Федеральное агентство по техническому регулированию и метрологии

Логотип национального органа по стандартизации

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 15408-1–
(проект, окончательная редакция)

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ч а с т ь 1

Введение и общая модель

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

Настоящий проект стандарта не подлежит применению до его принятия

Москва
2007

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 ООО «Центр безопасности информации», 4ЦНИИ Минобороны России, ФГУП Центр «Атомзащитаинформ», ФГУП «ЦНИИАТОМИНФОРМ» при участии экспертов Международной рабочей группы по Общим критериям

2 ВНЕСЕН ФСТЭК России, техническими комитетами по стандартизации ТК 362 "Защита информации" и ТК 22 "Информационные технологии"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ

4 Настоящий стандарт идентичен международному стандарту ISO/IEC 15408-1:2005

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 национального органа Российской Федерации по стандартизации в сети Интернет

Введение

Международный стандарт ISO/IEC 15408:2005 был подготовлен Совместным техническим комитетом ISO/IEC JTC 1 *«Информационные технологии»*, Подкомитет SC 27 *«Методы и средства обеспечения безопасности ИТ»*. Идентичный ISO/IEC 15408:2005 текст опубликован организациями-спонсорами проекта «Общие критерии» как «Общие критерии оценки безопасности информационных технологий» версии 2.3 (именуемые ОК 2.3).

Вторая редакция стандарта отменяет и заменяет первую редакцию (ISO/IEC 15408:1999), которая подверглась технической переработке.

ГОСТ Р ИСО/МЭК 15408, идентичный ISO/IEC 15408:2005, состоит из следующих частей под общим заголовком «Информационная технология – Методы и средства обеспечения безопасности – Критерии оценки безопасности информационных технологий»:

— Часть 1: Введение и общая модель;

— Часть 2: Функциональные требования безопасности;

— Часть 3: Требования доверия к безопасности.

ГОСТ Р ИСО/МЭК 15408 дает возможность сравнения результатов независимых оценок безопасности. Это достигается предоставлением общего набора требований к функциям безопасности продуктов и систем ИТ и к мерам доверия, применяемых 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.

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

ГОСТ Р ИСО/МЭК 15408 направлен на защиту информации от несанкционированного раскрытия, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью соответственно. ГОСТ Р ИСО/МЭК 15408 может быть также применим к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. ГОСТ Р ИСО/МЭК 15408 сосредоточен на угрозах информации, возникающих в результате действий человека как злоумышленных, так и иных, но возможно также применение ГОСТ Р ИСО/МЭК 15408 и для некоторых угроз, не связанных с человеческим фактором. Кроме того, ГОСТ Р ИСО/МЭК 15408 может быть применим и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

ГОСТ Р 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.

Содержание

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Ч а с т ь 1. Введение и общая модель

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

(IDT)

Дата введения – 200X-XX-XX

1 Область применения

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

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

a) ГОСТ Р ИСО/МЭК 15408 не содержит критериев оценки безопасности, касающихся административных мер безопасности, непосредственно не относящихся к мерам безопасности ИТ. Известно, однако, 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 ГОСТ Р ИСО/МЭК 15408 применимы и в этой области. В частности, рассмотрены некоторые аспекты физической защиты ОО.

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

d) Процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ГОСТ Р 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 на тех аспектах среды эксплуатации, которые могут непосредственно влиять на безопасное использование элементов ИТ. Результаты процесса оценки 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.

e) Критерии для оценки специфических качеств криптографических алгоритмов не входят в ГОСТ Р ИСО/МЭК 15408. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяется ГОСТ Р ИСО/МЭК 15408, должно быть предусмотрено проведение таких оценок.

Данная часть ГОСТ Р ИСО/МЭК 15408 определяет 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 потребите-

лями для спецификации и идентификации продуктов с характеристиками безопасности ИТ, которые будут удовлетворять их потребностям. Задание по безопасности (ЗБ) выражает 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 ГОСТ Р ИСО/МЭК 15408.

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

П р и м е ч а н и е: Раздел 2 содержит только те термины, которые используются во всем тексте ГОСТ Р ИСО/МЭК 15408 особым образом. Большинство терминов в ГОСТ Р 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 ГОСТ Р ИСО/МЭК 15408 и не вошедшие в данный раздел 2, объясняются непосредственно в тексте по месту использования. Объяснение терминов и понятий, применяемых особым образом в ГОСТ ИСО/МЭК 15408-2 и ГОСТ 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 ГОСТ Р ИСО/МЭК 15408-3 в 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 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 ПЗ, ЗБ или пакет**.**

2.10 связность (connectivity)**:** Свойство ОО, позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО. Это взаимодействие включает 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, 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 ГОСТ Р ИСО/МЭК 15408-3, представляющий некоторое положение на предопределенной в ГОСТ Р ИСО/МЭК 15408 шкале доверия.

2.15 орган оценки (evaluation authority)**:** Организация, которая посредством системы оценки обеспечивает реализацию ГОСТ Р 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 ГОСТ Р ИСО/МЭК 15408.

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

2.18 внешняя сущность ИТ (external IT entity)**:** Любые 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 описывает 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 либо полное или сокращенное имя этого пользователя, либо 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 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 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)**:** Добавление деталей в компонент.

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 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 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, которая инициирует 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 использоваться или потребляться в 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

Следующие сокращения являются общими для всех частей ГОСТ Р ИСО/МЭК 15408.

ЗБ (ST) Задание по безопасности

ИТ (IT) Информационная технология

ИФБО (TSFI) Интерфейс ФБО

ОДФ (TSC) Область действия ФБО

ОО (TOE) Объект оценки

ОУД (EAL) Оценочный уровень доверия

ПБО (TSP) Политика безопасности ОО

ПЗ (PP) Профиль защиты

ПФБ (SFP) Политика функции безопасности

СФБ (SOF) Стойкость функции безопасности

ФБ (SF) Функция безопасности

ФБО (TSF) Функции безопасности ОО

4 Краткий обзор

В этом разделе представлены основные концептуальные положения ГОСТ Р ИСО/МЭК 15408. В нем определены категории пользователей ГОСТ Р 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, будучи размещенной в продуктах или системах ИТ, останется приватной, доступной им по мере необходимости и не сможет быть подвергнута несанкционированной модификации. При выполнении продуктами или системами ИТ своих функций следует осуществлять надлежащее управление информацией для обеспечения ее защиты от опасностей типа нежелательного или неоправданного распространения, изменения или потери. Термин «безопасность ИТ» используется для того, чтобы охватить предотвращение и уменьшение этих и подобных опасностей.

Многие потребители ИТ из-за недостатка знаний, компетентности или ресурсов не будут уверены в безопасности применяемых продуктов и систем ИТ и, 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 (т.е. оценку безопасности).

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

4.1.1 Пользователи ГОСТ Р ИСО/МЭК 15408

В оценке характеристик безопасности продуктов и систем ИТ заинтересованы в основном потребители, разработчики и оценщики. Критерии, представленные в настоящем документе, структурированы в интересах этих групп, потому что именно они рассматриваются как основные пользователи ГОСТ Р ИСО/МЭК 15408. В последующих пунктах объясняется, какую пользу могут принести критерии каждой из этих групп.

4.1.1.1 Потребители

ГОСТ Р ИСО/МЭК 15408 играет важную роль в методической поддержке выбора потребителями требований безопасности ИТ для выражения своих потребностей. ГОСТ Р ИСО/МЭК 15408 написан, чтобы обеспечить посредством оценки удовлетворение запросов потребителей, поскольку это является основной целью и логическим обоснованием процесса оценки.

Результаты оценки помогают потребителям решить, вполне ли оцениваемый продукт или система удовлетворяет 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. Иерархическое представление требований доверия способствует этому.

ГОСТ Р 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

ГОСТ Р ИСО/МЭК 15408 предназначен для поддержки разработчиков при подготовке к оценке своих продуктов или систем и содействии в ее проведении, а также при установлении требований безопасности, которым должны удовлетворять каждый их продукт или система. Вполне возможно, что использование совместно с ГОСТ Р ИСО/МЭК 15408 методологии оценки, потенциально сопровождаемой соглашением о взаимном признании результатов оценки, позволит к тому же использовать ГОСТ Р ИСО/МЭК 15408 для поддержки иных лиц, помимо разработчиков ОО, при подготовке этого ОО к оценке и содействии в ее проведении.

Конструкции из ГОСТ Р ИСО/МЭК 15408 могут тогда использоваться для формирования утверждения о соответствии ОО установленным для него требованиям посредством подлежащих оценке специфицированных функций безопасности и мер доверия. Требования для каждого 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 ГОСТ Р ИСО/МЭК 15408 описаны функции безопасности, которые разработчик мог бы включить в ОО. ГОСТ Р ИСО/МЭК 15408 можно использовать 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

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

4.1.1.4 Прочие

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

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

b) аудиторы как внутренние, так и внешние, ответственные за оценку адекватности безопасности 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 устанавливает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться организациям, проводящим оценку, и самим оценщикам.

В ГОСТ Р ИСО/МЭК 15408 не излагаются требования к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок. На рисунке 1 показаны основные элементы формирования контекста для оценок.

Использование общей методологии оценки позволяет достичь повторяемости и объективности результатов, но только этого недостаточно. Многие из критериев оценки требуют привлечения экспертных решений и базовых знаний, добиться согласованности которых бывает нелегко. Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертификацию. Процедура сертификации представляет собой независимую инспекцию результатов оценки, которая завершается их утверждением или выдачей сертификата. Сведения о сертификатах обычно публикуются и являются общедоступными. Отметим, что сер-

тификация является средством обеспечения большей согласованности в применении критериев безопасности ИТ.

Система оценки, методология и процедуры сертификации находятся в ведении органов оценки, управляющих системами оценки, и не входят в область действия ГОСТ Р ИСО/МЭК 15408.

