеристик безопасности продукта или системы, а также их соотнесения с аспектами безопасности ИТ более приемлемы другие способы, аттестующим следует предусмотреть для этих аспектов особый подход.

Издание официальное

е) ИСО/МЭК 15408 не включает в себя критерии для оценки специфических качеств криптографических алгоритмов. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяется ИСО/МЭК 15408, должно быть предусмотрено проведение таких оценок.

Данная часть ИСО/МЭК 15408 устанавливает две формы представления функциональных требований и требований доверия к безопасности ИТ. Конструкция «профиль защиты» (ПЗ) предусматривает создание обобщенного, предназначенного для многократного использования набора этих требований безопасности. ПЗ может быть использован предполагаемыми потребителями для спецификации и идентификации продуктов с характеристиками безопасности ИТ, которые будут удовлетворять их потребностям. Задание по безопасности (ЗБ) содержит требования безопасности и специфицирует функции безопасности для конкретного продукта или системы, подлежащих оценке и называемых объектом оценки (ОО). ЗБ используется оценщиками в качестве основы для оценки, проводимой в соответствии с ИСО/МЭК 15408.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

Примечание — Раздел 2 содержит только специфичные термины, которые используются во всем тексте ИСО/МЭК 15408. Большинство терминов в ИСО/МЭК 15408 применяется согласно словарным или общепринятым определениям, которые включены в глоссарии по безопасности ИСО или в другие широко известные сборники терминов по безопасности. Некоторые комбинации общих терминов, используемые в ИСО/МЭК 15408 и не вошедшие в настоящий раздел, объясняются непосредственно в тексте (в месте использования). Объяснение специфичных терминов и понятий, применяемых в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, можно найти в их соответствующих разделах «Парадигма».

2.1 **активы** (assets): Информация или ресурсы, подлежащие защите контрмерами ОО.

2.2 **назначение** (assignment): Спецификация определенного параметра в компоненте.

2.3 **доверие** (assurance): Основание для уверенности в том, что сущность отвечает своим целям безопасности.

2.4 **потенциал нападения** (attack potential): Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя.

2.5 **усиление** (augmentation): Добавление одного или нескольких компонентов доверия из ИСО/МЭК 15408-3 в оценочный уровень доверия (ОУД) или пакет требований доверия.

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

2.7 **уполномоченный пользователь** (authorised user): Пользователь, которому в соответствии с политикой безопасности объекта оценки (ПБО) разрешено выполнять некоторую операцию.

2.8 **класс** (class): Группа семейств, объединенных общим назначением.

2.9 **компонент** (component): Наименьшая выбираемая совокупность элементов, которая может быть включена в профиль защиты (ПЗ), задание по безопасности (ЗБ) или пакет.

2.10 **связность** (connectivity): Свойство объекта оценки (ОО), позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО. Данное взаимодействие включает в себя обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

2.11 **зависимость** (dependency): Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено с тем, чтобы и другие требования могли отвечать своим целям.

2.12 **элемент** (element): Неделимое требование безопасности.

2.13 **оценка** (evaluation): Оценка ПЗ, ЗБ или ОО по определенным критериям.

2.14 **оценочный уровень доверия** (evaluation assurance level): Пакет компонентов доверия из ИСО/МЭК 15408-3, представляющий некоторое положение на определенной в ИСО/МЭК 15408 шкале доверия.

2.15 **орган оценки** (evaluation authority): Организация, которая посредством системы оценки обеспечивает реализацию ИСО/МЭК 15408 для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества.

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

2.17 **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.

2.18 **внешняя сущность ИТ** (external IT entity): Любой продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним.

2.19 **семейство** (family): Группа компонентов, которые направлены на достижение одних и тех же целей безопасности, но могут отличаться акцентами или строгостью.

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

2.21 **документация руководств** (guidance documentation): Документация руководств, описывающая поставку, установку, конфигурирование, эксплуатацию, управление и использование ОО в той части, в которой эти виды деятельности имеют отношение к пользователям, администраторам и интеграторам ОО. Требования к области применения и содержанию документированных руководств определяются в ПЗ и ЗБ.

2.22 **человек-пользователь** (human user): Любое лицо, взаимодействующее с ОО.

2.23 **идентификатор** (identity): Представление уполномоченного пользователя (например строка символов), однозначно его идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя или его псевдоним.

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

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

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

2.27 **передача между ФБО** (inter-TSF transfers): Передача данных между функциями безопасности объекта оценки (ФБО) и функциями безопасности других доверенных продуктов ИТ.

2.28 **итерация** (iteration): Более чем однократное использование компонента при различном выполнении операций.

2.29 **объект** (object): Сущность в пределах области действия ФБО (ОДФ), которая содержит или получает информацию и над которой субъекты выполняют операции.

2.30 **политика безопасности организации** (organisational security policies): Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

2.31 **пакет** (package): Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединенных для удовлетворения совокупности определенных целей безопасности.

2.32 **продукт** (product): Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

2.33 **профиль защиты** (protection profile): Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

2.34 **монитор обращений** (reference monitor): Концепция абстрактной машины, осуществляющей политики управления доступом ОО.

2.35 **механизм проверки правомочности обращений** (reference validation mechanism): Реализация концепции монитора обращений, обладающая следующими свойствами: защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования.

2.36 **уточнение** (refinement): Дополнение компонента деталями.

2.37 **роль** (role): Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО.

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

2.39 **атрибут безопасности** (security attribute): Характеристики субъектов, пользователей объектов, информации и/или ресурсов, которые используются для осуществления ПБО.

2.40 **функция безопасности** (security function): Функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

2.41 **политика функции безопасности** (security function policy): Политика безопасности, осуществляемая функцией безопасности (ФБ).

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

2.43 **задание по безопасности** (security target): Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.

2.44 **выбор** (selection): Выделение одного или нескольких элементов из перечня в компоненте.

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

2.46 **базовая СФБ** (SOF-basic): Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.

2.47 **высокая СФБ** (SOF-high): Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

2.48 **средняя СФБ** (SOF-medium): Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

2.49 **стойкость функции безопасности** (strength of function): Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности.

2.50 **субъект** (subject): Сущность в пределах ОДФ, инициирующая выполнение операций.

2.51 **система** (system): Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

2.52 **объект оценки** (target of evaluation): Продукт или система ИТ и связанная с ними документация руководств, являющиеся предметом оценки.

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

2.54 **функции безопасности ОО** (TOE security functions): Совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

2.55 **интерфейс функций безопасности ОО** (TOE security functions interface): Совокупность интерфейсов как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации.

2.56 **политика безопасности ОО** (TOE security policy): Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО.

2.57 **модель политики безопасности ОО** (TOE security policy model): Структурированное представление политики безопасности, которая должна быть осуществлена ОО.

2.58 **передача за пределы области действия ФБО** (transfers outside TSF control): Передача данных сущностям, не контролируемым ФБО.

2.59 **доверенный канал** (trusted channel): Средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО.

2.60 **доверенный маршрут** (trusted path): Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО.

2.61 **данные ФБО** (TSF data): Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

2.62 **область действия ФБО** (TSF scope of control): Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

2.63 **пользователь** (user): Любая сущность (человек-пользователь или внешняя сущность ИТ) вне ОО, которая взаимодействует с ОО.

2.64 **данные пользователя** (user data): Данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО.

3 Обозначения и сокращения

В ИСО/МЭК 15408 применяют следующие сокращения:

ЗБ (ST) — задание по безопасности;
ИТ (IT) — информационная технология;
ИФБО (TSFI) — интерфейс функции безопасности объекта оценки;
ОДФ (TSC) — область действия функции безопасности объекта оценки;
ОО (TOE) — объект оценки;
ОУД (EAL) — оценочный уровень доверия;
ПБО (TSP) — политика безопасности объекта оценки;
ПЗ (PP) — профиль защиты;
ПФБ (SFP) — политика функции безопасности;
СФБ (SOF) — стойкость функции безопасности;
ФБ (SF) — функция безопасности;
ФБО (TSF) — функции безопасности объекта оценки.

4 Краткий обзор

В настоящем разделе представлены основные положения ИСО/МЭК 15408. В нем определены категории пользователей ИСО/МЭК 15408, контекст оценки и принятый подход к представлению материала.

4.1 Введение

Информация, содержащаяся в системах или продуктах ИТ, является критическим ресурсом, позволяющим организациям успешно решать свои задачи. Кроме того, частные лица вправе ожидать, что их персональная информация, размещенная в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не будет подвергнута несанкционированной модификации. При выполнении продуктами или системами ИТ своих функций следует осуществлять надлежащее управление информацией для обеспечения ее защиты от опасностей нежелательного или неоправданного распространения, изменения или потери. Термин «безопасность ИТ» используется для того, чтобы рассмотреть предотвращение и уменьшение этих и подобных опасностей.

Многие потребители ИТ из-за недостатка знаний, компетентности или ресурсов, не будучи уверены в безопасности применяемых продуктов и систем ИТ, возможно, не захотят полагаться исключительно на заверения разработчиков. Чтобы повысить свою уверенность в мерах безопасности продукта или системы ИТ, потребители могут заказать проведение анализа безопасности этого продукта или системы (то есть оценку безопасности).

ИСО/МЭК 15408 может использоваться для выбора приемлемых мер безопасности ИТ. В нем содержатся критерии оценки требований безопасности.

4.1.1 Пользователи ИСО/МЭК 15408

В оценке характеристик безопасности продуктов и систем ИТ заинтересованы в основном потребители, разработчики и оценщики. Критерии, изложенные в настоящем стандарте, структурированы в интересах этих групп, потому что именно они рассматриваются как основные группы пользователей ИСО/МЭК 15408. В последующих подпунктах объяснено, какую пользу могут принести критерии каждой из этих групп.

4.1.1.1 Потребители

ИСО/МЭК 15408 играет важную роль в методической поддержке выбора потребителями требований безопасности ИТ для выражения своих потребностей. 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 оцениваемый продукт или система 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 продуктов и систем. Этому способствует иерархическое представление требований доверия.

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

4.1.1.2 Разработчики

ИСО/МЭК 15408 предназначен для поддержки разработчиков при подготовке к оценке своих продуктов или систем и ее проведении, а также при установлении требований безопасности, которым должны удовлетворять каждый их продукт или система. Использование совместно с ИСО/МЭК 15408 методологии оценки, потенциально сопровождаемой соглашением о взаимном признании результатов оценки, позволит использовать ИСО/МЭК 15408 для поддержки иных лиц, помимо разработчиков ОО, при подготовке этого ОО к оценке и содействовать ее проведению.

Конструкции из ИСО/МЭК 15408 могут использоваться для формирования утверждения о соответствии ОО установленным для него требованиям посредством подлежащих оценке специфицированных функций безопасности и мер доверия. Требования для конкретного ОО содержатся в зависимой от реализации конструкции, называемой заданием по безопасности (ЗБ). Требования широкого круга потребителей могут быть представлены в одном или нескольких ПЗ.

В ИСО/МЭК 15408 изложены функции безопасности, которые разработчик мог бы включить в ОО. ИСО/МЭК 15408 можно также применять для определения обязанностей и действий по подготовке свидетельств, необходимых при проведении оценки ОО. Он также определяет содержание и представление таких свидетельств.

4.1.1.3 Оценщики

ИСО/МЭК 15408 содержит критерии, предназначенные для использования оценщиками ОО при формировании заключения о соответствии объектов оценки предъявленным к ним требованиям безопасности. В ИСО/МЭК 15408 приведено описание совокупности основных действий, выполняемых оценщиком, и функций безопасности, к которым относятся эти действия. ИСО/МЭК 15408, однако, не определяет процедуры, которых следует придерживаться при выполнении данных действий.

4.1.1.4 Прочие

Хотя ИСО/МЭК 15408 ориентирован на определение и оценку характеристик безопасности ИТ для объектов оценки, он также может служить справочным материалом для тех, кто интересуется вопросами безопасности ИТ или несет ответственность за безопасность. Среди них можно выделить, например, следующие группы, представители которых смогут извлечь пользу из информации, содержащейся 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 (внутренние и внешние), ответственные за оценку адекватности безопасности системы;

c) проектировщики систем безопасности, ответственные за спецификацию основного содержания безопасности систем и продуктов ИТ;

d) аттестующие, ответственные за приемку системы ИТ 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.

4.2 Контекст оценки

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

ИСО/МЭК 15408 не содержит требований к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок. Основные элементы формирования контекста для оценок показаны на рисунке 1.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие критерии 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. Процедура 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.

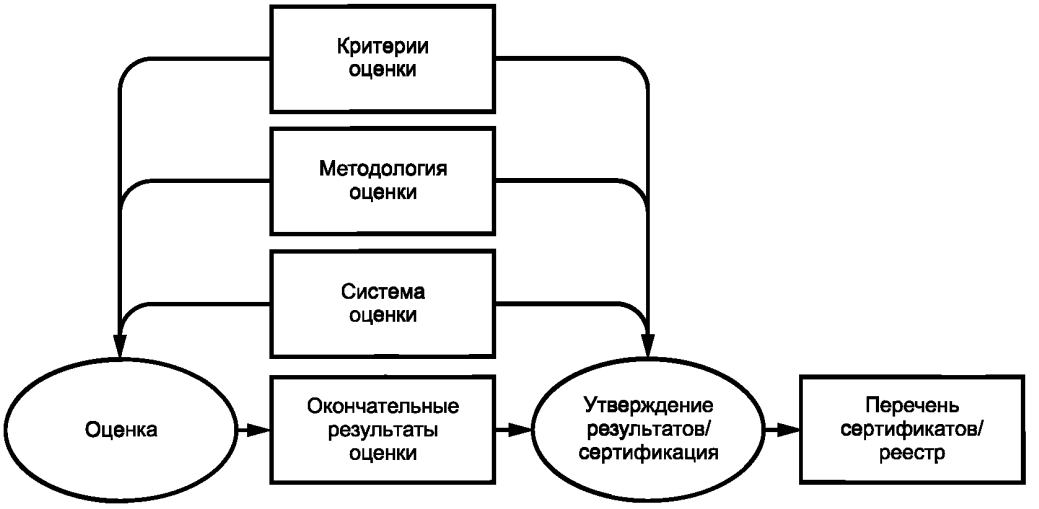


Рисунок 1 — Контекст оценки

Система оценки, методология и процедуры сертификации находятся в ведении органов оценки, управляющих системами оценки, и выходят за рамки действия ИСО/МЭК 15408.