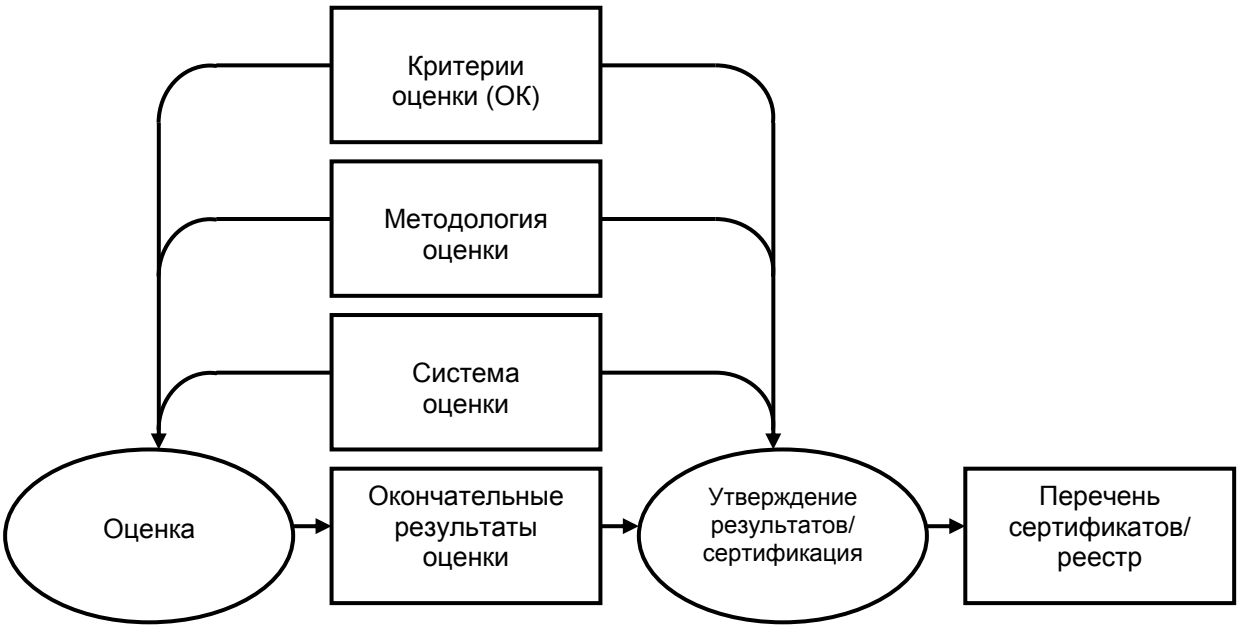

Рисунок 1 – Контекст оценки

4.3 Структура ГОСТ Р ИСО/МЭК 15408

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

a) **Часть 1 "Введение и общая модель"** является введением в ГОСТ Р ИСО/МЭК 15408. В ней определяются общие принципы и концепции оценки безопасности ИТ и приводится 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 ГОСТ Р ИСО/МЭК 15408 применительно к каждой из основных групп пользователей ГОСТ Р ИСО/МЭК 15408.

b) **Часть 2 "Функциональные требования безопасности"** устанавливает совокупность функциональных компонентов как стандартный способ выражения функциональных требований к ОО. 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. Содержит каталог всех компонентов, семейств и классов доверия. Кроме того, в этой части определены критерии оценки профилей защиты и заданий по безопасности и представлены оценочные уровни доверия (ОУД), которые определяют предопределенную в ГОСТ Р ИСО/МЭК 15408 шкалу ранжирования доверия к ОО.

Предполагается, что в поддержку трех частей ГОСТ Р ИСО/МЭК 15408, перечисленных выше, будут опубликованы и документы других типов, включая нормативно-методические материалы и руководства.

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

Т а б л и ц а 1 – Путеводитель по «Критериям оценки безопасности информационных технологий»

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

5 Общая модель

В этом разделе представлены общие понятия, используемые во всех частях ГОСТ Р ИСО/МЭК 15408, включая контекст использования этих понятий, и подход ГОСТ Р ИСО/МЭК 15408 к их применению. ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 развивают эти понятия в рамках описанного подхода. Этот раздел предполагает наличие определенных знаний по безопасности ИТ и не предназначен для использования в качестве учебного пособия в этой области.

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

5.1 Контекст безопасности

5.1.1 Общий контекст безопасности

Безопасность связана с защитой активов от угроз, где 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 с действиями человека, злонамеренными или иными. Рисунок 2 иллюстрирует высокоуровневые понятия безопасности и их взаимосвязь.

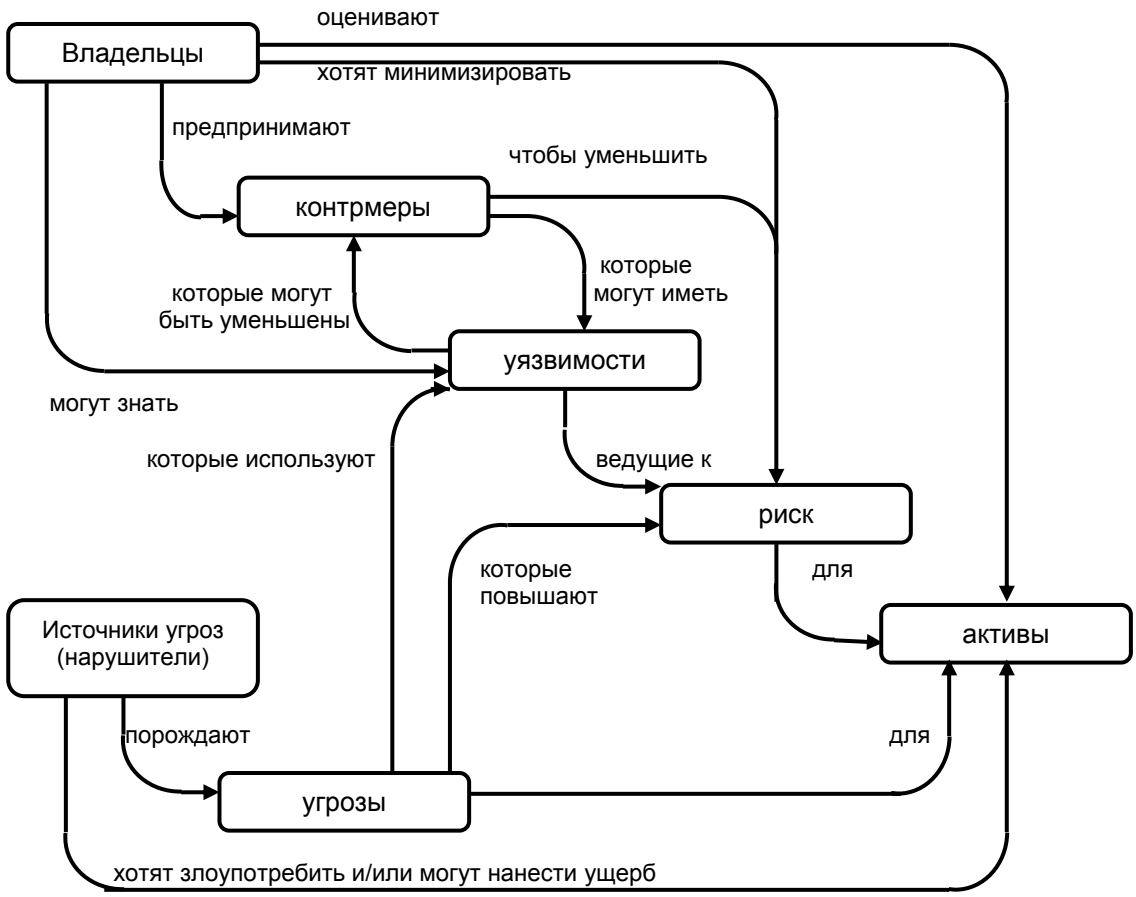

Рисунок 2 – Понятия безопасности и их взаимосвязь

За сохранность рассматриваемых активов отвечают их владельцы, для которых эти активы имеют ценность. Существующие или предполагаемые нарушители также могут придавать значение этим активам и стремиться использовать их вопреки интересам их владельца. Владельцы будут воспринимать подобные угрозы как потенциал воздействия на активы, приводящего к понижению их ценности для владельца. К специфическим нарушениям безопасности обычно относят (но не обязательно ими 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 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 между этими составляющими). Но и после введения этих контрмер могут сохраняться остаточные уязвимости. Такие уязвимости могут использоваться нарушителями, представляя уровень остаточного риска для активов. Владельцы будут стремиться минимизировать этот риск с учетом имеющихся ограничений.

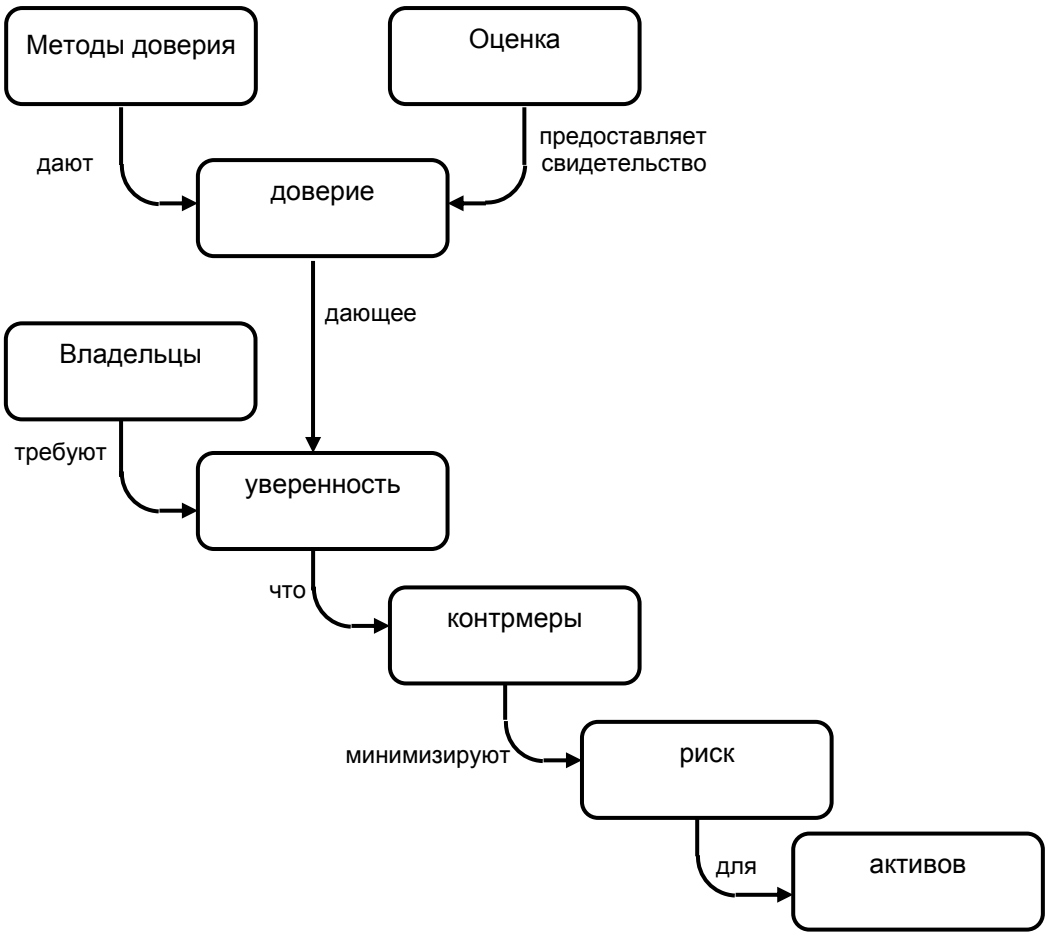

Рисунок 3 – Понятия, используемые при оценке, и их взаимосвязь

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, их владельцам 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 их оценку. Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В этом заключении устанавливается 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. Рисунок 3 иллюстрирует эту взаимосвязь.

Поскольку за активы несут ответственность их владельцы, то им следует иметь возможность отстаивать принятое решение о приемлемости риска для активов, 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 свидетельств.

5.1.2 Контекст безопасности информационных технологий

Многие активы представлены в виде информации, которая хранится, обрабатывается и передается продуктами или системами ИТ таким образом, чтобы удовлетворить требования владельцев этой информации. Владельцы информации вправе требовать, чтобы распространение и модификация любых таких представлений информации (данных) строго контролировались. Они могут запросить, 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 приобретаются и создаются для выполнения определенных требований, и при этом, по экономическим причинам, могут максимально использоваться 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 продуктах ИТ, и, следовательно, зависят от правильного выполнения функций безопасности продуктов ИТ. Поэтому продукты ИТ могут подлежать 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 выражать таким образом, чтобы имелась возможность использовать продукт в различных системах ИТ без излишнего повторения работ по экспертизе его безопасности.

Аттестующий систему ИТ имеет 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 оценку реализованных в ИТ контрмер, 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 ГОСТ Р ИСО/МЭК 15408

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

5.2.1 Разработка

ГОСТ Р ИСО/МЭК 15408 не предписывает конкретную методологию разработки или модель жизненного цикла. На рисунке 4 представлены основополагающие предположения о соотношениях между требованиями безопасности и собственно ОО. Этот рисунок используется для контекста обсуждения и его не следует интерпретировать как демонстрацию преимущества одной методологии разработки (например, каскадной) перед другой (например, по прототипу).

Существенно, чтобы требования безопасности, налагаемые на разработку 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.

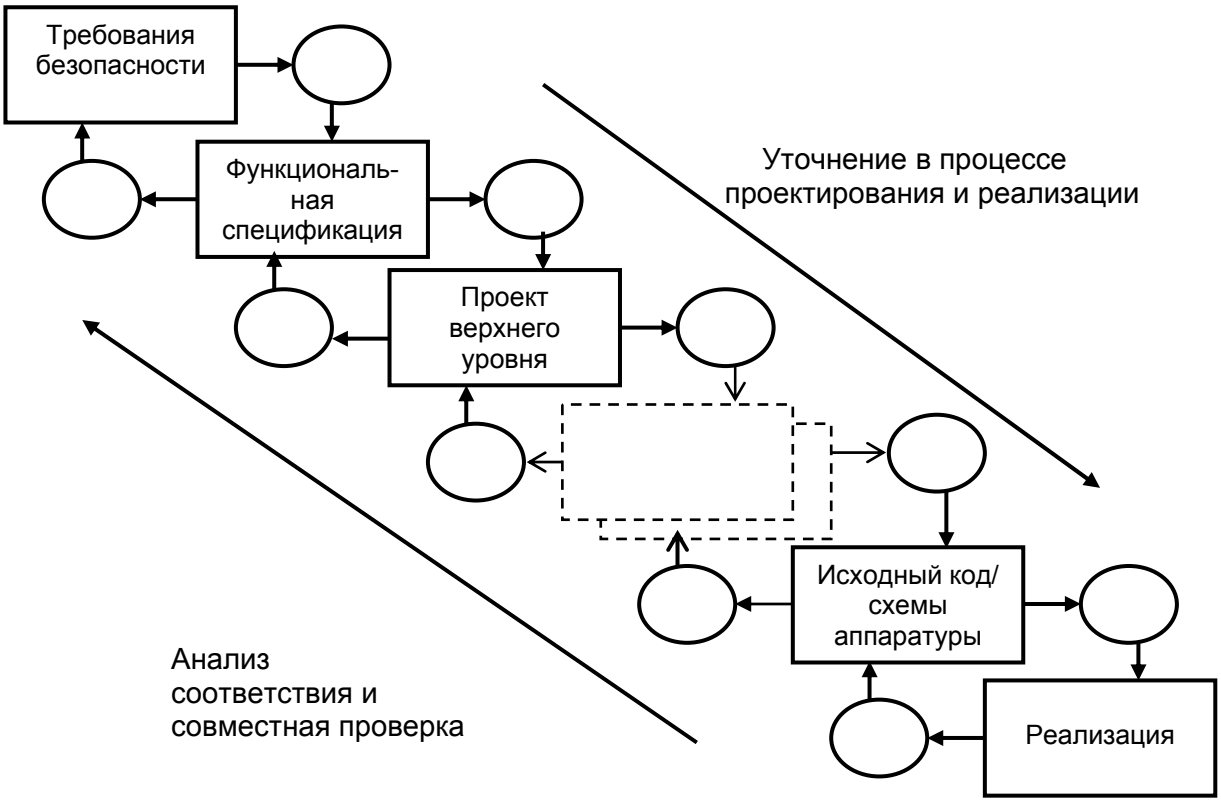

Рисунок 4 – Модель разработки ОО

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

ГОСТ Р ИСО/МЭК 15408 не предписывает конкретную совокупность представлений проекта. В ГОСТ Р ИСО/МЭК 15408 требуется, чтобы имелось достаточное число представлений проекта с достаточным уровнем детализации для демонстрации, если потребуется, 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 ГОСТ Р 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 ГОСТ Р ИСО/МЭК 15408.

5.2.2 Оценка ОО

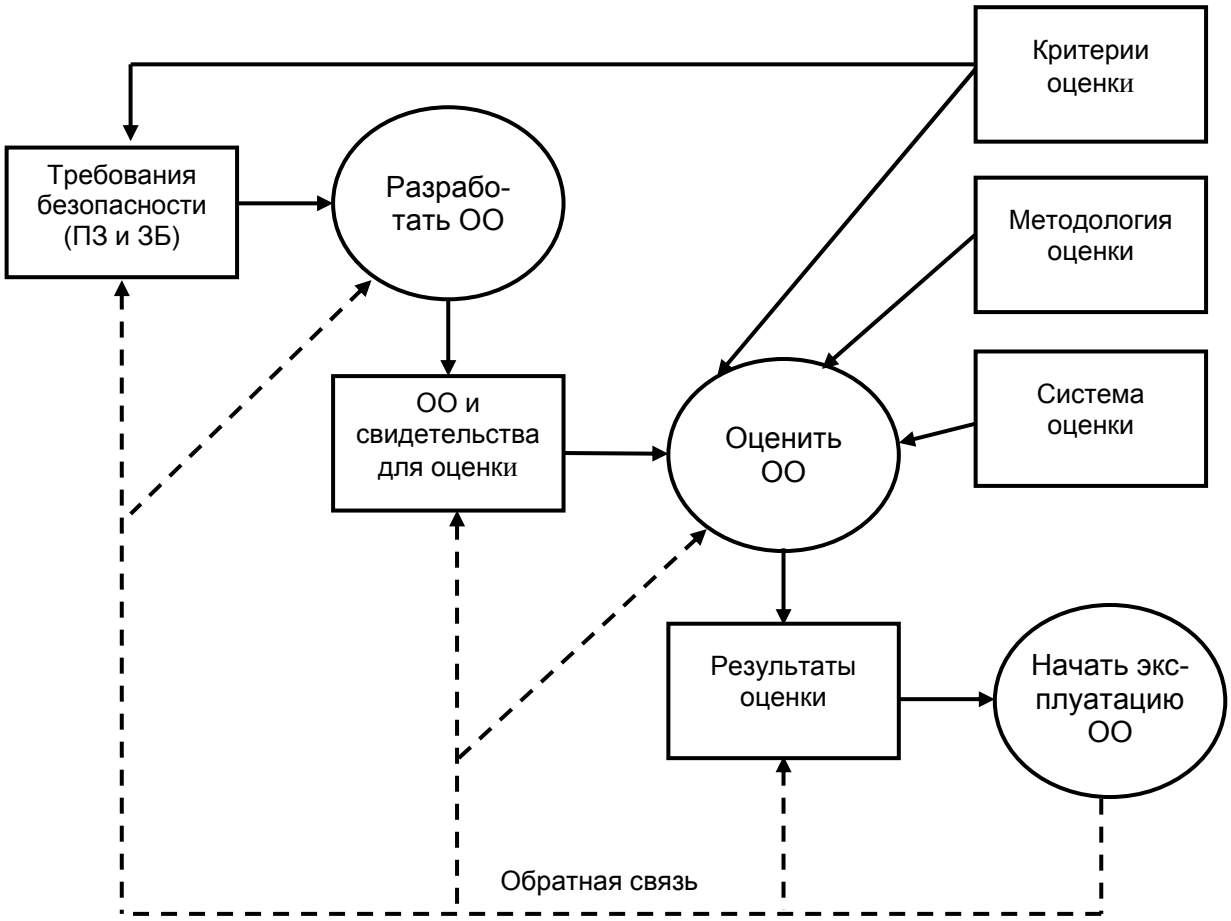

Рисунок 5 – Процесс оценки ОО

Процесс оценки ОО, как показано на рисунке 5, может проводиться параллельно с разработкой или следом 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.

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

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

Оценка может способствовать созданию более безопасных продуктов ИТ по двум направлениям. Оценка предназначена для выявления ошибок или уязвимостей в ОО, устраняя которые разработчик снижает вероятность нарушения безопасности ОО при его последующей эксплуата-

ции. 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 своих конкретных условиях. Не исключено, что при эксплуатации ОО могут проявиться 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, в свою очередь, могут привести к необходимости проведения новой оценки ОО или 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 ГОСТ Р ИСО/МЭК 15408.

5.3 Понятия безопасности

Критерии оценки наиболее полезны в контексте процессов проектирования и правовой базы, поддерживающих безопасную разработку и оценку ОО. Этот 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 ГОСТ Р ИСО/МЭК 15408.