4.3 Структура ИСО/МЭК 15408

ИСО/МЭК 15408 состоит из нескольких отдельных, но взаимосвязанных частей, перечисленных ниже. Термины, используемые при описании данных частей, пояснены в разделе 5.

a) Часть 1 «Введение и общая модель» является введением в ИСО/МЭК 15408. В ней определены общие принципы и концепции оценки безопасности ИТ и приведена общая модель оценки. Представлены конструкции для выражения целей безопасности ИТ, выбора и определения требований безопасности ИТ и написания высокоуровневых спецификаций для продуктов и систем. Кроме того, в этой части указано, в чем заключается полезность каждой из частей ИСО/МЭК 15408 применительно к каждой из основных групп пользователей ИСО/МЭК 15408.

b) Часть 2 «Функциональные требования безопасности» устанавливает совокупность функциональных компонентов как стандартный способ выражения функциональных требований к ОО и содержит каталог всех функциональных компонентов, семейств и классов.

c) Часть 3 «Требования доверия к безопасности» устанавливает совокупность компонентов доверия как стандартный способ выражения требований доверия к ОО и содержит каталог всех компонентов, семейств и классов доверия. Кроме того, в данной части определены критерии оценки профилей защиты и заданий по безопасности и представлены оценочные уровни доверия (ОУД), которые устанавливают предопределенную в ИСО/МЭК 15408 шкалу ранжирования доверия к ОО.

Предполагается, что в поддержку трех частей ИСО/МЭК 15408, перечисленных выше, будут опубликованы также 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 — Путеводитель по критериям оценки безопасностик информационных технологий

Часть	Потребитель	Разработчик	Оценщик
1	Общие сведения по применению. Руководство по структуре профилей защиты	Общие сведения и руководство по разработке требований и формулированию спецификаций безопасности для объектов оценки	Общие сведения и руководство по применению. Руководство по структуре профилей защиты и заданий по безопасности
2	Руководство и справочник по формулированию требований к функциям безопасности	Справочник по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки	Критерии оценки, используемые при определении эффективности выполнения объектом оценки заявленных функций безопасности
3	Руководство по определению требуемого уровня доверия	Справочник по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки	Критерии оценки, используемые при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности

5 Общая модель

В настоящем 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 развивают эти понятия в рамках описанного подхода. Данный раздел предполагает наличие определенных знаний по безопасности ИТ и не предназначен для использования в качестве учебного пособия в этой области.

Безопасность рассматривается в ИСО/МЭК 15408 с использованием совокупности понятий и терминологии в области безопасности. Их понимание является предпосылкой эффективного использования ИСО/МЭК 15408. Однако сами по себе эти понятия имеют самый общий характер и не должны ограничивать область проблем безопасности ИТ, к которым применим ИСО/МЭК 15408.

5.1 Контекст безопасности

5.1.1 Общий контекст безопасности

Безопасность связана с защитой активов от угроз, при этом угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами. Во внимание следует принимать все разновидности угроз, но в сфере безопасности наибольшее внимание уделяется тем из них, которые связаны со злонамеренными или иными действиями человека. Высокоуровневые понятия безопасности и их взаимосвязь представлены на рисунке 2.

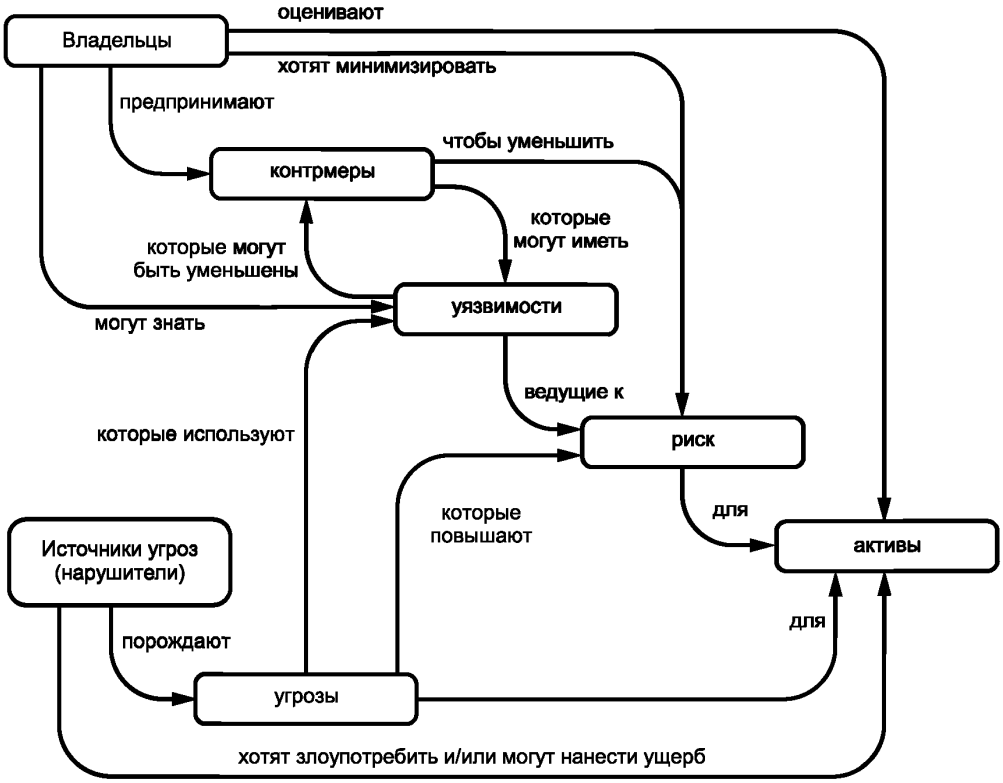


Рисунок 2 — Понятия безопасности и их взаимосвязь

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 владельцев. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельцев. К специфическим нарушениям безопасности обычно относят (но не ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателям (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Владельцы активов будут анализировать угрозы, применимые к их активам и среде, определяя связанные с ними риски. Анализ угроз может помочь при выборе контрмер для противостояния угрозам и уменьшения рисков до приемлемого уровня.

Контрмеры предпринимают для уменьшения уязвимостей и выполнения политики безопасности владельцев активов (прямо или косвенно распределяя их между этими составляющими). Но и после введения контрмер могут сохраняться остаточные уязвимости. Такие уязвимости могут использоваться нарушителями, определяя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск с учетом имеющихся ограничений.

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, владельцам активов необходимо убедиться, что предпринятые контрмеры обеспечат адекватное противостояние этим угрозам. Сами владельцы активов не всегда в состоянии судить обо всех аспектах предпринимаемых контрмер и поэтому могут потребовать проведение их оценки. Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В данном заключении устанавливают уровень доверия как результат применения контрмер. Доверие является той характеристикой контрмер, которая дает основание для уверенности в их надлежащем действии. Заключение о результатах оценки может быть использовано владельцем активов при принятии решения о приемлемости риска для активов, создаваемого угрозами. Взаимосвязь данных понятий, используемых при оценке, представлена на рисунке 3.

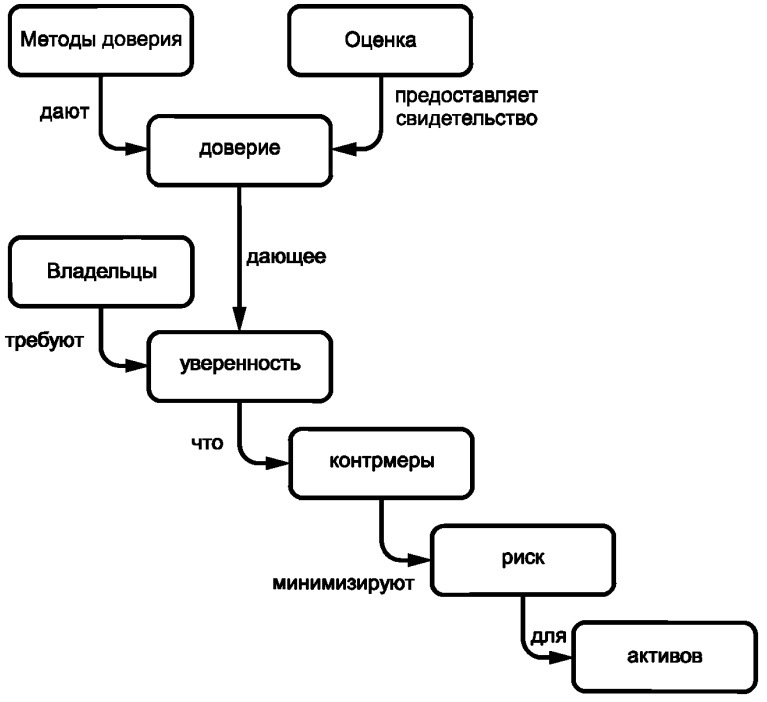


Рисунок 3 — Понятия, используемые при оценке, и их взаимосвязь

Поскольку ответственность за активы несут их владельцы, им следует иметь возможность отстаивать принятое решение о приемлемости для активов риска, создаваемого угрозами. Для этого требуется, чтобы результаты оценки были обоснованными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве доказательств.

5.1.2 Контекст безопасности информационных технологий

Многие активы представлены в виде информации, которая хранится, обрабатывается и передается продуктами или системами ИТ так, чтобы они соответствовали требованиям владельцев этой информации. Владельцы информации вправе потребовать, чтобы распространение и модификация любых

таких представлений информации (данных) строго контролировались. Они могут потребовать, чтобы продукт или система ИТ реализовали характерные для ИТ меры управления безопасностью как часть всей совокупности контрмер безопасности, применяемых для противостояния угрозам безопасности данных.

Системы ИТ приобретают и создают для выполнения конкретных требований и при этом по экономическим причинам могут максимально использовать имеющиеся коммерческие продукты ИТ, такие как операционные системы, компоненты прикладного программного обеспечения общего назначения и аппаратные платформы. Контрмеры безопасности ИТ, реализованные в системе, могут использовать функции, имеющиеся во включаемых в систему продуктах ИТ, и, следовательно, зависят от правильного выполнения функций безопасности продуктов ИТ. Поэтому продукты ИТ подлежат оценке в качестве составной части оценки безопасности системы ИТ.

Если продукт ИТ уже включен в состав различных систем ИТ или такое включение предполагается, то экономически целесообразна отдельная оценка аспектов безопасности подобного продукта и создание каталога оцененных продуктов. Результаты подобной оценки следует формулировать так, чтобы была возможность использования продукта в различных системах ИТ без повторения работ по экспертизе его безопасности.

Лица, аттестующие систему ИТ, должны иметь полномочия владельца информации для вынесения заключения о том, обеспечивает ли сочетание контрмер безопасности, относящихся и не относящихся к ИТ, адекватную защиту данных, и принятия на этом основании решения о допустимости эксплуатации данной системы. Аттестующий может потребовать оценки реализованных в ИТ контрмер, с тем чтобы решить, обеспечивают ли эти контрмеры адекватную защиту и правильно ли они реализованы в системе ИТ. Допускаются различные форма и степень строгости оценки в зависимости от правил, которыми руководствуется аттестующий или которые вводятся им.

5.2 Подход ИСО/МЭК 15408

Уверенность в безопасности ИТ может быть достигнута в результате действий, предпринятых в процессе разработки, оценки и эксплуатации ОО.

5.2.1 Разработка

ИСО/МЭК 15408 не предписывает конкретную методологию разработки или модель жизненного цикла. Основополагающие предположения о соотношениях между требованиями безопасности и собственно ОО представлены на рисунке 4. Рисунок 4 используется в качестве примера и его не следует интерпретировать как демонстрацию преимущества одной методологии разработки (например, каскадной) перед другой (например, по прототипу).

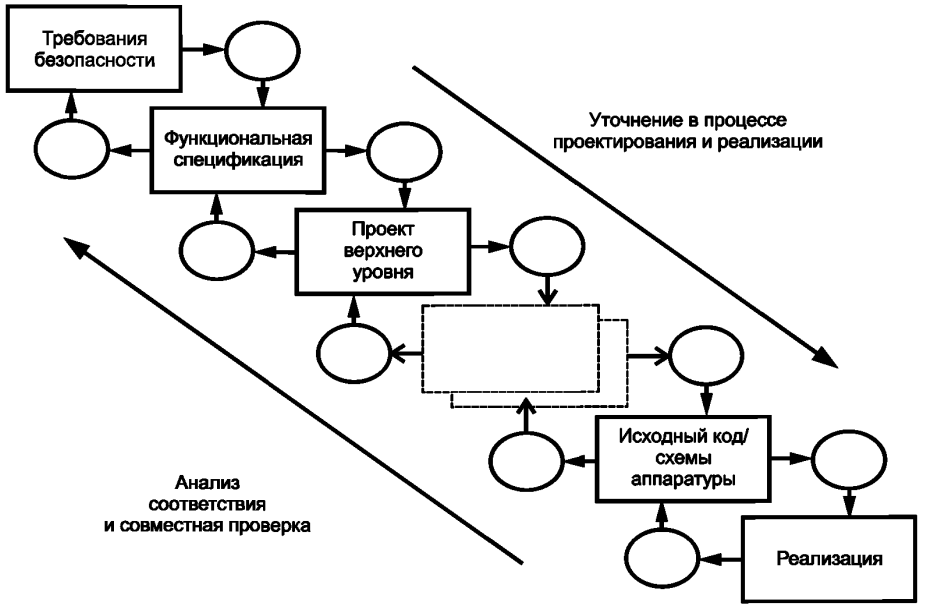


Рисунок 4 — Модель разработки ОО

Существенно, чтобы требования безопасности, предъявляемые к разработке ИТ, эффективно содействовали достижению целей безопасности, установленных потребителями. Если соответствующие требования не установлены до начала процесса разработки, то даже хорошо спроектированный конечный продукт может не отвечать целям предполагаемых потребителей.

Процесс разработки основан на уточнении требований безопасности, отображенных в краткой спецификации в составе задания по безопасности. Каждый последующий уровень уточнения представляет собой декомпозицию проекта с его дополнительной детализацией. Наименее абстрактным представлением является непосредственно реализация ОО.