ГОСТ Р ИСО/МЭК 15408 применим, если при использовании ИТ придают значение способности элементов ИТ обеспечить сохранность активов. Чтобы показать защищенность активов, вопросы безопасности необходимо рассмотреть на всех уровнях, начиная с самого абстрактного и до конечной реализации ИТ в среде их эксплуатации. Эти уровни представления, как описано в следующих подразделах, позволяют охарактеризовать и обсудить задачи и проблемы безопасности, однако сами по себе не демонстрируют, что конечная реализация ИТ действительно проявляет требуемый режим безопасности и поэтому может считаться доверенной.

В ГОСТ Р ИСО/МЭК 15408 требуется, чтобы определенные уровни представления содержали обоснование представления ОО на этом уровне. Это значит, что такой уровень должен содержать достаточно разумные и 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, приводится как довод корректности ОО. Обоснование, непосредственно демонстрирующее соответствие целям безопасности, поддерживает доводы об эффективности ОО в противостоянии угрозам и в осуществлении политики безопасности организации.

В ГОСТ Р ИСО/МЭК 15408 используются различные формы представления, что показано на рисунке 6, который иллюстрирует возможный способ последовательного формирования требований безопасности и спецификаций при разработке ПЗ или ЗБ. 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.

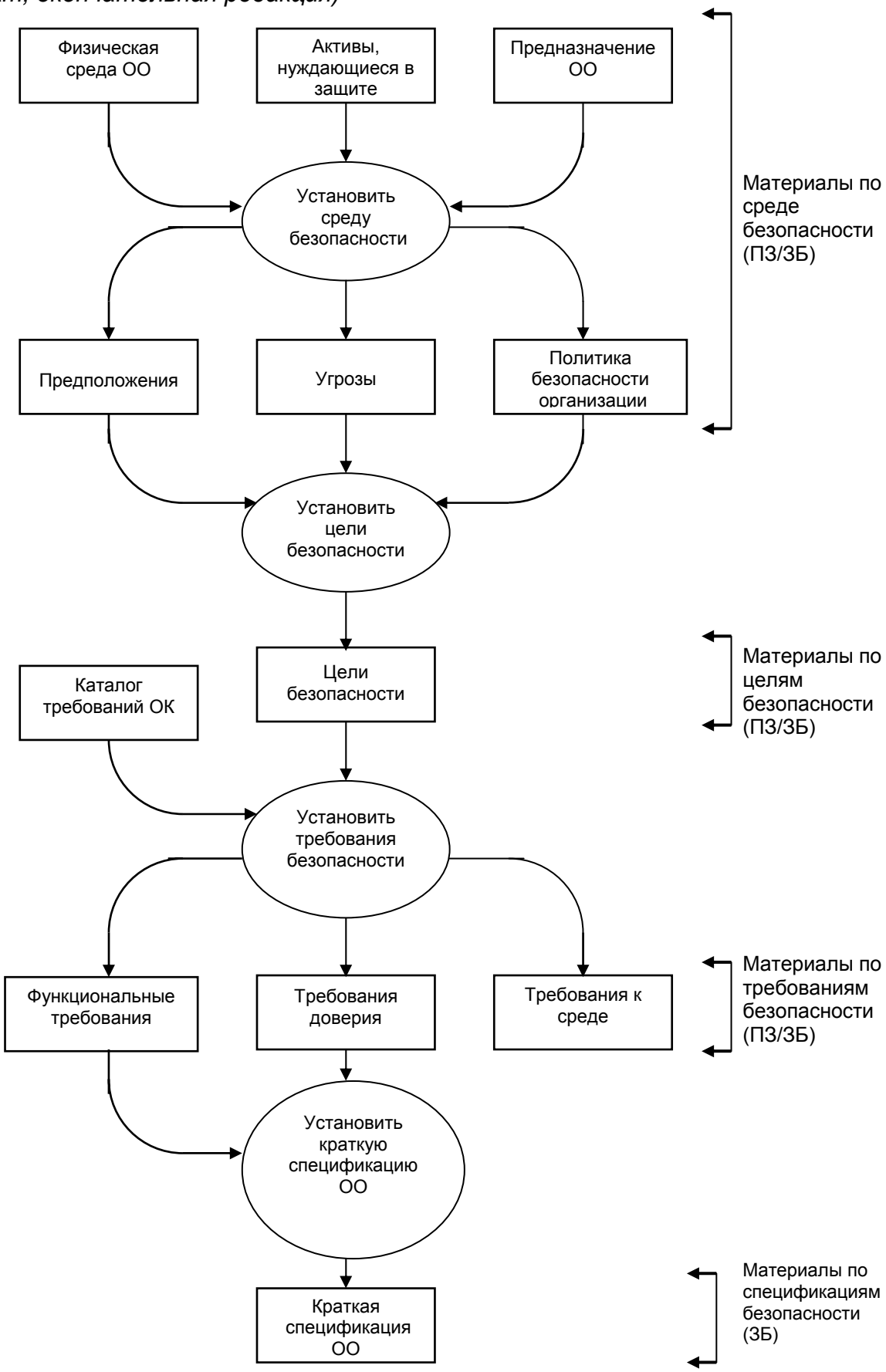

Рисунок 6 – Последовательное формирование требований и спецификаций

5.3.1 Среда безопасности

Среда безопасности включает все законы, политики безопасности организаций, опыт, специальные навыки и знания, для которых решено, что они имеют 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 активы, к которым это относится непосредственно, типа файлов и баз данных, а также активы, которые косвенно подчинены требованиям безопасности, типа данных 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 материалы, 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 ГОСТ Р ИСО/МЭК 15408 угрозы раскрываются через понятия источника угрозы, предполагаемого метода нападения, любых уязвимостей, которые являются предпосылкой для нападения, и идентификации активов, которые являются целью нападения. При оценке рисков безопасности будет квалифицирована каждая угроза безопасности с оценкой возможности ее перерастания в фактическое нападение, вероятности успешного проведения такого нападения и последствий любого возможного ущерба;

c) изложение политики безопасности, применяемой в организации, в котором были бы идентифицированы политики и правила, относящиеся к ОО. Для системы ИТ такая политика может быть описана достаточно точно, тогда как для продуктов ИТ общего предназначения или класса продуктов о политике безопасности организации могут быть сделаны, при необходимости, только рабочие предположения.

5.3.2 Цели безопасности

Результаты анализа среды безопасности могут затем использоваться 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 его целей безопасности.

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

Функциональные требования налагаются на те функции ОО, которые предназначены для поддержания безопасности ИТ и определяют желательный безопасный режим функционирования ОО. Функциональные требования определены в ГОСТ Р ИСО/МЭК 15408-2. Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности, неотказуемости источника (невозможности отказа от факта отправления сообщения).

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

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

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

a) уверенности в корректности реализации функций безопасности, т.е. оценки того, правильно ли они реализованы;

b) уверенности в эффективности функций безопасности, т.е. оценки того, действительно ли они отвечают изложенным целям безопасности.

Требования безопасности обычно включают 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 ГОСТ Р ИСО/МЭК 15408

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

5.4.1 Представление требований безопасности

ГОСТ Р 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 описана ниже и иллюстрируется на рисунке 7.

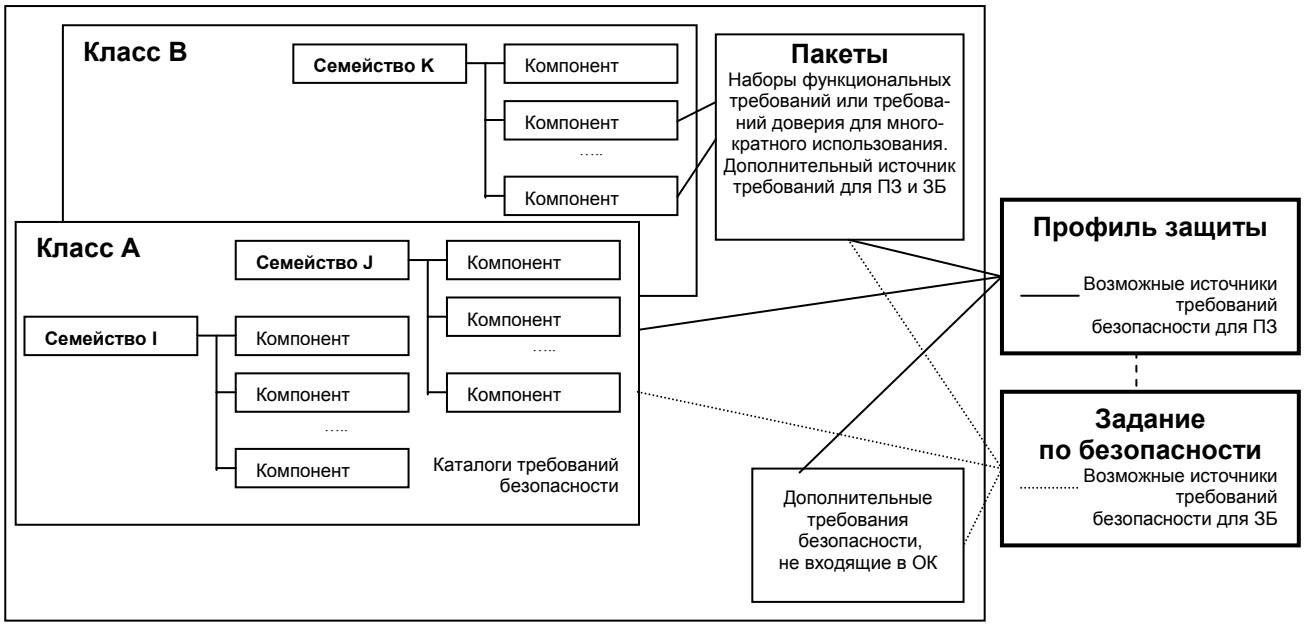

Рисунок 7 – Организация и структура требований

Организация требований безопасности в ГОСТ Р ИСО/МЭК 15408 в виде иерархии класс – семейство – компонент призвана помочь потребителям в поиске конкретных требований безопасности.

Функциональные требования и требования доверия представлены в ГОСТ Р 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 ГОСТ Р ИСО/МЭК 15408. Совокупность компонентов, входящих в семейство, может быть упорядочена для представления возрастания строгости или возможностей требований безопасности, имеющих общее назначение. Они могут быть также упорядочены частично, для представления связанных неиерархических наборов. Упорядочение не применимо в случае, когда в семействе имеется только один компонент.

Компоненты составлены из отдельных элементов. Элемент – это выражение требований безопасности на самом нижнем уровне. Он 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, когда 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 ГОСТ Р ИСО/МЭК 15408. Чтобы обеспечить полноту требований к ОО, следует удовлетворить, 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 ГОСТ Р ИСО/МЭК 15408 можно использовать точно так, как они сформулированы в ГОСТ Р ИСО/МЭК 15408, или же можно их конкретизировать, применяя разрешенные операции для удовлетворения некоторой цели безопасности. Когда некоторый 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, которые зависят от данного требования, были удовлетворены. Разрешенные операции выбираются 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 более 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 всегда повторять полный текст каждой итерации компонента, если так делать, то это привело бы к тому, что некоторые элементы в рамках компонента повторялись бы несколько раз без изменений. Допускается в ПЗ или ЗБ повторять только те элементы требований, которые каждый раз изменяются, либо путем уточнения, либо путем выполнения операций назначения или выбора (см. п. 5.4.1.3.2.4 «Уточнение» для дальнейшего руководства по итерации уточненных требований).

5.4.1.3.2.2 Назначение

Некоторые компоненты включают элементы, которые содержат параметры, дающие возможность разработчику ПЗ/ЗБ специфицировать совокупность величин для включения в ПЗ/ЗБ, чтобы удовлетворить некоторую цель 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 списка, чтобы ограничить область применения элемента в рамках компонента.

5.4.1.3.2.4 Уточнение

Для всех компонентов разработчику ПЗ/ЗБ разрешается ограничить множество допустимых реализаций путем определения дополнительных деталей для достижения некоторой цели безопасности. Уточнение некоторого элемента в рамках компонента заключается в добавлении этих технических деталей.

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 когда 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, которое является исключительно редакционным, такое как улучшение читабельности выполненного назначения или учет грамматических правил.

b) Изменение, которое не меняет область действия требования из-за контекста, в котором оно используется в ПЗ/ЗБ. Например, изменение требования, которое определяет «пользователей ОО» в качестве «telnet-пользователей ОО» будет допустимым уточнением, когда пользователи ОО являются только telnet-пользователями.

c) Изменение, которое предоставляет 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 ГОСТ Р ИСО/МЭК 15408-2 предоставляют руководство по допустимому выполнению операций выбора и назначения. Это руководство предоставляет нормативные инструкции по тому, как выполнять операции, и этим инструкциям должны следовать, если автор ПЗ/ЗБ логически не обоснует отклонение:

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

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

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

b) По отношению к выполнению операций назначения Приложения ГОСТ Р ИСО/МЭК 15408-2 указывают, когда «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 ГОСТ Р ИСО/МЭК 15408 определены три типа конструкций требований: пакет, ПЗ и ЗБ. Помимо этого, в ГОСТ Р ИСО/МЭК 15408 определена совокупность критериев безопасности ИТ, которые могут отвечать потребностям многих сообществ пользователей и поэтому служат основным исходным материалом для создания этих конструкций. Центральной идеей ГОСТ Р ИСО/МЭК 15408 является концепция максимально широкого использования определенных в ГОСТ Р ИСО/МЭК 15408 компонентов, которые представляют хорошо известную и понятную сферу применимости. Рисунок 8 показывает взаимосвязь между различными конструкциями.

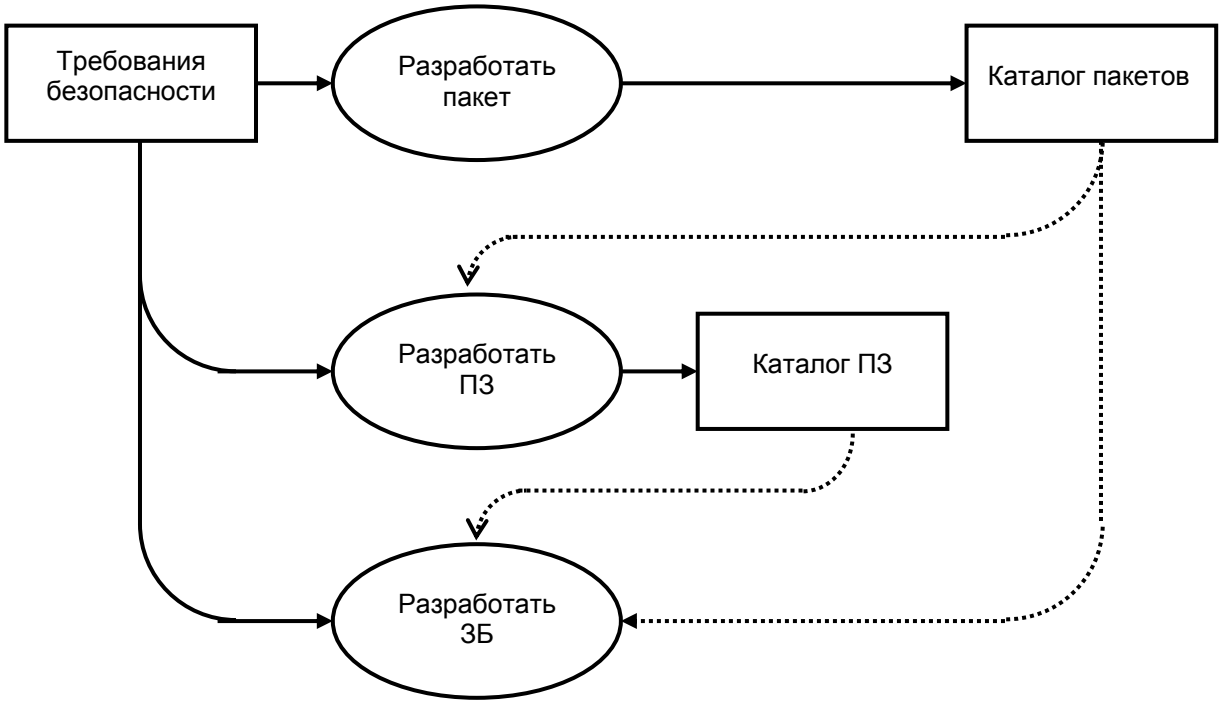

Рисунок 8 – Использование требований безопасности

5.4.1.4.1 Пакет

Промежуточная комбинация компонентов называется пакетом. Пакет позволяет выразить совокупность функциональных требований или требований доверия, которые отвечают идентифицируемому подмножеству целей безопасности. Пакет предназначен для многократного использования и определяет требования, которые известны 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 (ОУД) – это предопределенные пакеты требований доверия, содержащиеся в ГОСТ Р ИСО/МЭК 15408-3. ОУД является базовым набором требований доверия для оценки. Каждый ОУД определяет непротиворечивый набор требований доверия. Совместно ОУД формируют упорядоченное множество, которое является предопределенной в ГОСТ Р ИСО/МЭК 15408 шкалой доверия.

5.4.1.4.2 Профиль защиты

ПЗ содержит совокупность требований безопасности, взятых из ГОСТ Р ИСО/МЭК 15408, или сформулированных в явном виде, в которую следует включить 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 целей. ПЗ также содержит обоснование требований и целей безопасности.

ПЗ может разрабатываться сообществами пользователей, разработчиками продуктов ИТ или другими сторонами, заинтересованными в определении такой общей совокупности требова-

ний. 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 ГОСТ Р ИСО/МЭК 15408 или же сформулированы в явном виде. ЗБ позволяет выразить для конкретного ОО требования безопасности, которые по результатам оценки ЗБ признаны полезными и эффективными для достижения установленных целей безопасности.

ЗБ содержит краткую спецификацию ОО совместно с требованиями и целями безопасности и обоснованием для каждого из них. 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 ГОСТ Р ИСО/МЭК 15408-3. Требования доверия к ОО, входящие в ПЗ или ЗБ, должны включать какой-либо ОУД из ГОСТ Р 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 ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3;

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

Материалы имеющихся требований из ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 следует использовать всюду, где это допустимо. Использование существующего ПЗ поможет обеспечить 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

Оценка ПЗ выполняется согласно критериям оценки ПЗ, содержащимся в ГОСТ Р ИСО/МЭК 15408-3. Целью такой оценки является продемонстрировать, что профиль полон, непротиворечив, технически правилен и пригоден для использования при изложении требований к ОО, предполагаемому для оценки.

5.4.2.2 Оценка ЗБ

Оценка ЗБ для ОО выполняется согласно критериям оценки ЗБ, содержащимся в ГОСТ Р ИСО/МЭК 15408-3. Такая оценка имеет 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, когда в ЗБ имеется утверждение о соответствии некоторому ПЗ, – продемонстрировать, что ЗБ должным образом отвечает требованиям этого ПЗ.

5.4.2.3 Оценка ОО

Оценка ОО производится согласно критериям оценки, содержащимся в ГОСТ Р ИСО/МЭК 15408-3, с использованием в качестве основы в основном завершенного ЗБ. В основном завершенное ЗБ снижает риск проблем позднее в процессе оценки, в нем все разделы 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 ГОСТ Р ИСО/МЭК 15408 и результаты оценки