ИСО/МЭК 15408 не предписывает конкретную совокупность представлений проекта. ИСО/МЭК 15408 требует, чтобы имелось достаточное число представлений проекта с достаточным уровнем детализации для демонстрации того, что:

a) каждый уровень уточнения полностью отображает более высокие уровни (то есть все функции, характеристики и режимы безопасности ОО, которые определены на более высоком уровне абстракции, должны быть наглядно представлены на более низком уровне);

b) каждый уровень уточнения точно отображает более высокие уровни (то есть не должно быть функций, характеристик и режимов безопасности ОО, которые были бы определены на более низком уровне абстракции, но при этом не требовались на более высоком уровне).

Критерии доверия из ИСО/МЭК 15408 идентифицируют следующие уровни абстракции проекта: функциональная спецификация, проект верхнего уровня, проект нижнего уровня и реализация. В зависимости от выбранного уровня доверия может потребоваться, чтобы разработчики показали, насколько методология разработки отвечает требованиям доверия из ИСО/МЭК 15408.

5.2.2 Оценка ОО

Процесс оценки ОО, как показано на рисунке 5, может проводиться параллельно с разработкой или следовать за ней. Основными исходными материалами для оценки ОО являются:

a) совокупность свидетельств, характеризующих ОО, включая ЗБ в качестве основы оценки ОО;

b) ОО, безопасность которого требуется оценить;

c) критерии, методология и система оценки.

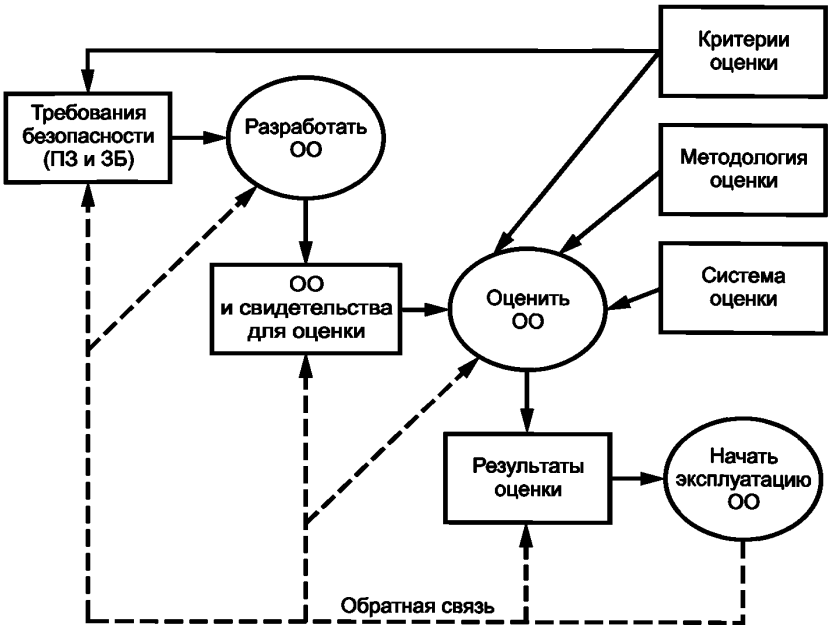


Рисунок 5 — Процесс оценки ОО

Кроме того, в качестве исходных материалов для оценки возможно также использование вспомогательных материалов (таких, например, как замечания по применению ИСО/МЭК 15408) и специальных знаний в области безопасности ИТ, которыми располагает оценщик и сообщество участников оценки.

Ожидаемым результатом оценки является подтверждение удовлетворения объектом оценки требований безопасности, изложенных в его ЗБ, а также один или несколько отчетов, документирующих выводы оценщика относительно ОО, сделанные в соответствии с критериями оценки. Такие отчеты, помимо разработчика, будут полезны также реальным и потенциальным потребителям продукта или системы, представленным как объект оценки.

Степень уверенности в безопасности ОО, получаемая в результате оценки, зависит от удовлетворенных при оценке требований доверия (например, от оценочного уровня доверия).

Оценка может способствовать созданию более безопасных продуктов ИТ двумя путями. Оценка позволяет выявить ошибки или уязвимости в ОО, устраняя которые разработчик снижает вероятность нарушения безопасности ОО при его последующей эксплуатации. Кроме того, готовясь к строгой оценке, разработчик, возможно, более внимательно отнесется к проектированию и разработке ОО. Поэтому процесс оценки может оказывать значительное, хотя и косвенное, положительное влияние на начальные требования, процесс разработки, конечный продукт и условия его эксплуатации.

5.2.3 Эксплуатация ОО

Потребители могут выбрать оцененный продукт для использования в конкретных условиях. Не исключено, что при эксплуатации ОО могут быть выявлены не обнаруженные до этого ошибки или уязвимости, а также может возникнуть необходимость пересмотра предположений относительно среды функционирования. Тогда по результатам эксплуатации потребуется внесение разработчиком исправлений в ОО либо переопределение требований безопасности или предположений относительно среды эксплуатации. Такие изменения могут привести к необходимости проведения новой оценки ОО или потребовать повышения безопасности среды его эксплуатации. В некоторых случаях для восстановления доверия к ОО достаточно оценить только требующиеся обновления. Детальное описание процедур переоценки, включая использование результатов ранее проведенных оценок, выходит за рамки ИСО/МЭК 15408.

5.3 Понятия безопасности

Критерии оценки наиболее полезны в контексте процессов проектирования и правовой базы, поддерживающих безопасную разработку и оценку ОО. Настоящий подраздел включен исключительно в иллюстративных и рекомендательных целях и не предназначен для регламентации процессов анализа, подходов к разработке или систем оценки, в рамках которых мог бы применяться ИСО/МЭК 15408.

ИСО/МЭК 15408 применяют, если при использовании ИТ придают значение способности элементов ИТ обеспечивать сохранность активов. Для того чтобы показать защищенность активов, вопросы безопасности необходимо рассматривать на всех уровнях, начиная с самого абстрактного и до конечной реализации ИТ в среде эксплуатации. Эти уровни представления, как описано в следующих пунктах, позволяют охарактеризовать задачи и проблемы безопасности, однако сами по себе не демонстрируют, что конечная реализация ИТ действительно соответствует требуемому режиму безопасности и поэтому может считаться доверенной.

ИСО/МЭК 15408 требует, чтобы конкретные уровни представления содержали обоснование представления ОО на данном уровне. Это значит, что такой уровень должен содержать убедительные аргументы, свидетельствующие о согласованности данного уровня с более высоким уровнем, а также о его полноте, корректности и внутренней непротиворечивости. Изложение обоснования, демонстрирующее согласованность со смежным более высоким уровнем представления, приводят как довод корректности ОО. Обоснование, непосредственно демонстрирующее соответствие ОО целям безопасности, поддерживает доводы о его эффективности в противостоянии угрозам и осуществлении политики безопасности организации.

В ИСО/МЭК 15408 использованы различные формы представления. Возможный способ последовательного формирования требований безопасности и спецификаций при разработке ПЗ или ЗБ представлен на рисунке 6. Все требования безопасности ОО, в конечном счете, следуют из рассмотрения предназначения и контекста ОО. Приведенная схема не предназначена для ограничения способов разработки ПЗ и ЗБ, а лишь иллюстрирует, каким образом результаты некоторых аналитических подходов связаны с содержанием ПЗ и ЗБ.

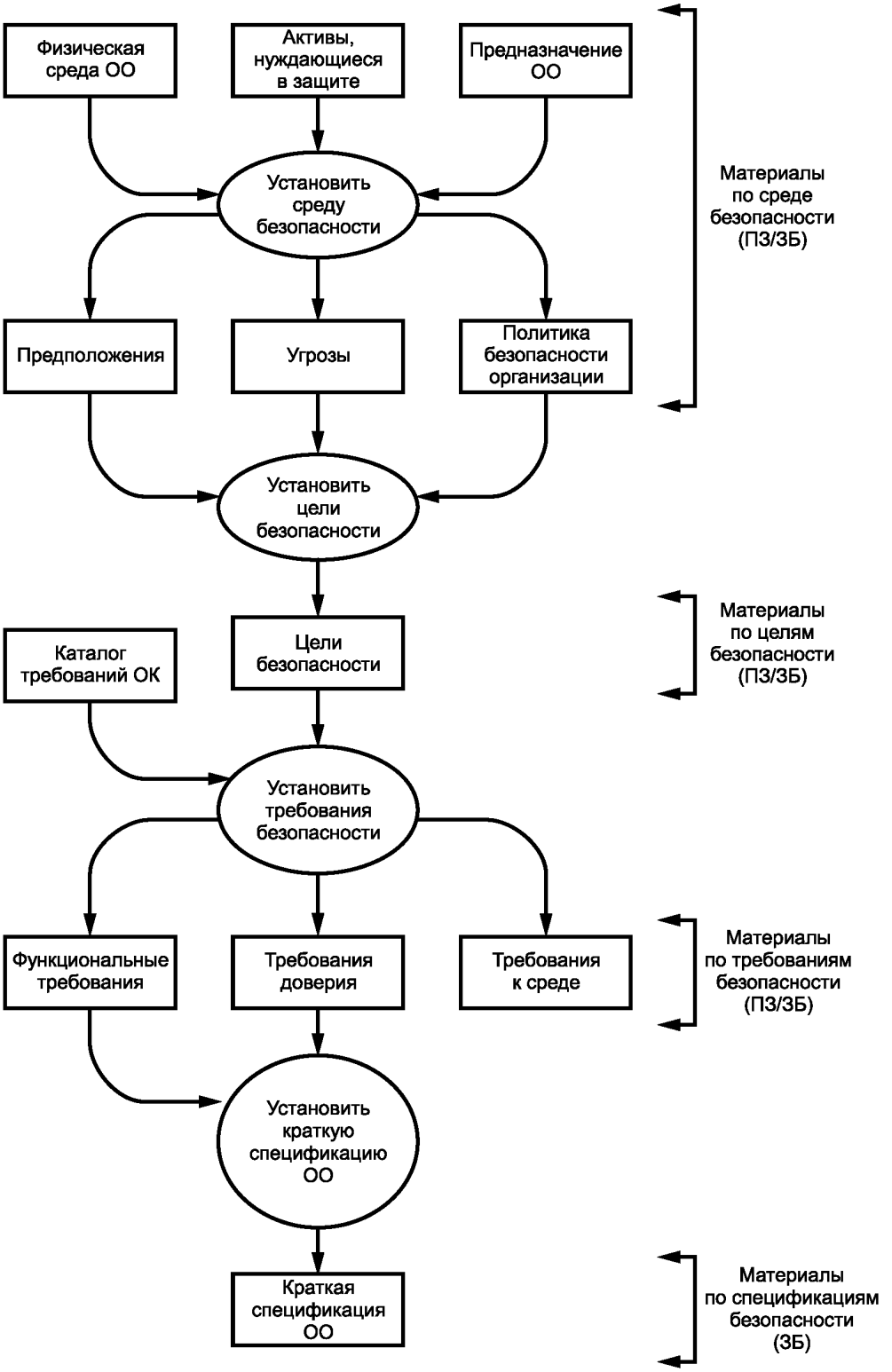


Рисунок 6 — Последовательное формирование требований и спецификаций

5.3.1 Среда безопасности

Среда безопасности включает в себя законы, политики безопасности организаций, опыт, специальные навыки и знания, имеющие отношение к безопасности. Таким образом, она определяет контекст предполагаемого применения ОО. Среда безопасности включает также угрозы безопасности, присутствие которых в этой среде установлено или предполагается.

При установлении среды безопасности автор ПЗ или ЗБ должен принять во внимание:

a) физическую среду ОО в той ее части, которая определяет все аспекты эксплуатационной среды ОО, касающиеся его безопасности, включая известные мероприятия, относящиеся к физической защите и персоналу;

b) активы, которые требуют защиты элементами ОО и к которым применяются требования или политики безопасности; они могут включать в себя активы, к которым это относится непосредственно, например файлы и базы данных, а также активы, которые косвенно подчинены требованиям безопасности, например, данные авторизации и собственно реализации ИТ;

c) предназначение ОО, включая тип продукта и предполагаемую сферу его применения.

Исследование политик безопасности, угроз и рисков должно позволить сформировать следующие специфичные для безопасности утверждения, относящиеся к ОО:

a) изложение предположений, которым удовлетворяла бы среда ОО для того, чтобы он считался безопасным. Это изложение может быть принято без доказательства при оценке ОО;

b) изложение угроз безопасности активов, в котором были бы идентифицированы все угрозы, прогнозируемые на основе анализа безопасности как относящиеся к ОО. В ИСО/МЭК 15408 угрозы раскрываются через понятия источника угрозы, предполагаемого метода нападения, любых уязвимостей, которые являются предпосылкой для нападения, и идентификации активов, являющихся целью нападения. При оценке рисков безопасности квалифицируют каждую угрозу безопасности с оценкой возможности ее перерастания в фактическое нападение, вероятности успешного проведения такого нападения и последствий любого возможного ущерба;

c) изложение политик безопасности, применяемых в организации, в котором были бы идентифицированы политики и правила, относящиеся к ОО. Для системы ИТ такие политики могут быть описаны достаточно точно, тогда как для продуктов ИТ или класса продуктов общего назначения о политике безопасности организации могут быть сделаны, при необходимости, только рабочие предположения.

5.3.2 Цели безопасности

Результаты анализа среды безопасности могут затем быть использованы для установления целей безопасности, которые направлены на противостояние установленным угрозам, а также проистекают из установленной политики безопасности организации и сделанных предположений. Цели безопасности должны быть согласованы с установленными целями применения или предназначением ОО как продукта, а также со всеми известными сведениями о физической среде ОО.

Смысл определения целей безопасности заключается в том, чтобы соотнести их со всеми поставленными ранее вопросами безопасности и декларировать, какие аспекты безопасности связаны непосредственно с ОО, а какие — с его средой. Такое разделение основано на совокупном учете инженерного опыта, политики безопасности, экономических факторов и решения о приемлемости рисков.

Цели безопасности для среды ОО достигаются как в рамках ИТ, так и нетехническими или процедурными способами.