6.1 Введение

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

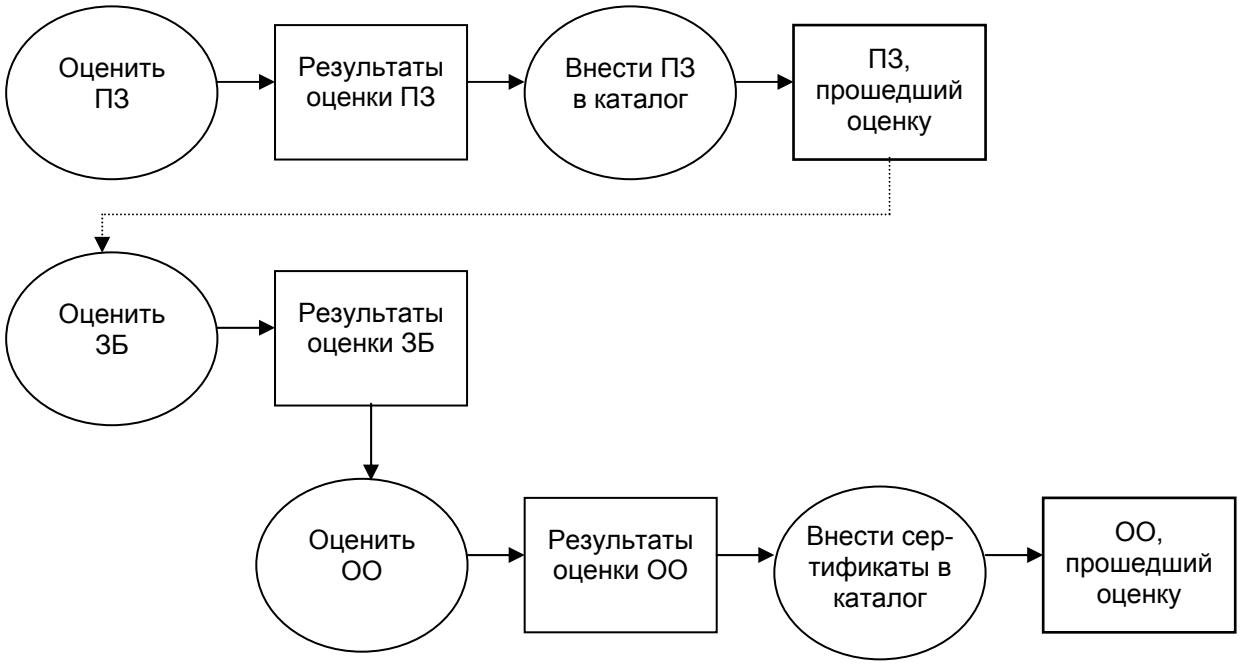

Рисунок 9 – Результаты оценки

Необходимо, чтобы оценка приводила к объективным и повторяемым результатам, на которые затем можно ссылаться как на свидетельство даже при отсутствии абсолютно объективной шкалы для представления результатов оценки безопасности ИТ. Наличие совокупности критериев оценки является необходимым предварительным условием для того, чтобы оценка приводила к значимому результату, предоставляя техническую основу для взаимного признания результатов оценки различными органами оценки. Но практическое применение критериев включает как объективные, так и субъективные элементы, поэтому невозможно получение абсолютно точных и универсальных рейтингов безопасности ИТ.

Рейтинг, полученный в соответствии с ГОСТ Р 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 и выводы оценки.

6.2 Требования, включаемые в ПЗ и ЗБ

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

В ГОСТ Р 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 в ПЗ или ЗБ таких расширенных требований должны быть выполнены следующие условия:

a) любые расширенные функциональные требования или требования доверия, включенные в ПЗ или ЗБ, должны иметь четкую и недвусмысленную формулировку, выраженную таким образом, что оценка и демонстрация соответствия ОО этим требованиям была бы возможна. В качестве образца должен использоваться уровень детализации и способ выражения существующих функциональных компонентов и компонентов доверия из ГОСТ Р ИСО/МЭК 15408;

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

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

6.2.1 Результаты оценки ПЗ

ГОСТ Р 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 формулироваться как "соответствие/несоответствие". ПЗ, для которого оценка заканчивается положительно, должен получить право включения в реестр.

6.3 Требования к ОО

ГОСТ Р ИСО/МЭК 15408 содержит критерии оценки, которые позволяют оценщику решить, удовлетворяет ли ОО требованиям безопасности, выраженным в ЗБ. Используя ГОСТ Р ИСО/МЭК 15408 при оценке ОО, оценщик сможет прийти к 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 ГОСТ Р ИСО/МЭК 15408, определяют хорошо отработанную сферу применимости критериев оценки безопасности ИТ. ОО, для которого требования безопасности выражены только в терминах функциональных требований и требований доверия из ГОСТ Р ИСО/МЭК 15408, может быть оценен по ГОСТ Р ИСО/МЭК 15408. Использование пакетов требований доверия, не содержащих ОУД, должно быть логически обосновано.

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

Результаты оценки ОО должны включать утверждение о соответствии ГОСТ Р ИСО/МЭК 15408. Описание безопасности ОО в терминах ГОСТ Р 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 формулироваться как "соответствие/несоответствие". ОО, для которого оценка заканчивается положительно, должен получить право включения в реестр. Результаты оценки должны также включать «Результаты оценки соответствия»

6.4 Результаты оценки соответствия

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

Результаты оценки соответствия включают одно из следующего:

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

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

а также одно из следующего:

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

b) «**расширение ГОСТ Р ИСО/МЭК 15408-3»** – ПЗ или ОО является расширенным по отношению к ГОСТ Р ИСО/МЭК 15408-3, если требования доверия включают требования доверия не из ГОСТ Р ИСО/МЭК 15408-3;

Кроме того, результат оценки соответствия может включать утверждение, сделанное относительно набора определенных требований; в данном случае результат оценки соответствия включает 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 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 утверждение, сделанное относительно профилей защиты; в данном случае результат оценки соответствия включает следующее:

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

6.5 Использование результатов оценки ОО

Продукты и системы ИТ отличаются в отношении использования результатов оценки. На рисунке 10 показаны различные пути использования результатов оценки. Продукты можно оценивать и каталогизировать последовательно на все более высоких уровнях агрегирования вплоть до достижения уровня эксплуатируемых систем, когда продукты могут подлежать оценке в связи с аттестацией системы.

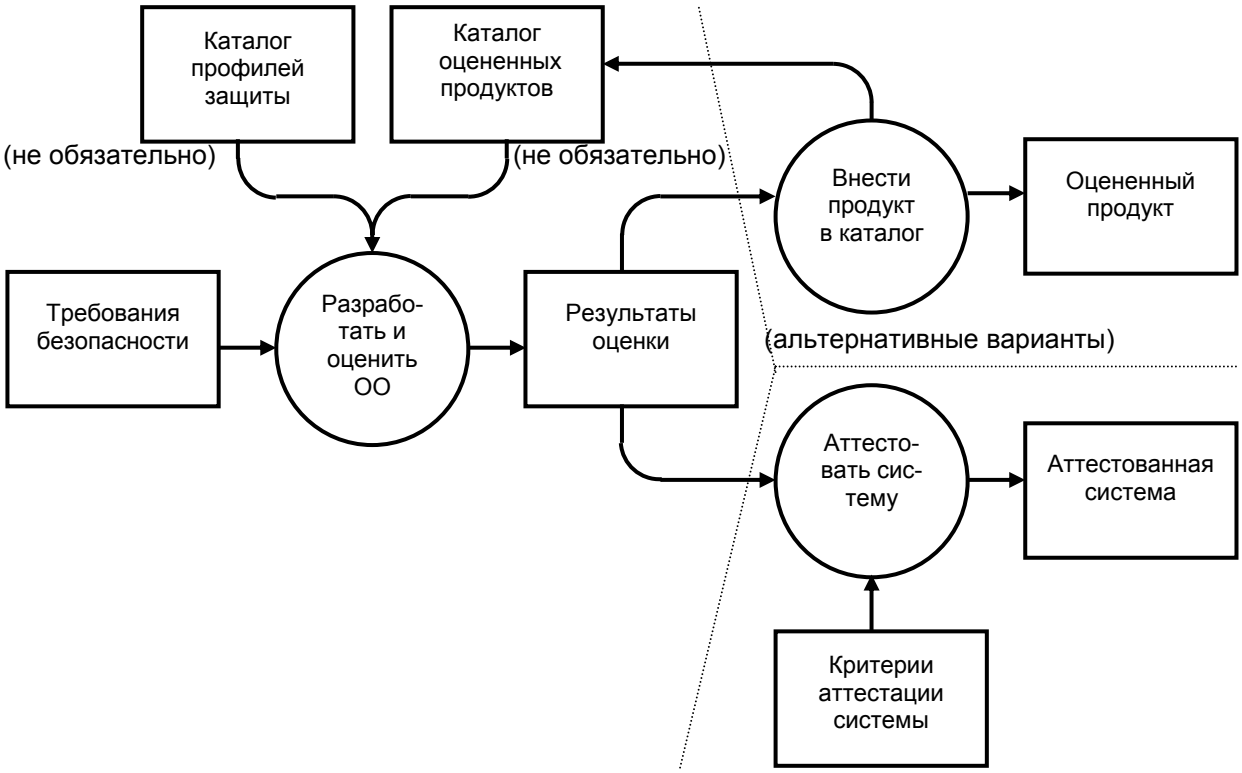

Рисунок 10 – Использование результатов оценки ОО

ОО разрабатывается 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 делаются ссылки. Последующая оценка ОО приводит к получению совокупности результатов оценки, документирующих данные, полученные при оценке.

После завершения оценки продукта ИТ, предназначенного для широкого использования, краткое заключение с данными оценки может быть помещено 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, которая подвергается оценке, результаты его оценки предоставляются аттестующему систему. Тогда результаты оценки, проведенной согласно ГОСТ Р ИСО/МЭК 15408, могут быть учтены аттестующим при применении принятых в организации критериев аттестации, требующих оценки по ГОСТ Р ИСО/МЭК 15408. Результаты оценки по ГОСТ Р 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.

Данное приложение содержит требования к ПЗ в описательной форме. В классе доверия APE, в разделе 8 ГОСТ Р ИСО/МЭК 15408-3, эти 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 данном приложении. ПЗ следует представлять как ориентированный на пользователя документ с минимумом ссылок на другие материалы, которые могут быть недоступны пользователю этого ПЗ. Обоснование, при необходимости, может быть оформлено отдельно.