Требования безопасности ИТ проистекают только из целей безопасности ОО и целей безопасности его среды, относящихся к ИТ.

5.3.3 Требования безопасности ИТ

Требования безопасности ИТ являются результатом преобразования целей безопасности в совокупность требований безопасности для ОО и требований безопасности для среды, которые, в случае их удовлетворения, обеспечат для ОО способность достижения целей его безопасности.

В ИСО/МЭК 15408 представлены две различные категории требований безопасности — функциональные требования и требования доверия.

Функциональные требования предъявляются к тем функциям ОО, которые предназначены для поддержания безопасности ИТ и определяют желательный безопасный режим функционирования ОО. Функциональные требования определены в ИСО/МЭК 15408-2. Примерами функциональных требова-

ний являются требования к идентификации, аутентификации, аудиту безопасности, неотказуемости источника (невозможности отказа от факта отправления сообщения).

Если ОО содержит функции безопасности, которые реализуются вероятностными или перестановочными механизмами (например, паролем или хэш-функцией), то требования доверия могут определять, что заявленный минимальный уровень стойкости согласуется с целями безопасности. При этом специфицированный уровень стойкости будет выбираться из следующих: базовая стойкость функции безопасности (СФБ), средняя СФБ, высокая СФБ. От каждой такой функции потребуется соответствие минимальному уровню стойкости или, по меньшей мере, дополнительно определенной специальной метрике.

Степень доверия к заданной совокупности функциональных требований может меняться; это, как правило, выражается через возрастание уровня строгости, задаваемого компонентами доверия. ИСО/МЭК 15408-3 определяет требования доверия и шкалу оценочных уровней доверия (ОУД), формируемых с использованием этих компонентов. Требования доверия предъявляются к действиям разработчика, представленным свидетельствам и действиям оценщика. Примерами требований доверия являются требования к строгости процесса разработки, поиску потенциальных уязвимостей и анализу их влияния на безопасность.

Доверие к тому, что цели безопасности достигаются посредством выбранных функций безопасности, зависит от уверенности:

a) в корректности реализации функций безопасности, то есть оценки того, правильно ли они реализованы;

b) в эффективности функций безопасности, то есть оценки того, действительно ли они отвечают изложенным целям безопасности.

Требования безопасности обычно включают в себя как требования наличия желательных режимов функционирования, так и требования отсутствия нежелательных режимов. Наличие желательного режима обычно можно продемонстрировать путем непосредственного применения или испытаний (тестирования). Не всегда удается убедительно продемонстрировать отсутствие нежелательного режима. Уменьшению риска наличия нежелательного режима в значительной мере способствуют испытания (тестирование), экспертиза проекта и окончательной реализации. Изложение обоснования представляет дополнительную поддержку утверждению об отсутствии нежелательного режима.

5.3.4 Краткая спецификация ОО

Краткая спецификация ОО, предусмотренная в составе ЗБ, определяет отображение требований безопасности для ОО. В ней обеспечивается высокоуровневое определение функций безопасности, заявляемых для удовлетворения функциональных требований, и мер доверия, предпринимаемых для удовлетворения требований доверия.

5.3.5 Реализация ОО

Реализацией ОО является его воплощение, основанное на функциональных требованиях безопасности и краткой спецификации ОО, содержащейся в ЗБ. При осуществлении реализации ОО используются инженерные навыки и знания в области ИТ и безопасности. ОО будет отвечать целям безопасности, если он правильно и эффективно реализует все требования безопасности, содержащиеся в ЗБ.

5.4 Описательные возможности ИСО/МЭК 15408

ИСО/МЭК 15408 устанавливает базовую структуру для проведения оценки. Представлением требований к свидетельствам и анализу может достигаться получение более объективных и, следовательно, более значимых результатов оценки. В ИСО/МЭК 15408 вводятся общая совокупность конструкций и язык для выражения и взаимосвязи аспектов безопасности ИТ, что дает возможность воспользоваться накопленным опытом и специальными знаниями.

5.4.1 Представление требований безопасности

ИСО/МЭК 15408 определяет совокупность конструкций, объединяемых в содержательные наборы требований безопасности известной пригодности, которые затем могут быть использованы при установлении требований безопасности к перспективным продуктам и системам. Взаимосвязь различных конструкций для выражения требований изложена ниже и представлена на рисунке 7.

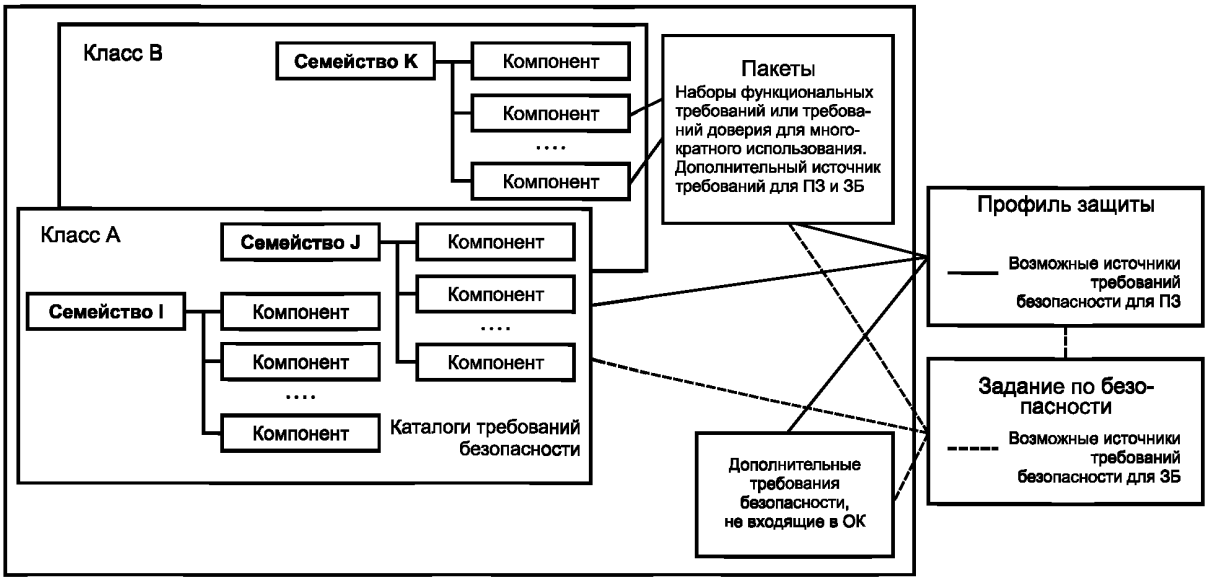


Рисунок 7 — Организация и структура требований

Организация требований безопасности в ИСО/МЭК 15408 в виде иерархии «класс — семейство — компонент» призвана помочь потребителям в поиске конкретных требований безопасности.

Функциональные требования и требования доверия представлены в ИСО/МЭК 15408 в едином стиле с использованием одной и той же структуры и терминологии.

5.4.1.1 Класс

Термин «класс» применяется для наиболее общего группирования требований безопасности. Все составляющие класса имеют общую направленность, но различаются по охвату целей безопасности.

Составляющие класса называются «семействами».

5.4.1.2 Семейство

Семейство — это группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью.

Составляющие семейства называются «компонентами».

5.4.1.3 Компонент

Компонент описывает специфический набор требований безопасности, который является наименьшим выбираемым набором требований безопасности для включения в структуры, определенные в ИСО/МЭК 15408. Совокупность компонентов, входящих в семейство, может быть упорядочена для представления возрастания строгости или возможностей требований безопасности, имеющих общее назначение. Компоненты могут быть также упорядочены частично, для представления связанных неиерархических наборов. Упорядочение неприменимо в случае, когда в семействе имеется только один компонент.

Компоненты состоят из отдельных элементов. Элемент — это выражение требований безопасности на самом нижнем уровне. Элемент является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

5.4.1.3.1 Зависимости между компонентами

Между компонентами могут существовать зависимости. Зависимости возникают, если компонент не самодостаточен и предполагает наличие другого компонента. Зависимости могут существовать между функциональными компонентами, между компонентами доверия, а также между функциональными компонентами и компонентами доверия.

Описание зависимостей компонента является частью определения компонента в ИСО/МЭК 15408. Для обеспечения полноты требований к ОО следует удовлетворить там, где это необходимо, зависимости всех компонентов при их включении в ПЗ и ЗБ.

5.4.1.3.2 Разрешенные операции на компонентах

Функциональные компоненты и компоненты доверия из ИСО/МЭК 15408 можно использовать так, как они сформулированы в ИСО/МЭК 15408, или можно их конкретизировать, применяя разрешенные операции для удовлетворения какой-то цели безопасности. Если какой-то элемент в рамках компонента

подвергается уточнению, автор ПЗ/ЗБ должен четко идентифицировать, что такое уточнение было выполнено. Автор ПЗ/ЗБ должен также отследить, чтобы требуемые зависимости других требований, зависящих 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 специфицировать параметры;

c) выбор (selection) — позволяет специфицировать один или несколько пунктов из перечня;

d) уточнение (refinement) — позволяет осуществлять детализацию.

5.4.1.3.2.1 Итерация

Там, где необходимо охватить различные аспекты одного и того же требования (например, идентифицировать несколько типов пользователей), разрешается повторное использование одного и того же компонента, позволяющее охватить каждый аспект.

Хотя итерация относится к уровню компонента требования, нет необходимости при каждой итерации повторять полный текст компонента, так как это привело бы к повторению без изменений некоторых элементов в рамках компонента. Допускается в ПЗ или ЗБ повторять только те элементы требований, которые каждый раз изменяются путем уточнения либо выполнения операций назначения или выбора (см. 5.4.1.3.2.4 для дальнейшего руководства по итерации уточненных требований).

5.4.1.3.2.2 Назначение

Некоторые компоненты включают в себя элементы, которые содержат параметры, дающие возможность разработчику ПЗ/ЗБ специфицировать совокупность величин, включаемых в ПЗ/ЗБ для достижения какой-то цели безопасности. Эти элементы четко идентифицируют каждый такой параметр и ограничения на значения, которые может принимать этот параметр.

Любой аспект элемента, допустимые значения которого могут быть однозначно описаны или перечислены, может быть представлен параметром. Параметр может быть атрибутом или правилом, сводящим требование к определенному значению или диапазону значений. Например, некоторый элемент в рамках компонента, направленный на достижение определенной цели безопасности, может установить, что данную операцию следует выполнять несколько раз. В этом случае назначение установит число возможных повторений (или диапазон для него), которое будет использоваться для данного параметра.

5.4.1.3.2.3 Выбор

Операция заключается в выборе одного или нескольких пунктов из перечня для ограничения области применения элемента в рамках конкретного компонента.

5.4.1.3.2.4 Уточнение

Для всех компонентов разработчику ПЗ/ЗБ разрешается ограничить набор допустимых реализаций путем определения дополнительных деталей для достижения некоторой цели безопасности. Уточнение элемента в рамках компонента заключается в дополнении этими техническими деталями.

Для того чтобы изменение в компоненте считалось допустимым уточнением, оно должно удовлетворять всем перечисленным ниже условиям:

a) ОО, отвечающий уточненному требованию, также должен отвечать исходному требованию, интерпретированному в контексте ПЗ/ЗБ;

b) в случаях если уточненное требование подвергается итерации, допускается, чтобы каждая итерация относилась только к подмножеству области действия данного требования; тем не менее все итерации в совокупности должны охватывать всю область действия исходного требования;

c) уточненное требование не должно расширять область действия исходного требования;

d) уточненное требование не должно изменять список зависимостей исходного требования.

Несколько примеров допустимых уточнений:

a) любое изменение, являющееся исключительно редакционным, такое как улучшение читабельности выполненного назначения или соблюдение правил грамматики;

b) изменение, не меняющее область действия требования из-за контекста, в котором оно используется в ПЗ/ЗБ. Например, изменение требования, определяющего «пользователей ОО» в качестве «telnet-пользователей ОО» будет допустимым уточнением, если пользователи ОО являются только telnet-пользователями;

c) изменение, предоставляющее информацию о допустимых подходах к реализации, не расширяя область действия требования. Примером допустимого уточнения является изменение требования «обеспечить способность верифицировать» на «обеспечить способность верифицировать путем применения криптографических контрольных сумм». Изменение устанавливает ограничения на тип механизма, используемого при выполнении существующего требования, и не расширяет область действия исходного требования.

Приложения ИСО/МЭК 15408-2 предоставляют руководство по допустимому выполнению операций выбора и назначения. Данное руководство предоставляет нормативные инструкции по выполнению операций, и этим инструкциям необходимо следовать, если автор ПЗ/ЗБ логически не обоснует отклонение:

a) отклонение «Нет» допускается как вариант выполнения выбора только в случае, если данный вариант 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 выбора. Если отклонение «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 в приложениях ИСО/МЭК 15408-2 указывается, когда отклонение «Нет» является допустимым выполнением.

Некоторые требуемые операции могут быть завершены (полностью или частично) в ПЗ или оставлены для завершения в ЗБ. Однако в ЗБ все операции должны быть завершены.

5.4.1.4 Использование требований безопасности

В ИСО/МЭК 15408 определены три типа конструкций требований: пакет, ПЗ и ЗБ. Помимо этого в ИСО/МЭК 15408 определена совокупность критериев безопасности ИТ, которые могут отвечать потребностям многих сообществ потребителей и поэтому служат основным исходным материалом для создания указанных конструкций. При разработке ИСО/МЭК 15408 предусматривалось использование везде, где это возможно, определенных в ИСО/МЭК 15408 компонентов требований безопасности, представляющих известную и понятную сферу применения. Взаимосвязь между различными конструкциями требований безопасности представлена на рисунке 8.

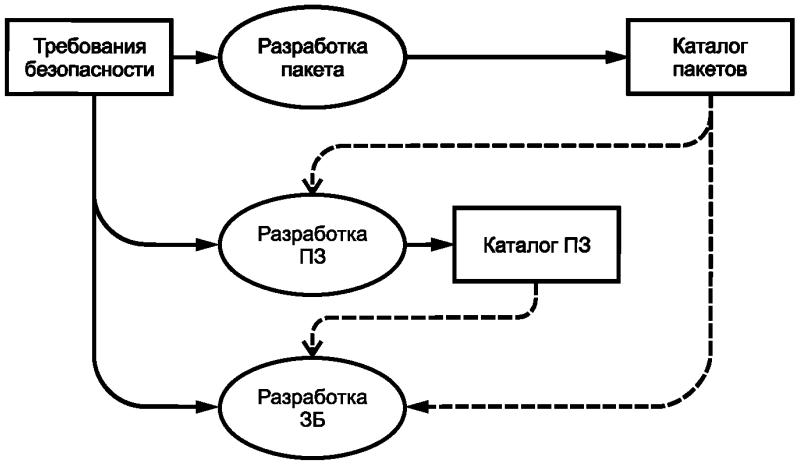


Рисунок 8 — Взаимосвязь между конструкциями требований безопасности

5.4.1.4.1 Пакет

Промежуточная комбинация компонентов называется пакетом. Пакет позволяет выразить совокупность функциональных требований или требований доверия, отвечающих идентифицируемому подмножеству целей безопасности. Пакет предназначен для многократного использования и определяет требования, известные как полезные и эффективные для достижения установленных целей. Допускается применение пакета при создании более крупных пакетов, профилей защиты и заданий по безопасности.

Оценочные уровни доверия — это предопределенные пакеты требований доверия, содержащиеся в ИСО/МЭК 15408-3. ОУД является базовым набором требований доверия для оценки. Каждый ОУД устанавливает непротиворечивый набор требований доверия. Совместно оценочные уровни доверия

образуют упорядоченное множество, которое является предопределенной в ИСО/МЭК 15408 шкалой доверия.

5.4.1.4.2 Профиль защиты

ПЗ содержит совокупность требований безопасности, взятых из ИСО/МЭК 15408 или сформулированных в явном виде, в которую следует включать ОУД (возможно усиленный дополнительными компонентами доверия). ПЗ позволяет выразить независимые от конкретной реализации требования безопасности для некоторой совокупности ОО, полностью согласованные с набором целей безопасности. ПЗ предназначен для многократного использования и определения как функциональных требований, так и требований доверия к ОО, которые полезны и эффективны для достижения установленных в ПЗ целей безопасности. ПЗ также содержит обоснование требований и целей безопасности.

Допускается разработка ПЗ сообществами потребителей, разработчиками продуктов ИТ или другими сторонами, заинтересованными в определении такой общей совокупности требований. ПЗ предоставляет потребителям средство ссылки на определенную совокупность потребностей в безопасности и облегчает будущую оценку в соответствии с этими потребностями.

5.4.1.4.3 Задание по безопасности

ЗБ содержит совокупность требований безопасности, которые могут быть определены ссылками на ПЗ, непосредственно на функциональные компоненты или компоненты доверия из ИСО/МЭК 15408 или сформулированы в явном виде. ЗБ позволяет выразить для конкретного ОО требования безопасности, которые по результатам оценки ЗБ признаны полезными и эффективными для достижения установленных в ЗБ целей безопасности.

ЗБ содержит краткую спецификацию ОО совместно с требованиями и целями безопасности и соответствующим обоснованием. ЗБ является основой для соглашения между всеми сторонами относительно того, какую безопасность предлагает ОО.

5.4.1.5 Источники требований безопасности

Требования безопасности ОО могут быть скомпонованы с использованием следующих источников:

a) существующих ПЗ: требования безопасности ОО в ЗБ могут быть адекватно выражены непосредственно через требования, содержащиеся в существующем ПЗ, или предполагать согласование с ними. Существующие ПЗ можно использовать как основу для создания нового ПЗ;

b) существующих пакетов: часть требований безопасности ОО для ПЗ или ЗБ может быть уже выражена в пакете, который может быть использован.

Совокупностью предопределенных пакетов являются ОУД, определенные в ИСО/МЭК 15408-3. Требования доверия к ОО, входящие в ПЗ или ЗБ, должны включать в себя какой-либо ОУД из ИСО/МЭК 15408-3;

c) существующих компонентов функциональных требований или требований доверия: функциональные требования или требования доверия в ПЗ или ЗБ могут быть выражены непосредственно через компоненты, приведенные в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3;

d) расширенных требований: в ПЗ или ЗБ могут быть использованы дополнительные функциональные требования, не содержащиеся в ИСО/МЭК 15408-2, и/или дополнительные требования доверия, не содержащиеся в ИСО/МЭК 15408-3.

Требования из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 следует использовать всюду, где это допустимо. Использование существующего ПЗ обеспечивает выполнение объектом оценки апробированной совокупности требований известной полезности и, как следствие, более широкое признание ОО.

5.4.2 Виды оценок

5.4.2.1 Оценка ПЗ

Оценку ПЗ проводят по критериям оценки ПЗ, содержащимся в ИСО/МЭК 15408-3. Целью такой оценки является продемонстрировать, что профиль защиты является полным, непротиворечивым, технически правильным и пригодным для использования при изложении требований к ОО, предполагаемому для оценки.

5.4.2.2 Оценка ЗБ

Оценку ЗБ для ОО проводят по критериям оценки ЗБ, содержащимся в ИСО/МЭК 15408-3. Такая оценка преследует две цели: во-первых, продемонстрировать, что ЗБ является полным, непротиворечивым, технически правильным и, следовательно, пригодным для использования в качестве основы для оценки соответствующего ОО; во-вторых, в случае, если в ЗБ имеется утверждение о соответствии какому-либо ПЗ, — продемонстрировать, что ЗБ должным образом отвечает требованиям данного ПЗ.

5.4.2.3 Оценка ОО

Оценку ОО проводят по критериям оценки, содержащимся в ИСО/МЭК 15408-3, с использованием в качестве основы в основном завершенного ЗБ. В основном завершенное ЗБ снижает риск проблем в

процессе оценки, в нем все разделы должны быть завершены до приемлемой для системы оценки степени и по отношению к нему не предвидится серьезных трудностей, связанных с оценкой. Результаты оценки ОО должны продемонстрировать, что ОО отвечает требованиям безопасности, содержащимся в оцененном ЗБ.

6 Требования ИСО/МЭК 15408 и результаты оценки

6.1 Введение

В настоящем разделе представлены ожидаемые результаты оценки ПЗ и ОО. Оценки профилей защиты или объектов оценки позволяют создавать каталоги ПЗ или ОО, прошедших оценку. Оценка ЗБ дает промежуточные результаты, которые затем используют при оценке ОО.

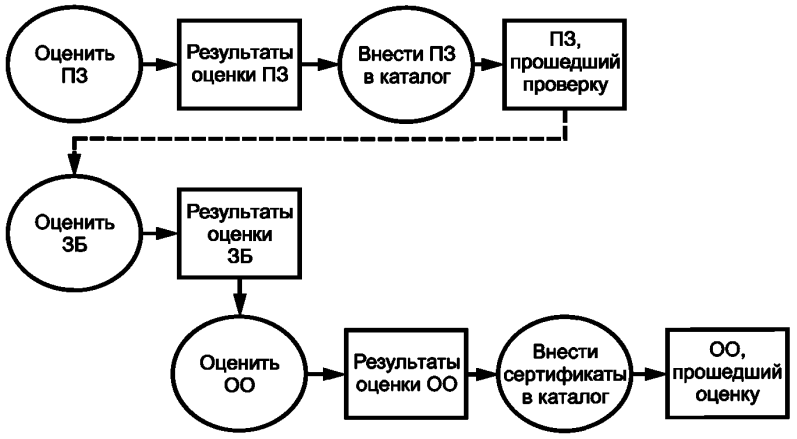


Рисунок 9 — Результаты оценки

Необходимо, чтобы оценка ПЗ и ОО приводила к объективным и повторяемым результатам, на которые затем можно ссылаться как на свидетельство даже при отсутствии 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. Практическое применение критериев включает в себя как объективные, так и субъективные элементы оценки, поэтому получение абсолютно точных и универсальных рейтингов безопасности ИТ невозможно.

Рейтинг, полученный в соответствии с ИСО/МЭК 15408, представляет итоговые данные специфического типа исследования характеристик безопасности ОО. Такой рейтинг 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 также выводы оценки.

6.2 Требования, включаемые в профиль защиты и задание по безопасности

В ИСО/МЭК 15408 определена совокупность критериев безопасности ИТ, которая может отвечать потребностям многих сообществ потребителей. ИСО/МЭК 15408 разработан, исходя из принципа, что для формирования требований к ОО в виде профилей защиты и заданий по безопасности предпочтительно использование функциональных компонентов безопасности из ИСО/МЭК 15408-2, ОУД и компонентов доверия из ИСО/МЭК 15408-3, поскольку они представляют хорошо известную и понятную сферу применения.

В ИСО/МЭК 15408 допускается возможность того, что при формировании полного набора требований к безопасности ИТ могут понадобиться функциональные требования и требования доверия, не включенные в соответствующие каталоги. Для включения таких расширенных требований в ПЗ или ЗБ должны быть выполнены следующие условия:

а) любые расширенные функциональные требования или требования доверия, включенные в ПЗ или ЗБ, должны быть четко и недвусмысленно сформулированы и выражены так, чтобы была возможна

оценка и демонстрация соответствия ОО этим требованиям. В качестве образца должны использоваться уровень детализации и способ выражения существующих функциональных компонентов и компонентов доверия из ИСО/МЭК 15408;

b) результаты оценки, полученные с использованием расширенных функциональных требований и требований доверия, должны содержать соответствующие пояснения;

c) включение, при необходимости, в состав ПЗ или ЗБ расширенных функциональных требований или требований доверия должно соответствовать требованиям классов APE или ASE из ИСО/МЭК 15408-3.

6.2.1 Результаты оценки ПЗ

ИСО/МЭК 15408 содержит критерии оценки, позволяющие оценщику установить, является ли ПЗ полным, непротиворечивым, технически правильным и, следовательно, пригодным для изложения требований к потенциально оцениваемому ОО.

Результат оценки ПЗ должен быть сформулирован как «соответствие/несоответствие». ПЗ, для которого оценка заканчивается положительно, должен получить право включения в реестр.

6.3 Требования к объекту оценки

ИСО/МЭК 15408 содержит критерии оценки, позволяющие оценщику решать, соответствует ли ОО требованиям безопасности, выраженным в ЗБ. Применяя ИСО/МЭК 15408 при оценке ОО, оценщик может прийти к следующим выводам:

a) отвечают ли специфицированные функции безопасности ОО функциональным требованиям и, следовательно, эффективны ли они для достижения целей безопасности ОО;

b) правильно ли реализованы специфицированные функции безопасности ОО.

Требования безопасности, содержащиеся в ИСО/МЭК 15408, определяют хорошо отработанную сферу применения критериев оценки безопасности ИТ. ОО, для которого требования безопасности выражены только в терминах функциональных требований и требований доверия из ИСО/МЭК 15408, может быть оценен по ИСО/МЭК 15408. Использование пакетов требований доверия, не содержащих ОУД, должно быть логически обосновано.

Может возникнуть потребность, чтобы какой-либо ОО отвечал требованиям безопасности, непосредственно не выраженным в ИСО/МЭК 15408. В ИСО/МЭК 15408 признается необходимость оценки подобных ОО, но, поскольку дополнительные требования лежат вне известной сферы применения ИСО/МЭК 15408, результаты такой оценки должны сопровождаться соответствующим пояснением. Для подобных ОО может быть поставлено под угрозу признание результатов оценки заинтересованными органами оценки.

Результаты оценки ОО должны включать в себя утверждение о соответствии ИСО/МЭК 15408. Описание безопасности ОО в терминах ИСО/МЭК 15408 дает возможность сравнения характеристик безопасности различных ОО.

6.3.1 Результаты оценки ОО

В результате оценки ОО должна быть установлена степень доверия тому, что ОО соответствует требованиям.

Результат оценки ОО должен быть сформулирован как «соответствие/несоответствие». ОО, для которого оценка заканчивается положительно, должен получить право включения в реестр. Результаты оценки должны также включать в себя «Результаты оценки соответствия».

6.4 Результаты оценки соответствия

Результаты оценки соответствия указывают на источник совокупности требований, которым удовлетворяет ОО или ПЗ, проходящие оценку. Результаты оценки соответствия представляют путем соотнесения с ИСО/МЭК 15408-2 (функциональные требования) ИСО/МЭК 15408-3 (требования доверия) и, если применимо, с предопределенным набором требований (например ОУД, профиль защиты).

Результаты оценки соответствия должны включать в себя один из следующих вариантов:

a) «соответствие ИСО/МЭК 15408-2» — ПЗ или ОО соответствует ИСО/МЭК 15408-2, если функциональные требования основаны только на функциональных компонентах из ИСО/МЭК 15408-2;

b) «расширение ИСО/МЭК 15408-2» — ПЗ или ОО является расширенным по отношению к ИСО/МЭК 15408-2, если функциональные требования включают в себя функциональные компоненты, не содержащиеся в ИСО/МЭК 15408-2;

а также одно из следующего:

a) «соответствие ИСО/МЭК 15408-3» — ПЗ или ОО соответствует ИСО/МЭК 15408-3, если требования доверия основаны только на компонентах доверия из ИСО/МЭК 15408-3;

b) «расширение ИСО/МЭК 15408-3» — ПЗ или ОО является расширенным по отношению к ИСО/МЭК 15408-3, если требования доверия включают требования доверия не из ИСО/МЭК 15408-3.

Кроме того, результат оценки соответствия может включать в себя утверждение, сделанное относительно набора определенных требований; в данном случае результат оценки соответствия включает в себя одно из следующего:

a) «соответствие именованному пакету» — ПЗ или ОО соответствует предопределенному именованному функциональному пакету и/или пакету доверия (например ОУД), если требования (функциональные или доверия) включают в себя все компоненты, перечисленные в пакете, как часть результата оценки соответствия;

b) «усиление именованного пакета» — ПЗ или ОО является усилением предопределенного именованного функционального пакета и/или пакета доверия (например ОУД), если требования (функциональные или доверия) являются надлежащим надмножеством всех компонентов, перечисленных в пакете, как часть результата оценки соответствия.

Результат оценки соответствия может также включать в себя утверждение, сделанное относительно профилей защиты; в данном случае результат оценки соответствия включает в себя следующее:

a) «соответствие ПЗ» — ОО удовлетворяет конкретному ПЗ (профилям защиты), который(ые) перечислен(ы) как часть результата оценки соответствия.