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

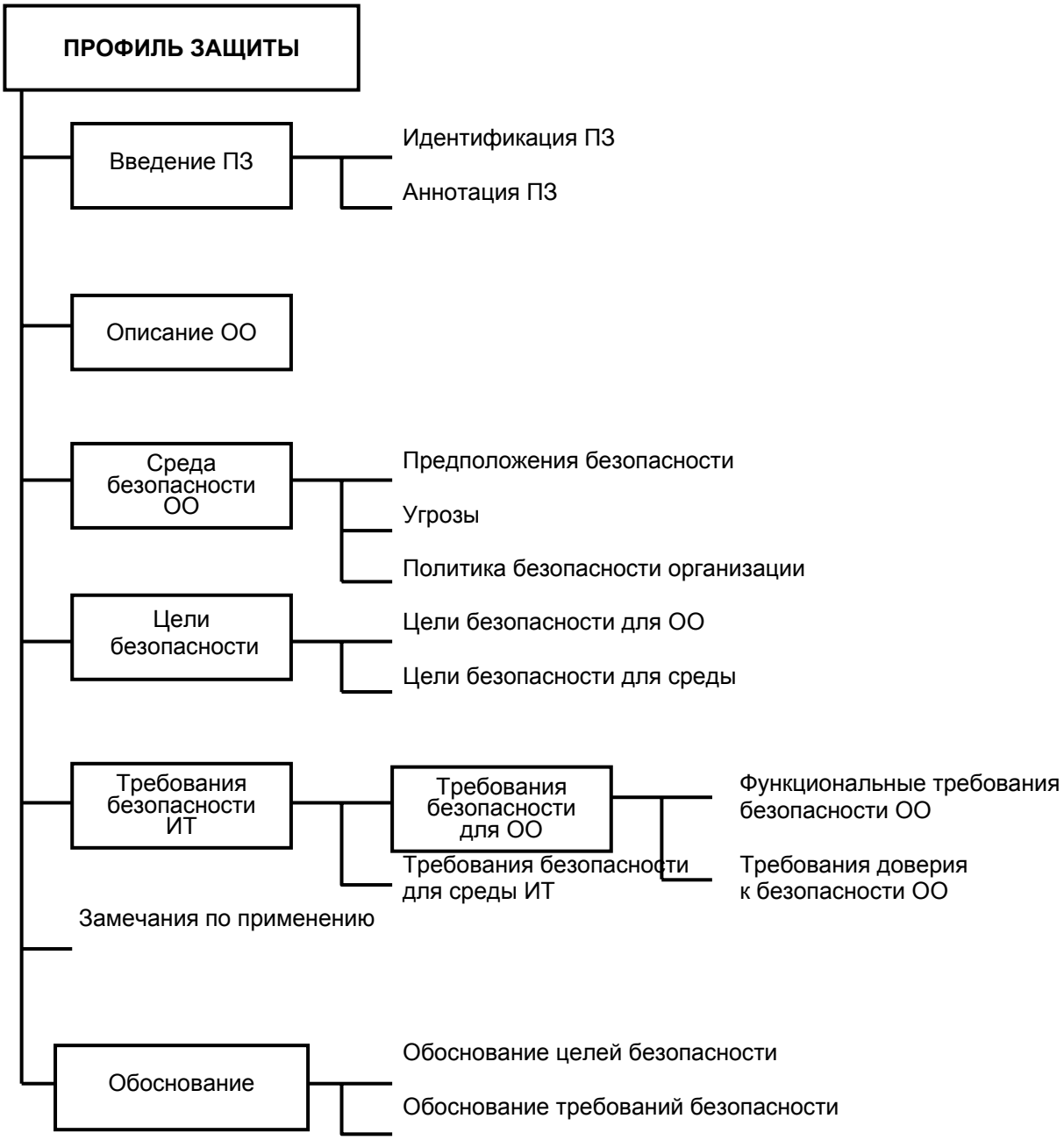

Рисунок А.1 – Содержание профиля защиты

А.2.2 Введение ПЗ

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

a) **идентификация ПЗ** должна обеспечить маркировку и описательную информацию, необходимые, чтобы идентифицировать, каталогизировать, регистрировать ПЗ и ссылаться на него;

b) **аннотация ПЗ** должна дать общую характеристику ПЗ в описательной форме. Она должна быть достаточно подробной, чтобы потенциальный пользователь ПЗ мог решить, представляет ли ПЗ для него интерес. Аннотация должна быть также применима для размещения в виде самостоятельного реферата в каталогах и реестрах ПЗ.

А.2.3 Описание ОО

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

Описание ОО предоставляет контекст для оценки. Информация, содержащаяся в описании ОО, будет использована 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 эта часть ПЗ может быть использована для описания более широкого контекста возможного 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. Это изложение должно включать следующее.

a) Описание **предположений,** содержащее аспекты безопасности среды, в которой ОО будет использоваться или предполагается к использованию. Оно должно также содержать:

- информацию относительно предполагаемого использования ОО, включая такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования;
- информацию относительно среды применения ОО, включая аспекты физического окружения, персонала и внешних связей.

b) Описание **угроз,** содержащее все те угрозы активам, против которых требуется защита средствами ОО или его среды. Заметим, что необходимо приводить не все угрозы, которые могут встретиться в среде, а только те из них, которые влияют 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 подчиняться 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 идентифицированы категории целей безопасности, приведенные ниже. Если при этом противостояние угрозе или проведение политики безопасности частично возлагается 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 отвечать 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.

Необходимо отметить, что цели безопасности для среды могут повторять, частично или полностью, некоторые предположения, сделанные при изложении среды безопасности ОО.

А.2.6 Требования безопасности ИТ

В этой 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 возможно повторное использование (то есть, применение операции итерации) одного и того же компонента ГОСТ Р ИСО/МЭК 15408-2, 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 излагаться следующим образом.

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

   Если требования доверия к ОО включают компонент AVA_SOF.1 (например, ОУД2 и выше), то при изложении функциональных требований безопасности ОО должен устанавливаться минимальный уровень стойкости для функций безопасности, реализуемых с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Все подобные функции должны удовлетворять 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.

   Как составная часть оценки стойкости функций безопасности ОО (AVA_SOF.1) будут оценены 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 ГОСТ Р ИСО/МЭК 15408-3. Расширение ОУД в ПЗ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в ГОСТ Р ИСО/МЭК 15408-3

b) Необязательное изложение **требований безопасности для среды ИТ** должно определять требования безопасности ИТ, которым должна отвечать среда ИТ этого ОО. Требования в этой части ПЗ могут быть взяты из ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 и, если так, то должна быть изменена их формулировка, чтобы четко показать, что среда ИТ, а не ОО, должна отвечать данному требованию. Подобное изменение формулировки является особым случаем уточнения и не является предметом требований оценки, связанных с модифицированными компонентами ГОСТ Р ИСО/МЭК 15408. Если безопасность ОО не зависит от среды ИТ, то эта 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) Когда это применимо, все требования безопасности ИТ следует вводить ссылкой на компоненты требований безопасности из ГОСТ Р ИСО/МЭК 15408-2 или ГОСТ Р ИСО/МЭК 15408-3. Если при формировании всех либо части требований не применимы компоненты из ГОСТ Р ИСО/МЭК 15408-2 или ГОСТ Р ИСО/МЭК 15408-3, то в ПЗ допускается сформулировать необходимые требования безопасности явным образом, без ссылки на содержание ГОСТ Р ИСО/МЭК 15408.

2) Любые функциональные требования и требования доверия к ОО, сформулированные явным образом, должны быть четко и однозначно выражены, чтобы были возможны оценка и демонстрация соответствия им. Уровень детализации и способ выражения функциональных требований и требований доверия, принятый в ГОСТ Р ИСО/МЭК 15408, должен использоваться как образец.

3) Если выбраны компоненты требований, в которых специфицированы требуемые операции (назначение, выбор), то эти 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 дополнительно разрешать или запрещать, при необходимости, использование определенных механизмов безопасности, применяя разрешенные операции над компонентами требований.

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

А.2.7 Замечания по применению

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

А.2.8 Обоснование

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

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 сопоставима с ними. Должно быть продемонстрировано следующее:

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

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

3) выбор требований безопасности логически обоснован. Каждое из перечисленных ниже условий должно быть логически обосновано:

   - выбор требований, не содержащихся в ГОСТ Р ИСО/МЭК 15408-2 или ГОСТ Р 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 для ОО.

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

В ЗБ разрешено включать требования из одного или нескольких ПЗ или утверждать о соответствии им. Влияние таких утверждений о соответствии ПЗ не учитывается при первоначальном определении требуемого содержания ЗБ в подразделе В.2. Влияние утверждения о соответствии ПЗ на содержание ЗБ рассматривается в В.2.8.

Данное приложение содержит требования к ЗБ в описательной форме. В классе доверия ASE, в разделе 9 ГОСТ Р ИСО/МЭК 15408-3, 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 данном приложении. ЗБ следует представлять в виде ориентированного на пользователя документа, с минимумом ссылок на другие материалы, которые могут быть недоступны пользователю этого ЗБ. Обоснование, при необходимости, может быть оформлено отдельно.

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

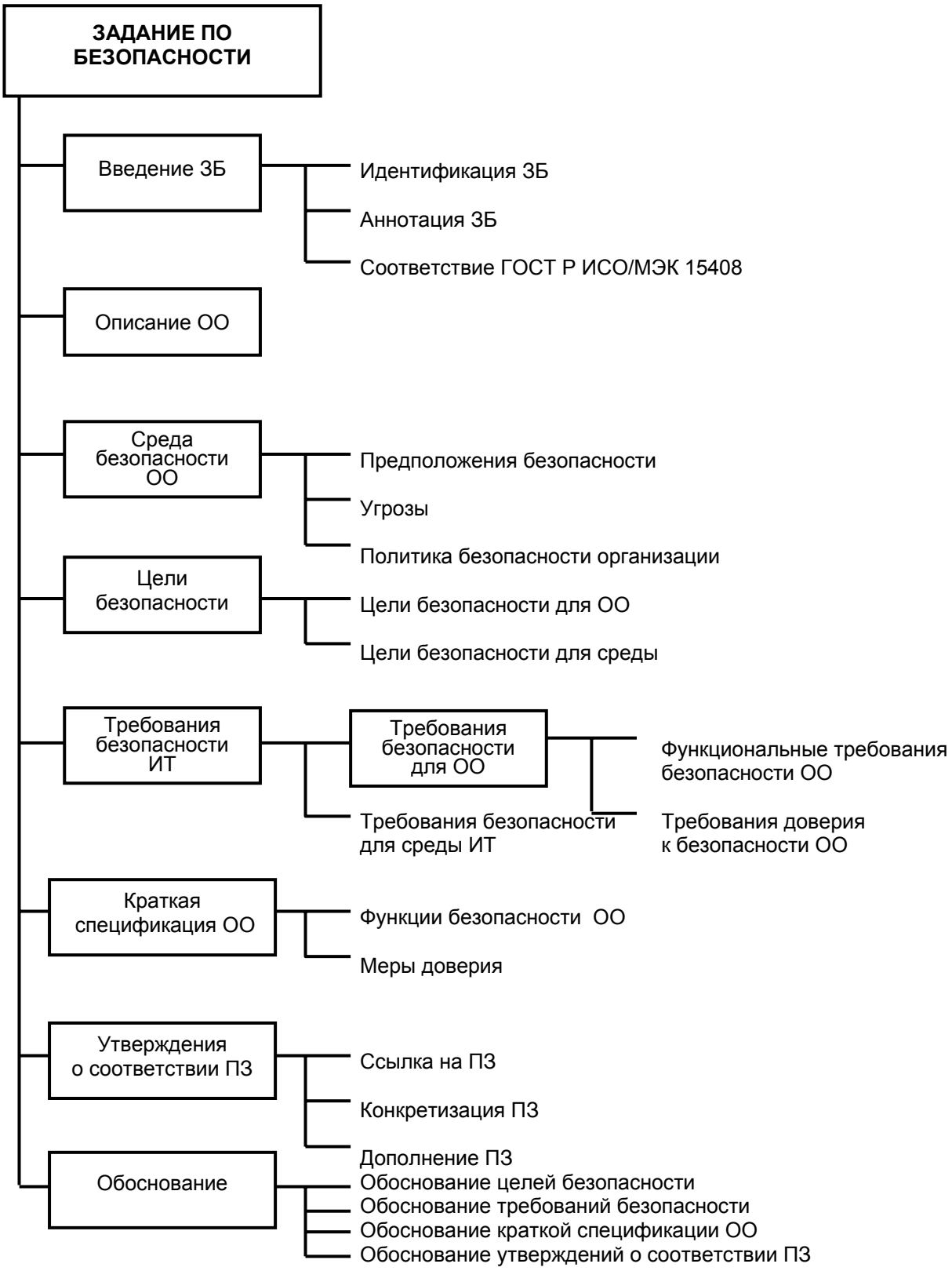

Рисунок В.1 – Содержание задания по безопасности

В.2.2 Введение ЗБ

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

a) **идентификация ЗБ** должна обеспечить маркировку и описательную информацию, необходимые, чтобы контролировать и идентифицировать ЗБ и ОО, к которому оно относится;

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

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

В.2.3 Описание ОО

Эта часть ЗБ должна содержать описание ОО, служащее цели лучшего понимания его требований безопасности и дающее представление о типе продукта или системы. Область и ограничения применения ОО должны быть описаны в общих терминах как в отношении физической (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. Информация, содержащаяся в описании ОО, будет использована в процессе оценки для выявления противоречий. Если ОО представляет собой продукт или систему, основной функцией которых является безопасность, то эту часть ЗБ разрешается использовать для более подробного описания контекста возможного 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. Это изложение должно включать следующее.

a) Описание **предположений**, содержащее аспекты безопасности среды, в которой ОО будет использоваться или предполагается к использованию. Оно должно также содержать:

- информацию относительно предполагаемого использования ОО, включая такие аспекты, как предполагаемая область применения, потенциальная значимость активов и возможные ограничения на использование;
- информацию относительно среды применения ОО, включая аспекты физического окружения, персонала и внешних связей.

b) Описание **угроз**, содержащее все те угрозы активам, против которых требуется защита средствами ОО или его среды. Заметим, что необходимо приводить не все угрозы, которые могут встретиться в среде, а только те из них, которые влияют 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 подчиняться 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.

B.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 идентифицированы категории целей безопасности, приведенные ниже. Если при этом противостояние угрозе или проведение политики безопасности частично возлагается 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 отвечать 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.

Необходимо отметить, что цели безопасности для среды могут повторять, частично или полностью, некоторые предположения, сделанные при изложении среды безопасности ОО.

B.2.6 Требования безопасности ИТ

В этой 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 возможно повторное использование (то есть, применение операции итерации) одного и того же компонента ГОСТ Р ИСО/МЭК 15408-2, 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 излагаться следующим образом.

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

   Если требуется охватить различные аспекты одного и того же требования (например, при идентификации пользователей нескольких типов), то возможно повторение использования одного и того же компонента из ГОСТ Р ИСО/МЭК 15408-2 (т.е. применение к нему операции итерации), чтобы охватить каждый аспект.

   Если требования доверия к ОО включают компонент AVA_SOF.1 (например, ОУД2 и выше), то при изложении функциональных требований безопасности ОО должен устанавливаться минимальный уровень стойкости для функций безопасности, реализуемых с помощью вероятностного или перестановочного механизма (например, пароля или хэш-функции). Все подобные функции должны удовлетворять 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.

   Как составная часть оценки стойкости функций безопасности ОО (AVA_SOF.1) будут оценены 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 ГОСТ Р ИСО/МЭК 15408-3. Расширение ОУД в ЗБ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в ГОСТ Р ИСО/МЭК 15408-3.

b) Необязательное изложение **требований безопасности для среды ИТ** должно определять требования безопасности ИТ, которым должна отвечать среда ИТ этого ОО. Требования в этой части ПЗ могут быть взяты из ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 и, если так, то должна быть изменена их формулировка, чтобы четко показать, что среда ИТ, а не ОО, должна отвечать требованию. Подобное изменение формулировки является особым случаем уточнения и не является предметом требований оценки, связанных с модифицированными компонентами ГОСТ Р ИСО/МЭК 15408. Если безопасность ОО не зависит от среды ИТ, то эта часть ЗБ может быть опущена.

Отметим, что хотя **требования безопасности среды, не относящиеся к ИТ**, часто бывают полезны на практике, не требуется, чтобы они являлись формальной частью ЗБ, поскольку они не связаны непосредственно с реализацией ОО.

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

2) Все функциональные требования и требования доверия к ОО, сформулированные явным образом, должны быть четко и однозначно выражены, чтобы были возможны оценка и демонстрация соответствия им. Уровень детализации и способ выражения функциональных требований и требований доверия, принятый в ГОСТ Р ИСО/МЭК 15408, должен использоваться как образец.

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

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

B.2.7 Краткая спецификация ОО

Краткая спецификация ОО должна определить отображение требований безопасности для ОО. Эта спецификация должна предоставить описание функций безопасности и мер доверия к ОО, которые отвечают 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 следующее.

a) **Изложение функций безопасности ОО**, которое должно охватывать все функции безопасности ИТ и определять, каким образом эти функции удовлетворяют функциональным требованиям безопасности ОО. Изложение должно включать в себя двунаправленное сопоставление функций и требований с четким указанием, в удовлетворении каких требований участвует каждая функция, и что при этом удовлетворены все требования. Каждая функция безопасности должна участвовать в удовлетворении, по меньшей мере, одного функционального требования безопасности ОО.

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

2) Все ссылки в ЗБ на механизмы безопасности должны быть сопоставлены с соответствующими функциями безопасности таким образом, 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 либо 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 сделать 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 таким образом, чтобы было понятно, какие меры в удовлетворении каких требований участвуют.

Там, где это возможно, меры доверия разрешается определить путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

B.2.8 Утверждения о соответствии ПЗ

В ЗБ могут быть утверждения, что ОО соответствует требованиям одного или, возможно, нескольких ПЗ. Для каждого из имеющихся утверждений ЗБ должно включать изложение **утверждения о соответствии ПЗ**, содержащее объяснение, логическое обоснование и любые 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 ЗБ утверждения о соответствии ПЗ может быть сведено в итоге к одному из следующих вариантов.

a) Если утверждений о соответствии ПЗ нет, то следует привести полное описание целей и требований безопасности ОО, как определено в данном приложении. При этом данный раздел ЗБ опускается.

b) Если в ЗБ утверждается только о соответствии требованиям какого-либо ПЗ без необходимости их дальнейшего уточнения, то ссылки на ПЗ достаточно, чтобы определить и логически обосновать цели и требования безопасности ОО. Повторное изложение содержания ПЗ не является обязательным.

c) Если в ЗБ утверждается 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. При такой ситуации в ЗБ разрешается сослаться на эти требования, но при этом завершить операции в пределах ЗБ. В некоторых случаях, когда завершение операций приводит к существенным изменениям, может оказаться предпочтительным для ясности повторно изложить содержание ПЗ в составе ЗБ.

d) Если в ЗБ утверждается о соответствии требованиям какого-либо ПЗ, но последний расширяется путем добавления 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 некоторых случаях, когда дополнения к ПЗ существенны, может оказаться предпочтительным для ясности повторно изложить содержание ПЗ в составе ЗБ.

e) Случай, когда в ЗБ утверждается о частичном соответствии ПЗ, не приемлем для оценки в рамках ГОСТ Р ИСО/МЭК 15408.

ГОСТ Р ИСО/МЭК 15408 не содержит жестких правил предпочтения ссылки на ПЗ повторению 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 яв-

лялось 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 следующий материал для каждого ПЗ.

a) **Ссылку на ПЗ,** идентифицирующую ПЗ, соответствие которому утверждается, плюс любые дополнительные материалы, которые могут потребоваться в соответствии с этим утверждением. Обоснованное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

b) **Конкретизацию ПЗ,** идентифицирующую те 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.

B.2.9 Замечания по применению

Эта часть ЗБ не является обязательной и может содержать дополнительную информацию, которая считается уместной или полезной для понимания ЗБ. Необходимо отметить, что если в ЗБ утверждается о соответствии требованиям ПЗ, это может быть уместным, чтобы определенная информация, содержащаяся в потенциальном подразделе ПЗ «Замечания по применению», была отражена в других подразделах ЗБ. Например, информацию, касающуюся конструкции ОО, вероятно более уместно представить в краткой спецификации ОО или в разделе ЗБ «Обоснование», чем в отдельном подразделе ЗБ «Замечания по применению». Для упрощения оценки ЗБ и принимая во внимание, что структура представления ЗБ, изложенная в этом приложении, не является нормативной, замечания по применению, содержащие необходимый для оценки материал, должны быть частью подраздела ЗБ, который предоставляет свидетельство для данного аспекта оценки.

B.2.10 Обоснование

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

a) **Обоснование целей безопасности,** демонстрирующее, что изложенные цели безопасности сопоставимы 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 следующее:

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

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

3) выбор требований безопасности логически обоснован. При этом должны быть логически обоснованы:

   - выбор требований, не содержащихся в ГОСТ Р ИСО/МЭК 15408-2 или ГОСТ Р 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 для ОО.

c) **Обоснование краткой спецификации** ОО, показывающее, что функции безопасности и меры доверия к ОО пригодны, чтобы отвечать требованиям безопасности ОО. Должно быть продемонстрировано следующее:

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

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

3) логически обосновано утверждение, что изложенные меры доверия соответствуют требованиям доверия.

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. Эта часть ЗБ может быть опущена, если не сделано утверждений о соответствии ПЗ, или если цели и требования безопасности ЗБ и каждого ПЗ, соответствие которому утверждается, полностью совпадают.

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

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, March1976.

[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] ISO/IEC 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model, Part 2: Security Architecture.

[9] 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.

[11] ISO/IEC Directives, Part 2 Rules for the structure and drafting of International Standards, http://www.iec.ch/tiss/iec/Directives-Part2-Ed5.pdf

УДК 681.324:006.354 ОКС 35.040 П85 ОКСТУ 4002

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

Председатель ТК 362
начальник ГНИИИ ПТЗИ ФСТЭК России В.Г.Герасименко

Ответственный секретарь ТК 362
начальник отдела
ГНИИИ ПТЗИ ФСТЭК России Ю.Г.Кирсанов

Руководитель разработки
ведущий научный сотрудник
ООО «Центр безопасности информации» М.Т.Кобзарь