6.5 Использование результатов оценки объекта оценки

Продукты и системы ИТ отличаются в отношении использования результатов оценки. Различное использование результатов оценки показано на рисунке 10. Продукты ИТ можно оценивать и каталогизировать последовательно на все более высоких уровнях агрегатирования вплоть до уровня эксплуатируемых систем, когда продукты могут подлежать оценке в связи с аттестацией системы.

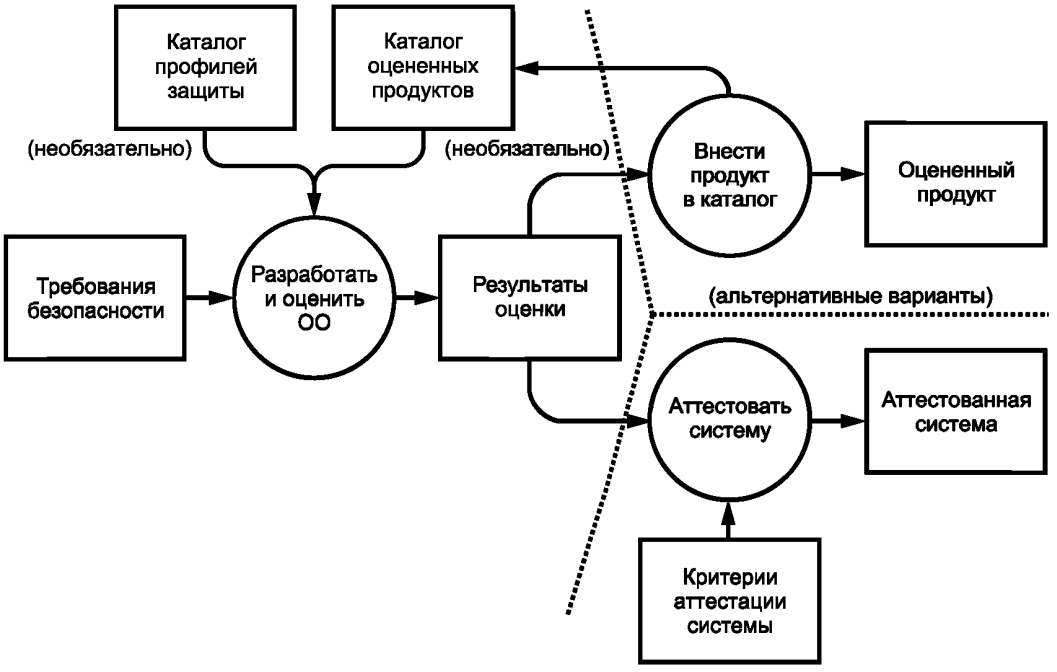


Рисунок 10 — Использование результатов оценки ОО

ОО разрабатывают в соответствии с требованиями, в которых могут быть приняты во внимание характеристики безопасности любых ранее оцененных продуктов, входящих в его состав, и профилей защиты, на которые даются ссылки. Последующая оценка ОО приводит к получению совокупности результатов оценки, документирующих данные, полученные при оценке.

После оценки продукта ИТ, предназначенного для широкого использования, краткое заключение с данными оценки помещают в каталог оцененных продуктов, чтобы оно было доступно широкому кругу потребителей, нуждающихся в безопасных продуктах ИТ.

Если ОО включен или будет включен в состав установленной системы ИТ, подвергаемой оценке, результаты его оценки предоставляют аттестующему систему. Результаты оценки ОО, проведенной в соответствии с ИСО/МЭК 15408, могут быть учтены аттестующим систему ИТ при применении принятых в конкретной организации критериев аттестации, требующих оценки по ИСО/МЭК 15408. Результаты оценки по ИСО/МЭК 15408 являются частью исходных данных для процесса аттестации, ведущего к принятию решения о приемлемости риска эксплуатации системы.

Приложение А
(обязательное)

Спецификация профилей защиты

А.1 Краткий обзор

ПЗ определяет независимую от конкретной реализации совокупность требований ИТ для некоторой категории ОО. Такие ОО предназначены для удовлетворения общих запросов потребителей в безопасности ИТ. Поэтому потребители могут выразить свои запросы в безопасности ИТ, используя существующий или формируя новый ПЗ, без ссылки на какой-либо конкретный ОО.

Настоящее приложение содержит требования к ПЗ в повествовательной форме. В классе доверия APE, в ИСО/МЭК 15408-3, раздел 8, данные требования приведены в форме компонентов доверия, которые следует использовать при оценке ПЗ.

А.2 Содержание профиля защиты

А.2.1 Содержание и представление

ПЗ должен соответствовать требованиям к содержанию, изложенным в настоящем приложении. ПЗ следует представлять в виде ориентированного на пользователя документа, содержащего минимум ссылок на другие материалы, которые могут быть недоступны пользователю данного ПЗ. Обоснование допускается оформлять отдельно.

Содержание ПЗ представлено на рисунке А.1, который следует использовать при создании структурной схемы документа «Профиль защиты».

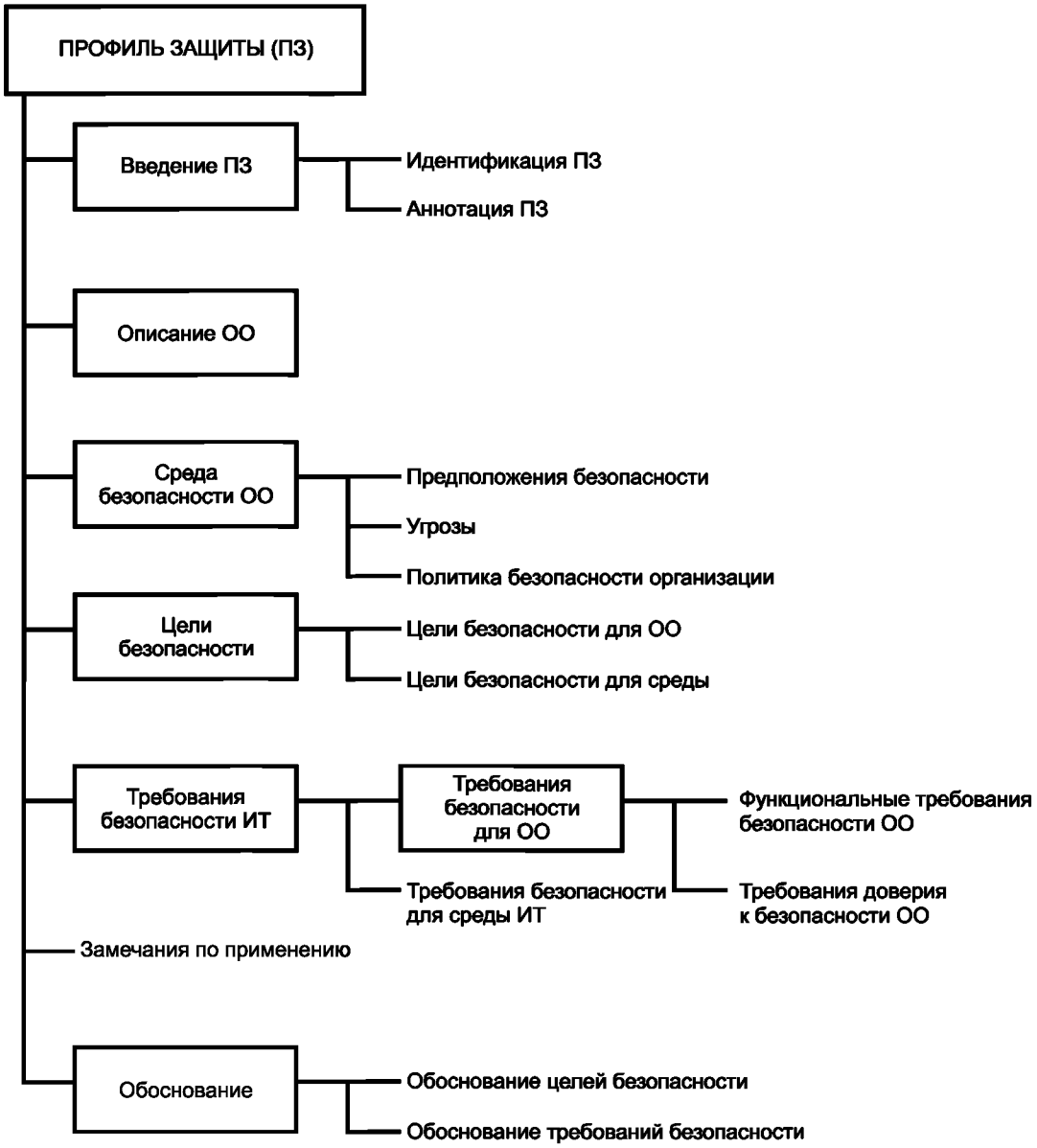


Рисунок А.1 — Содержание профиля защиты

А.2.2 Введение ПЗ

Введение ПЗ должно содержать следующую информацию для управления документооборотом и обзорную информацию, необходимую для работы с реестром ПЗ:

a) идентификация ПЗ — должна обеспечивать маркировку и описательную информацию, необходимые для идентификации, каталогизации, регистрации ПЗ и ссылки на него;

b) аннотация ПЗ — должна давать общую характеристику ПЗ в повествовательной форме. Аннотация должна быть достаточно подробной, чтобы потенциальный пользователь ПЗ мог решить, представляет ли ПЗ для него интерес. Аннотация должна быть также пригодна для размещения в виде самостоятельного реферата в каталогах и реестрах ПЗ.

А.2.3 Описание ОО

Данная часть ПЗ должна содержать описание ОО, служащее цели лучшего понимания требований его безопасности и дающее представление о типе продукта и основных характерных особенностях ИТ применительно к ОО.

Описание ОО предоставляет контекст для оценки. Информацию, содержащуюся в описании ОО, используют в процессе оценки для выявления противоречий. Поскольку ПЗ обычно не ссылается на конкретную реализацию, то характерные особенности ОО могут быть представлены в виде предположений. Если ОО является продуктом или системой, основной функцией которых является безопасность, то данная часть ПЗ может быть использована для более подробного описания возможностей применения ОО.

А.2.4 Среда безопасности ОО

Изложение среды безопасности ОО должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО, и ожидаемый способ его применения. Данное изложение должно включать в себя:

a) описание предположений, содержащее аспекты безопасности среды, в которой ОО будет использован или предполагается к использованию, а также содержать:

1) информацию о предполагаемом использовании ОО, включая такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования ОО,

2) информацию относительно среды применения ОО, включая аспекты физического окружения, персонала и внешних связей;

b) описание угроз, содержащее угрозы активам, против которых требуется защита средствами ОО или его среды. В описании предположений необходимо приводить не все угрозы, которые могут встретиться в среде, а только влияющие на безопасную эксплуатацию ОО.

Угроза должна быть описана с использованием понятий идентифицированного нарушителя, нападения и актива, который подвергается нападению. Нарушителя следует описывать через такие аспекты, как компетентность, доступные ресурсы и мотивация. Нападение следует описывать через такие аспекты, как возможность, метод нападения и используемые уязвимости.

Если цели безопасности ОО следуют только из политики безопасности организации и предположений, то описание угроз может быть опущено;

c) описание политики безопасности организации, идентифицирующее и, при необходимости, объясняющее все положения политики безопасности организации или правила, которым должен следовать объект оценки. Для представления любого положения политики, позволяющего использовать его для установления четких целей безопасности, могут понадобиться объяснения и интерпретации.

Если цели безопасности следуют только из угроз и предположений безопасности, описание политики безопасности организации может быть опущено.

Для физически распределенного ОО может быть необходимо рассмотреть аспекты среды безопасности (предположения, угрозы, политику безопасности организации) отдельно для каждой из различных областей среды ОО.

А.2.5 Цели безопасности

Изложение целей безопасности должно определять цели безопасности как для ОО, так и для его среды. Цели безопасности должны учитывать все установленные аспекты среды безопасности. Цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации. Угрозе может быть противопоставлена одна или более целей для ОО, одна или более целей для среды или их сочетание. Должны быть также идентифицированы категории целей безопасности, приведенные ниже. Если противостояние угрозе или проведение политики безопасности возлагается частично на ОО, а частично на его среду, соответствующая цель безопасности должна повторяться в каждой категории:

a) цели безопасности для ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО, и/или с политикой безопасности организации, которой должен удовлетворять ОО;

b) цели безопасности для среды ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противостоит ОО, и/или с политикой безопасности организации и предположениями, не полностью удовлетворяемыми ОО.

Цели безопасности для среды могут частично или полностью повторять некоторые предположения, сделанные при изложении среды безопасности ОО.

А.2.6 Требования безопасности ИТ

В данной части ПЗ подробно определяются требования безопасности ИТ, которые должны удовлетворяться ОО или его средой. Требования безопасности ОО должны быть изложены следующим образом:

a) если необходимо охватить различные аспекты одного и того же требования (например, при идентификации более чем одного типа пользователя), то допускается повторное использование (то есть применение операции итерации) одного и того же компонента из ИСО/МЭК 15408-2 с тем, чтобы охватить каждый аспект. При изложении требований безопасности ОО должны быть определены функциональные требования и требования доверия, которым должны удовлетворять ОО, и свидетельства поддержки его оценки для достижения целей безопасности ОО. Требования безопасности ОО должны быть изложены следующим образом:

1) При изложении функциональных требований безопасности ОО следует определять функциональные требования к ОО, где это возможно, в виде функциональных компонентов из ИСО/МЭК 15408-2.

Если требования доверия к ОО включают в себя компонент AVA_SOF.1 (например ОУД2 и выше), то при изложении функциональных требований безопасности ОО должен быть установлен минимальный уровень стойкости функций безопасности, реализуемых с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Все подобные функции должны соответствовать этому минимальному уровню. Уровень должен быть одним из следующих: базовая СФБ, средняя СФБ и высокая СФБ. Уровень должен выбираться в соот-

ветствии с установленными целями безопасности ОО. Для достижения некоторых целей безопасности ОО могут быть определены специальные метрики стойкости функций для выбранных функциональных требований.

В качестве составной части оценки стойкости функций безопасности ОО (AVA_SOF.1) оценивают и утверждения о стойкости, сделанные для отдельных функций безопасности ОО, и минимальный уровень стойкости для ОО в целом,

2) при изложении требований доверия к безопасности ОО следует определять их как один из ОУД, возможно, усиленный другими компонентами доверия из ИСО/МЭК 15408-3. Расширение ОУД в ПЗ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в ИСО/МЭК 15408-3;

b) необязательное изложение требований безопасности для среды ИТ должно определять требования безопасности ИТ, которым должна соответствовать среда ИТ данного ОО. Требования для данной части ПЗ могут быть взяты из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3, и в этом случае должна быть изменена их формулировка с тем, чтобы четко показать, что данному требованию должна отвечать среда ИТ, а не ОО. Подобное изменение формулировки является особым случаем уточнения и не является предметом требований оценки, связанных с модифицированными компонентами ИСО/МЭК 15408. Если безопасность ОО не зависит от среды ИТ, то данная часть ПЗ может быть опущена;

c) перечисленные ниже общие условия в равной степени относятся к выражению функциональных требований и требований доверия как для ОО, так и для его среды ИТ:

1) если применимо, все требования безопасности ИТ следует устанавливать ссылкой на компоненты требований безопасности из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3. Если при формировании всех либо части требований не применимы компоненты из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, то в ПЗ допускается сформулировать необходимые требования безопасности явным образом, без ссылки на ИСО/МЭК 15408,

2) любые функциональные требования и требования доверия к ОО, сформулированные явным образом, должны быть четко и однозначно выражены с тем, чтобы были возможны оценка и демонстрация соответствия данным требованиям. Уровень детализации и способ выражения функциональных требований и требований доверия, принятый в ИСО/МЭК 15408, должны использоваться как образец,

3) если выбраны компоненты требований, в которых специфицированы требуемые операции (назначение, выбор), то данные операции должны использоваться в ПЗ для конкретизации требований до уровня детализации, необходимого для демонстрации достижения целей безопасности. Все разрешенные операции, которые не исполнены в ПЗ, должны быть отмечены как незавершенные,

4) при изложении требований безопасности ОО допускается, при необходимости, дополнительно разрешать или запрещать использование определенных механизмов безопасности, применяя разрешенные операции над компонентами требований,

5) все зависимости между требованиями безопасности ИТ должны быть удовлетворены. Зависимости могут быть удовлетворены включением необходимых требований в состав требований безопасности ОО или требований к среде.

А.2.7 Замечания по применению

Данная часть ПЗ не является обязательной и может содержать дополнительную информацию, которая считается необходимой или полезной для создания, оценки и использования ОО.

А.2.8 Обоснование

В данной части ПЗ представляется свидетельство, используемое при оценке ПЗ. Данное свидетельство поддерживает утверждения, что ПЗ является полной и взаимосвязанной совокупностью требований и соответствующий ему ОО обеспечит эффективный набор контрмер безопасности ИТ в определенной среде безопасности. Обоснование должно включать в себя:

a) обоснование целей безопасности, демонстрирующее, что изложенные цели безопасности сопоставлены со всеми идентифицированными аспектами среды безопасности ОО и пригодны для их охвата;

b) обоснование требований безопасности, демонстрирующее, что совокупность требований безопасности (ОО и его среды) пригодна для достижения целей безопасности и сопоставлена с ними. Должно быть продемонстрировано, что:

1) сочетание отдельных компонентов функциональных требований и требований доверия для ОО и его среды ИТ в совокупности соответствует изложенным целям безопасности,

2) данный набор требований безопасности образует единое и внутренне непротиворечивое целое,

3) выбор требований безопасности логически обоснован. Должны быть логически обоснованы:

- выбор требований, не содержащихся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3;
- выбор требований доверия, не включенных в какой-либо ОУД;
- случаи неудовлетворения зависимостей,

4) выбранный для ПЗ уровень стойкости функций и заявленная в явном виде стойкость функций согласуются с целями безопасности ОО.

Данный потенциально объемный материал допускается распространять отдельно, поскольку он необходим или полезен не для всех пользователей ПЗ.

Приложение В
(обязательное)

Спецификация заданий по безопасности

В.1 Краткий обзор

ЗБ содержит требования безопасности ИТ для конкретного ОО и специфицирует функции безопасности и меры доверия, предлагаемые объектом оценки для удовлетворения установленных требований.

ЗБ для ОО является основой соглашения между разработчиками, оценщиками и, где необходимо, потребителями по характеристикам безопасности ОО и области применения оценки. Круг лиц, заинтересованных в ЗБ, не ограничивается только лицами, ответственными за разработку ОО и его оценку, но может включать в себя также лиц, ответственных за управление, маркетинг, продажу, инсталляцию, конфигурирование, функционирование и использование ОО.

В ЗБ разрешено включать требования одного или нескольких ПЗ или утверждать о соответствии им. Влияние утверждения о соответствии ПЗ на содержание ЗБ рассматривается в В.2.8.

Настоящее приложение содержит требования к ЗБ в повествовательной форме. В классе доверия ASE, в ИСО/МЭК 15408-3, раздел 9, эти требования приведены в форме компонентов доверия, которые следует использовать при оценке ЗБ.

В.2 Содержание задания по безопасности

В.2.1 Содержание и представление

ЗБ должно соответствовать требованиям к содержанию, изложенным в настоящем приложении. ЗБ следует представлять в виде ориентированного на пользователя документа, содержащего минимум ссылок на другие материалы, которые могут быть недоступны пользователю данного ЗБ. Обоснование допускается оформлять отдельно.

Содержание ЗБ представлено на рисунке В.1, который следует использовать при создании структурной схемы ЗБ.

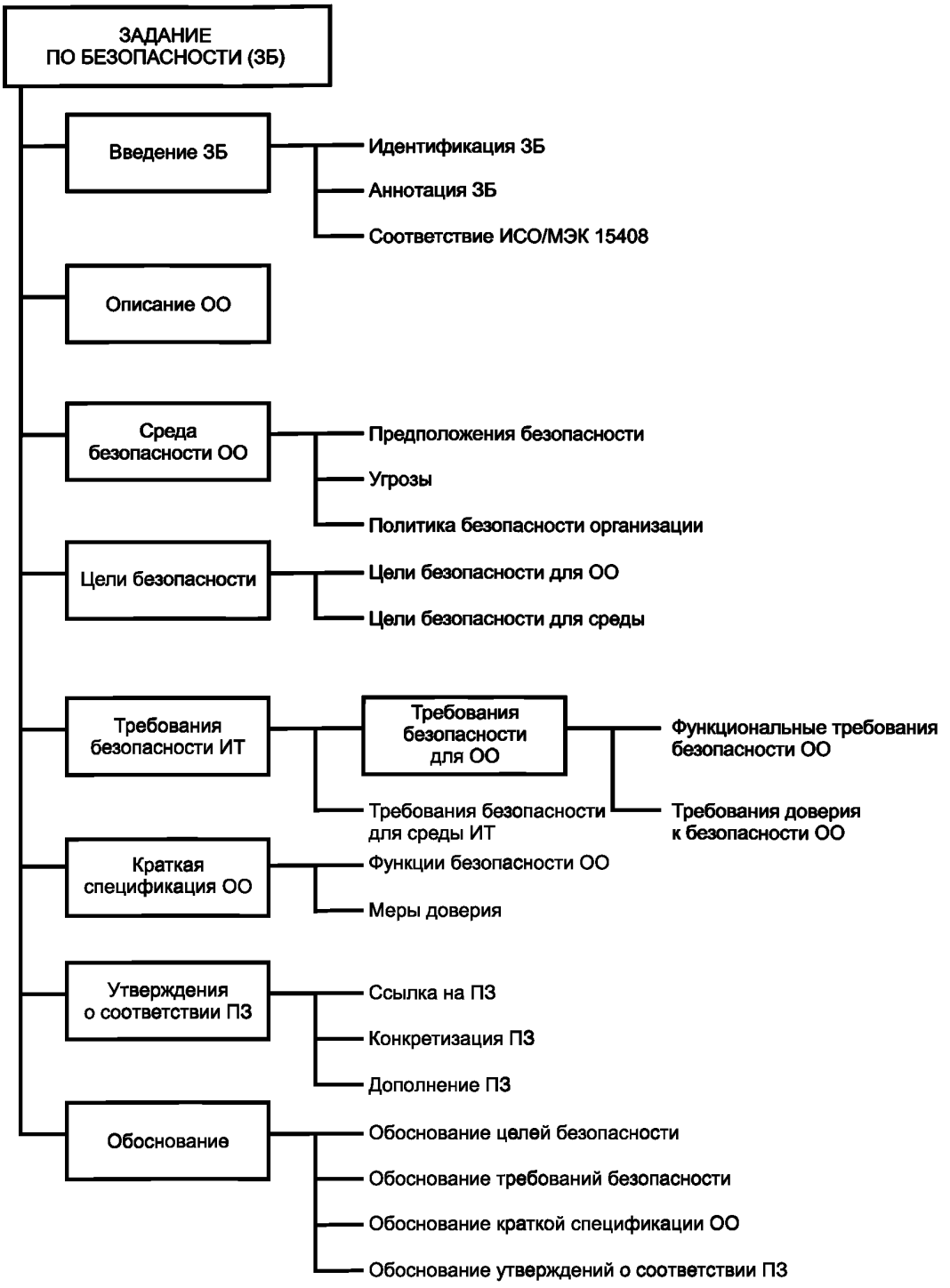


Рисунок В.1 — Содержание задания по безопасности

В.2.2 Введение ЗБ

Введение ЗБ должно содержать следующую информацию для управления документооборотом и обзорную информацию:

а) идентификация ЗБ должна обеспечивать маркировку и описательную информацию, необходимые, чтобы контролировать и идентифицировать ЗБ и ОО, к которому оно относится;

b) аннотация ЗБ должна давать общую характеристику ЗБ в повествовательной форме. Аннотация должна быть достаточно подробной, чтобы потенциальный потребитель ОО мог решить, представляет ли ОО для него интерес. Аннотация должна быть также пригодна для размещения в виде самостоятельного реферата в перечнях оцененных продуктов;

c) утверждение о соответствии ИСО/МЭК 15408 должно содержать каждое поддающееся оценке утверждение о соответствии ОО ИСО/МЭК 15408, как указано в подразделе 6.4.

В.2.3 Описание ОО

Данная часть ЗБ должна содержать описание ОО, служащее цели лучшего понимания требований его безопасности и дающее представление о типе продукта или системы. Область и ограничения применения ОО должны быть описаны в общих терминах как в отношении физической организации ОО (аппаратные и/или программные компоненты/модули), так и логической его организации (характерные возможности ИТ и безопасности, предлагаемые объектом оценки).

Описание ОО предоставляет контекст для оценки. Информацию, содержащуюся в описании ОО, используют в процессе оценки для выявления противоречий. Если ОО является продуктом или системой, основной функцией которых является безопасность, то данная часть ЗБ может быть использована для более подробного описания возможностей применения ОО.

В.2.4 Среда безопасности ОО

Изложение среды безопасности ОО должно содержать описание аспектов безопасности среды, в которой предполагается использовать ОО, и ожидаемый способ его применения. Данное изложение должно включать в себя:

a) описание предположений, содержащее аспекты безопасности среды, в которой ОО будет использоваться или предполагается к использованию, а также содержать:

1) информацию о предполагаемом использования ОО, включая такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования ОО,

2) информацию относительно среды применения ОО, включая аспекты физического окружения, персонала и внешних связей;

b) описание угроз, содержащее угрозы активам, против которых требуется защита средствами ОО или его среды. В описании предположений необходимо приводить не все угрозы, которые могут встретиться в среде, а только влияющие на безопасную эксплуатацию ОО.

Угроза должна быть описана с использованием понятий идентифицированного нарушителя, нападения и актива, который подвергается нападению. Нарушителя следует описывать через такие аспекты, как компетентность, доступные ресурсы и мотивация. Нападение следует описывать через такие аспекты, как возможность, метод нападения и используемые уязвимости.

Если цели безопасности ОО следуют только из политики безопасности организации и предположений, то описание угроз может быть опущено;

c) описание политики безопасности организации, идентифицирующее и, при необходимости, объясняющее все положения политики безопасности организации или правила, которым должен следовать объект оценки. Для представления любого положения политики, позволяющего использовать его для установления четких целей безопасности, могут понадобиться объяснения и интерпретации.

Если цели безопасности следуют только из угроз и предположений безопасности, описание политики безопасности организации может быть опущено.

Для физически распределенного ОО может быть необходимо рассмотреть аспекты среды безопасности (предположения, угрозы, политику безопасности организации) отдельно для каждой из различных областей среды ОО.

В.2.5 Цели безопасности

Изложение целей безопасности должно определять цели безопасности как для ОО, так и для его среды. Цели безопасности должны учитывать все установленные аспекты среды безопасности. Цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации. Угрозе может быть противопоставлена одна или более целей для ОО, одна или более целей для среды или их сочетание. Должны быть также идентифицированы категории целей безопасности, приведенные ниже. Если при этом противостояние угрозе или проведение политики безопасности частично возлагается не на ОО, а на его среду, соответствующая цель безопасности должна повторяться в каждой категории:

a) цели безопасности для ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым необходимо противостоять средствами ОО, и/или с политикой безопасности организации, которой должен удовлетворять ОО;

b) цели безопасности для среды ОО должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противостоит ОО, и/или с политикой безопасности организации и предположениями, не полностью удовлетворяемыми ОО.

Цели безопасности для среды могут частично или полностью повторять некоторые предположения, сделанные при изложении среды безопасности ОО.

В.2.6 Требования безопасности ИТ

В данной части ЗБ подробно определяются требования безопасности ИТ, которые должны удовлетворяться ОО или его средой. Требования безопасности ОО должны быть изложены следующим образом:

a) если необходимо охватить различные аспекты одного и того же требования (например, при идентификации более чем одного типа пользователя), то допускается повторное использование (то есть применение операции итерации) одного и того же компонента из ИСО/МЭК 15408-2 с тем, чтобы охватить каждый аспект. При изложении требований безопасности ОО должны быть определены функциональные требования и требования доверия, которым должны удовлетворять ОО и свидетельства поддержки его оценки для достижения целей безопасности ОО. Требования безопасности ОО должны быть изложены следующим образом:

1) При изложении функциональных требований безопасности ОО следует определять функциональные требования к ОО, где это возможно, в виде функциональных компонентов из ИСО/МЭК 15408-2.

Если требования доверия к ОО включают в себя компонент AVA_SOF.1 (например ОУД2 и выше), то при изложении функциональных требований безопасности ОО должен быть установлен минимальный уровень стойкости функций безопасности, реализуемых с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Все подобные функции должны соответствовать этому минимальному уровню. Уровень должен быть одним из следующих: базовая СФБ, средняя СФБ и высокая СФБ. Уровень должен выбираться в соответствии с установленными целями безопасности ОО. Для достижения некоторых целей безопасности ОО могут быть определены специальные метрики стойкости функций для выбранных функциональных требований.

В качестве составной части оценки стойкости функций безопасности ОО (AVA_SOF.1) оценивают и утверждения стойкости, сделанные для отдельных функций безопасности ОО, и минимальный уровень стойкости для ОО в целом,

2) при изложении требований доверия к безопасности ОО следует определять их как один из ОУД, возможно, усиленный другими компонентами доверия из ИСО/МЭК 15408-3. Расширение ОУД в ЗБ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в ИСО/МЭК 15408-3;

b) необязательное изложение требований безопасности для среды ИТ должно определять требования безопасности ИТ, которым должна соответствовать среда ИТ данного ОО. Требования для данной части ПЗ могут быть взяты из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 и в этом случае должна быть изменена их формулировка с тем, чтобы четко показать, что данному требованию должна отвечать среда ИТ, а не ОО. Подобное изменение формулировки является особым случаем уточнения и не является предметом требований оценки, связанных с модифицированными компонентами ИСО/МЭК 15408. Если безопасность ОО не зависит от среды ИТ, то данная часть ЗБ может быть опущена;

c) перечисленные ниже общие условия в равной степени относятся к выражению функциональных требований и требований доверия как для ОО, так и для его среды ИТ:

1) если применимо, все требования безопасности ИТ следует устанавливать ссылкой на компоненты требований безопасности из ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3. Если при формировании всех либо части требований не применимы компоненты из ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3, то в ЗБ допускается сформулировать необходимые требования безопасности явным образом, без ссылки на ИСО/МЭК 15408,

2) любые функциональные требования и требования доверия к ОО, сформулированные явным образом, должны быть четко и однозначно выражены с тем, чтобы были возможны оценка и демонстрация соответствия данным требованиям. Уровень детализации и способ выражения функциональных требований и требований доверия, принятые в ИСО/МЭК 15408, должны использоваться как образец,

3) любые требуемые операции для раскрытия требований до уровня детализации, необходимого для демонстрации достижения целей безопасности, должны быть использованы. Все специфицированные операции в компонентах требований должны быть завершены,

4) все зависимости между требованиями безопасности ИТ должны быть удовлетворены. Зависимости могут быть удовлетворены включением необходимых требований в состав требований безопасности ОО или требований к среде.

В.2.7 Краткая спецификация ОО

Краткая спецификация ОО должна определить отображение требований безопасности для ОО. Данная спецификация должна предоставить описание функций безопасности и мер доверия к ОО, отвечающих требованиям безопасности ОО. Следует отметить, что информация о функциях безопасности, являющаяся частью краткой спецификации ОО, в некоторых случаях может быть идентична информации, предоставляемой для ОО частью требований семейства ADV_FSP.

Краткая спецификация ОО включает в себя:

a) изложение функций безопасности ОО, которое должно охватывать все функции безопасности ИТ и определять соответствие этих функций функциональным требованиям безопасности ОО. Изложение должно включать в себя сопоставление функций и требований с четким указанием, в удовлетворении каких требований участвует каждая функция, и что все требования удовлетворены. Каждая функция безопасности должна участвовать в удовлетворении, по меньшей мере, одного функционального требования безопасности ОО. При изложении функций безопасности:

1) функции безопасности ИТ должны быть определены неформальным образом на уровне детализации, необходимом для понимания их предназначения,

2) все ссылки на механизмы безопасности, включенные в ЗБ, должны быть сопоставлены с соответствующими функциями безопасности так, чтобы было видно, какие механизмы безопасности используются при реализации каждой функции,

3) если в состав требований доверия к ОО включен компонент AVA_SOF.1, то должны быть идентифицированы все функции безопасности ИТ, реализованные с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Возможность нарушения механизмов таких функций посредством преднамеренного или случайного воздействия имеет непосредственное отношение к безопасности ОО. Должен быть проведен анализ стойкости всех этих функций. Стойкость каждой идентифицированной функции должна быть определена и заявлена как базовая СФБ, средняя СФБ или высокая СФБ либо с применением дополнительно введенной метрики стойкости. Свидетельство, приводимое в отношении стойкости функции безопасности, должно быть достаточным, чтобы позволить оценщикам провести свою независимую оценку и подтвердить, что утверждения о стойкости адекватны и корректны;

b) Изложение мер доверия, которое должно специфицировать меры доверия к ОО, заявленные для удовлетворения изложенных требований доверия. Меры доверия должны быть сопоставлены с требованиями так, чтобы было понятно, какие меры в удовлетворении каких требований участвуют.

Там, где это возможно, меры доверия разрешается определять ссылкой на соответствующие планы обеспечения качества, жизненного цикла или управления.

В.2.8 Утверждения о соответствии ПЗ

ЗБ может содержать утверждения о соответствии требованиям одного или нескольких ПЗ. Для каждого из имеющихся утверждений ЗБ должно включать в себя изложение утверждения о соответствии ПЗ, содержащее объяснение, логическое обоснование и другие вспомогательные материалы, необходимые для подкрепления данного утверждения.

Содержание и представление в ЗБ целей и требований для ОО может зависеть от того, делаются ли для ОО утверждения о соответствии ПЗ. Влияние на содержание ЗБ утверждения о соответствии ПЗ может быть сведено в итоге к одному из следующих вариантов:

a) если утверждений о соответствии ПЗ нет, то приводят полное описание целей и требований безопасности ОО в соответствии с настоящим приложением. При этом данный раздел ЗБ опускается;

b) если ЗБ содержит утверждение о соответствии требованиям какого-либо ПЗ без необходимости их дальнейшего уточнения, то ссылки на ПЗ достаточно для определения и логического обоснования целей и требований безопасности ОО. Повторное изложение содержания ПЗ не является обязательным;

c) если ЗБ содержит утверждение о соответствии требованиям какого-либо ПЗ и требования этого ПЗ нуждаются в дальнейшем уточнении, то в ЗБ должно быть показано, что требования по уточнению ПЗ удовлетворены. Такая ситуация обычно возникает, если ПЗ содержит незавершенные операции. В этом случае в ЗБ допускается ссылка на эти требования, но при этом следует завершить операции в пределах ЗБ. В некоторых случаях, если завершение операций приводит к существенным изменениям, может быть предпочтительным повторно изложить содержание ПЗ в составе ЗБ;

d) если ЗБ содержит утверждение о соответствии требованиям какого-либо ПЗ, но последний расширяется добавлением дополнительных целей и требований, то в ЗБ должны быть определены эти дополнения с учетом того, что ссылки на ПЗ может быть достаточно для определения целей и требований безопасности ПЗ. В случаях, если дополнения к ПЗ существенны, может быть предпочтительным повторно изложить содержание ПЗ в составе ЗБ;

e) вариант, когда в ЗБ утверждается о частичном соответствии ПЗ, неприемлем для оценки по ИСО/МЭК 15408.

ИСО/МЭК 15408 не предписывает выбор ссылки на ПЗ или повторение изложения его целей и требований. Основным является требование, чтобы содержание ЗБ было полным, ясным и однозначным настолько, чтобы оценка ЗБ была возможной, а само ЗБ являлось приемлемой основой для оценки ОО и четко прослеживалось соответствие каждому заявленному ПЗ.

Если сделано утверждение о соответствии какому-либо ПЗ, то изложение утверждений о соответствии должно содержать для каждого ПЗ:

a) ссылку на ПЗ, идентифицирующую ПЗ, соответствие которому утверждается, и любые дополнительные материалы, которые необходимы для данного утверждения. Обоснованное утверждение о соответствии подразумевает, что ОО удовлетворяет всем требованиям ПЗ;

b) конкретизацию ПЗ, идентифицирующую требования безопасности ИТ, в которых выполняются операции, разрешенные в ПЗ, или дополнительно уточняются требования ПЗ;

c) дополнение ПЗ, идентифицирующее цели и требования безопасности ОО, которые дополняют цели и требования ПЗ.

В.2.9 Замечания по применению

Данная часть ЗБ не является обязательной и может содержать дополнительную информацию, которая считается необходимой или полезной для понимания ЗБ. Необходимо отметить, что если ЗБ содержит утверждение о соответствии требованиям ПЗ, то может быть уместным, чтобы определенная информация, содержащаяся в потенциальном подразделе ПЗ «Замечания по применению», была отражена в других подразделах ЗБ. Например, информацию о конструкции ОО более уместно представить в краткой спецификации ОО или в разделе ЗБ «Обоснование», чем в подразделе ЗБ «Замечания по применению». Для упрощения оценки ЗБ замечания по применению,

содержащие необходимый для оценки материал, следует помещать в тот подраздел ЗБ, который предоставляет свидетельство для соответствующего аспекта оценки.

В.2.10 Обоснование

В данной части ЗБ представляется свидетельство, используемое при оценке ЗБ. Данное свидетельство поддерживает утверждения, что ЗБ является полной и взаимосвязанной совокупностью требований и соответствующий ему ОО обеспечит эффективный набор контрмер безопасности ИТ в определенной среде безопасности, а краткая спецификация ОО согласуется с требованиями безопасности. Обоснование также демонстрирует, что все утверждения о соответствии ПЗ справедливы. Обоснование должно включать в себя:

a) обоснование целей безопасности, демонстрирующее, что изложенные цели безопасности сопоставлены со всеми идентифицированными аспектами среды безопасности ОО и пригодны для их охвата;

b) обоснование требований безопасности, демонстрирующее, что совокупность требований безопасности (ОО и его среды) пригодна для достижения целей безопасности и сопоставлена с ними. Должно быть продемонстрировано, что:

1) сочетание отдельных компонентов функциональных требований и требований доверия для ОО и его среды ИТ в совокупности соответствует изложенным целям безопасности,

2) данный набор требований безопасности образует единое и внутренне непротиворечивое целое,

3) выбор требований безопасности логически обоснован. Должны быть логически обоснованы:

- выбор требований, не содержащихся в ИСО/МЭК 15408-2 или ИСО/МЭК 15408-3;
- выбор требований доверия, не включенных в какой-либо ОУД;
- случаи неудовлетворения зависимостей,

4) выбранный для ЗБ уровень стойкости функций и заявленная в явном виде стойкость функций согласуются с целями безопасности ОО;

c) обоснование краткой спецификации ОО, показывающее, что функции безопасности и меры доверия к ОО пригодны для того, чтобы соответствовать требованиям безопасности ОО. Должно быть продемонстрировано, что:

1) сочетание специфицированных для ОО функций безопасности ИТ при совместном использовании удовлетворяет функциональным требованиям безопасности ОО,

2) сделанные утверждения о стойкости функций безопасности ОО либо заявление, что в таких утверждениях нет необходимости, справедливы,

3) утверждение о соответствии изложенных мер доверия требованиям доверия логически обосновано.

Уровень детализации обоснования должен соответствовать уровню детализации определения функций безопасности;

d) обоснование утверждений о соответствии ПЗ, объясняющее любые различия между целями и требованиями безопасности ЗБ и любого ПЗ, соответствие которому утверждается. Данная часть ЗБ может быть опущена, если ЗБ не содержит утверждений о соответствии ПЗ или цели и требования безопасности ЗБ и каждого ПЗ, соответствие которому утверждается, полностью совпадают.

Данный потенциально объемный материал допускается распространять отдельно, поскольку он необходим или полезен не для всех пользователей ЗБ.

Приложение С
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица С.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 15408-1:2005	ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ИСО/МЭК 15408-2:2005	ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ИСО/МЭК 15408-3:2005	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

Библиография

[1] Bell, D. E. and LaPadula, L. J., Secure Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-75-306, MITRE Corporation MTR-2997, Bedford MA, March 1976

[2] Biba, K. J., Integrity Considerations for Secure Computer Systems, ESD-TR-372, ESD/ AFSC, Hanscom AFB, Bedford MA., April 1977

[3] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0, Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993

[4] Federal Criteria for Information Technology Security, Draft Version 1.0 (Volumes I and II), jointly published by the National Institute of Standards and Technology and the National Security Agency, US Government, January 1993

[5] Goguen, J. A. and Meseguer, J., «Security Policies and Security Models», 1982 Symposium on Security and Privacy, pp.11—20, IEEE, April 1982

[6] Goguen, J.A. and Meseguer, J., «Unwinding and Inference Control», 1984 Symposium on Security and Privacy, pp.75—85, IEEE, May 1984

[7] Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 1991

[8] ИСО/МЭК 7498-2:1989 Системы обработки информации. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности

(ISO/IEC 7498-2:1987) (Information processing systems — Open Systems Interconnection — Basic Reference Model, Part 2: Security Architecture)

[9] ИСО/МЭК 15292:2001 Информационная технология. Методы и средства обеспечения безопасности. Процедуры регистрации профилей защиты

(ISO/IEC 15292:2001) (Information technology — Security techniques — Protection Profile registration procedures)

[10] Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985

УДК 351.864.1:004:006.354 ОКС 35.040 Т00

Ключевые слова: информационная технология, задание по безопасности, профиль защиты, объект оценки, критерии оценки безопасности, функция безопасности

Редактор *В.Н. Копысов*
Технический редактор *Н.С. Гришанова*
Корректор *Т.И. Кононенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 18.03.2009. Подписано в печать 25.05.2009. Формат 60 × 84 1/8. Бумага офсетная. Гарнитура Ариал.
Печать офсетная. Усл. печ. л. 4,65. Уч.-изд. л. 4,20. Тираж 328 экз. Зак. 319.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru