ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

Издание официальное

БЗ 5—2001/80

ГОССТАНДАРТ РОССИИ
Москва

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Центром безопасности информации, 4 ЦНИИ Министерства обороны РФ, Центром «Атомзащитаинформ», ЦНИИАТОМИНФОРМ, ВНИИстандарт при участии экспертов Международной рабочей группы по Общим критериям

ВНЕСЕН Гостехкомиссией России, Техническими комитетами по стандартизации ТК 362Р «Защита информации» и ТК 22 «Информационные технологии»

2 ПРИНЯТ И ВВЕДЕН В ДЕЙСТВИЕ Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст

3 Настоящий стандарт содержит полный аутентичный текст международного стандарта ИСО/МЭК 15408-1—99 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

4 ВВЕДЕН ВПЕРВЫЕ

© ИПК Издательство стандартов, 2002

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта России

Содержание

1 Область применения . . . 1
2 Определения . . . 2
2.1 Общие сокращения . . . 2
2.2 Область применения глоссария . . . 2
2.3 Глоссарий . . . 3
3 Краткий обзор . . . 5
3.1 Введение . . . 5
3.2 Пользователи ОК . . . 6
3.3 Контекст оценки . . . 7
3.4 Структура ОК . . . 7
4 Общая модель . . . 8
4.1 Контекст безопасности . . . 8
4.2 Подход Общих критериев . . . 10
4.3 Понятия безопасности . . . 12
4.4 Описательные возможности ОК . . . 16
4.5 Виды оценок . . . 18
4.6 Поддержка доверия . . . 19
5 Требования общих критериев и результаты оценки . . . 19
5.1 Введение . . . 19
5.2 Требования, включаемые в ПЗ и ЗБ . . . 20
5.3 Требования к ОО . . . 20
5.4 Пояснение результатов оценки . . . 20
5.5 Использование результатов оценки ОО . . . 21
Приложение А Проект общих критериев . . . 23
А.1 Предыстория . . . 23
А.2 Разработка Общих критериев . . . 23
А.3 Организации—спонсоры проекта Общих критериев . . . 23
Приложение Б Спецификация профилей защиты . . . 25
Б.1 Краткий обзор . . . 25
Б.2 Содержание профиля защиты . . . 25
Приложение В Спецификация заданий по безопасности . . . 29
В.1 Краткий обзор . . . 29
В.2 Содержание задания по безопасности . . . 29
Приложение Г Библиография . . . 34

Введение

Проблема обеспечения безопасности информационных технологий занимает все более значительное место в реализации компьютерных систем и сетей по мере того, как возрастает их роль в информатизации общества. Обеспечение безопасности информационных технологий (ИТ) представляет собой комплексную проблему, которая решается в направлениях совершенствования правового регулирования применения ИТ, совершенствования методов и средств их разработки, развития системы сертификации, обеспечения соответствующих организационно-технических условий эксплуатации. Ключевым аспектом решения проблемы безопасности ИТ является выработка системы требований, критериев и показателей для оценки уровня безопасности ИТ.

ГОСТ Р ИСО/МЭК 15408 содержит общие критерии оценки безопасности информационных технологий.

ГОСТ Р ИСО/МЭК 15408-1 устанавливает общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (утроз, предположений, политики безопасности).

ГОСТ Р ИСО/МЭК 15408-2 содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

ГОСТ Р ИСО/МЭК 15408-3 включает в себя систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. Здесь же содержатся оценочные уровни доверия, определяющие шкалу требований, которые позволяют с возрастающей степенью полноты и строгости оценить проектную, тестовую и эксплуатационную документацию, правильность реализации функций безопасности ОО, уязвимости продукта или системы ИТ, стойкость механизмов защиты и сделать заключение об уровне доверия к безопасности объекта оценки.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Часть 1

Введение и общая модель

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

Дата введения 2004—01—01

1 Область применения

ГОСТ Р ИСО/МЭК 15408 определяет критерии, за которыми исторически закрепилось название «Общие критерии» (ОК). ОК предназначены для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий (ИТ). Устанавливая общую базу критериев, ОК делают результаты оценки безопасности ИТ значимыми для более широкой аудитории.

ОК дают 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 помогут потребителям решить, являются ли продукты или системы ИТ достаточно безопасными для их предполагаемого применения и приемлемы ли прогнозируемые риски при их использовании.

ОК полезны 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.

ОК направлены 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. ОК могут быть также применены к тем аспектам безопасности ИТ, которые выходят за пределы этих трех понятий. ОК сосредоточены на угрозах информации, возникающих в результате действий человека, как злоумышленных, так и иных, но возможно также применение ОК и для некоторых угроз, не связанных с человеческим фактором. Кроме того, ОК могут быть применены и в других областях ИТ, но не декларируется их правомочность вне строго ограниченной сферы безопасности ИТ.

ОК применимы 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.

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

Издание официальное

а) ОК не содержат 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, управление персоналом, физическая защита и процедурный контроль. 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.

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

в) В ОК не рассматривается ни методология оценки, ни административно-правовая структура, в рамках которой критерии могут применяться органами оценки. Тем не менее, ожидается, что ОК будут использоваться для целей оценки в контексте такой структуры и такой методологии.

г) Процедуры использования результатов оценки при аттестации продуктов и систем ИТ находятся вне области действия ОК. 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.

д) Критерии для оценки специфических качеств криптографических алгоритмов не входят в ОК. Если требуется независимая оценка математических свойств криптографии, встроенной в ОО, то в системе оценки, в рамках которой применяются ОК, необходимо предусмотреть проведение таких оценок.

2 Определения

2.1 Общие сокращения

Следующие сокращения являются общими для всех частей ОК.

ЗБ (ST)	Задание по безопасности
ИТ (IT)	Информационная технология
ИФБО (TSFI)	Интерфейс ФБО
ОДФ (TSC)	Область действия ФБО
ОК (CC)	Общие критерии, исторически сложившееся название, часто используемое в ГОСТ Р ИСО/МЭК 15408 вместо его официального названия «Критерии оценки безопасности информационных технологий»
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

2.2 Область применения глоссария

Подраздел 2.3 содержит только те термины, которые используются во всем тексте ОК особым образом. Большинство терминов в ОК 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 ОК и не вошедшие в глоссарий, объясняются непосредственно в тексте по месту использования. Объяснение терминов и понятий, применяемых особым образом в ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3, можно найти в подразделе «Парадигма» соответствующего стандарта.

2.3 Глоссарий

В ГОСТ Р ИСО/МЭК 15408 применяются следующие термины.

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

атрибут безопасности: Информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления ПБО. **security attribute**

аутентификационные данные: Информация, используемая для верифика- ции предъявленного идентификатора пользователя. **authentication data**

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

внешний объект ИТ: Любые продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним. **external IT entity**

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

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

высокая СФБ: 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. **SOF-high**

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

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

доверенный канал: Средство взаимодействия между ФБО и удаленным до- веренным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО. **trusted channel**

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

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

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

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

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

интерфейс функций безопасности ОО: 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. **TOE security functions interface**

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

класс: Группа семейств, объединенных общим назначением. **class**

компонент: Наименьшая выбираемая совокупность элементов, которая может быть включена в ПЗ, ЗБ или пакет. **component**

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

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

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

назначение: Спецификация определенного параметра в компоненте. **assignment**

неформальный: Выраженный на естественном языке. **informal**

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

объект: Сущность в пределах ОДФ, которая содержит или получает информацию и над которой субъекты выполняют операции. **object**

объект оценки: Подлежащие оценке продукт ИТ или система с руководствами администратора и пользователя. **target of evaluation**

орган оценки: Организация, которая посредством системы оценки обеспечивает реализацию ОК для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества. **evaluation authority**

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

оценочный уровень доверия: Пакет компонентов доверия из части 3 ОК, представляющий некоторое положение на предопределенной в ОК шкале доверия. **evaluation assurance level**

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

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

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

передача между ФБО: Передача данных между ФБО и функциями безопасности других доверенных продуктов ИТ. **inter-TSF transfers**

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

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

политика функции безопасности: Политика безопасности, осуществляемая ФБ. **security function policy**

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

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

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

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

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

расширение: Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в части 2 ОК, и/или требований доверия, не содержащихся в части 3 ОК. **extension**

ресурс ОО: Все, что может использоваться или потребоваться в ОО. **TOE resource**

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

связность: Свойство ОО, позволяющее ему взаимодействовать с объектами 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. **connectivity**

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

семейство: Группа компонентов, которые объединены одинаковыми целями безопасности, но могут отличаться акцентами или строгостью. **family**

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

система оценки: Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ОК. **evaluation scheme**

средняя СФБ: 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. **SOF-medium**

стойкость функции безопасности: 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. **strength of function**

субъект: Сущность в пределах ОДФ, которая инициирует выполнение операций. **subject**

уполномоченный пользователь: Пользователь, которому в соответствии с ПБО разрешено выполнять какую-либо операцию. **authorised user**

усиление: Добавление одного или нескольких компонентов доверия из части 3 ОК в ОУД или пакет требований доверия. **augmentation**

уточнение: Добавление деталей в компонент. **refinement**

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

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

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

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

цель безопасности: Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности органи- зации и предположениям. **security objective**

элемент: Неделимое требование безопасности. **element**

3 Краткий обзор

В этом разделе представлены основные концептуальные положения ОК, определены категории лиц, для которых предназначены ОК, контекст оценки и способ представления материала.

3.1 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 их функций следует осуществлять надлежащий контроль информации, что обеспечило бы ее защиту от опасностей типа нежелательного или неоправданного распространения, изменения или потери. Термин «безопасность ИТ» охватывает 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).

ОК могут использоваться для выбора приемлемых мер безопасности ИТ. В них содержатся критерии оценки требований безопасности.

3.2 Пользователи ОК

В оценке характеристик безопасности продуктов и систем ИТ заинтересованы в основном потребители, разработчики и оценщики. Представленные критерии структурированы в интересах этих групп, потому что именно они рассматриваются как основные пользователи ОК. В последующих пунктах объясняется, какую пользу могут принести критерии каждой из этих групп.

3.2.1 Потребители

ОК играют важную роль в методической поддержке выбора потребителями требований безопасности ИТ для выражения своих потребностей. ОК написаны, чтобы обеспечить посредством оценки удовлетворение запросов потребителей, поскольку это является основной целью и 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.

ОК предоставляют 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.

3.2.2 Разработчики

ОК предназначены 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 ОК методологии оценки, потенциально сопровождаемой соглашением о взаимном признании результатов оценки, позволит к тому же использовать ОК для поддержки иных лиц, помимо разработчиков ОО, при подготовке этого ОО к оценке и содействии в ее проведении.

Конструкции из ОК 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 ОК описаны функции безопасности, которые разработчик мог бы включить в ОО. ОК можно использовать для определения обязанностей и действий по подготовке свидетельств, необходимых при проведении оценки ОО. Они также определяют содержание и представление таких свидетельств.

3.2.3 Оценщики

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

3.2.4 Прочие

Хотя ОК ориентированы на определение и оценку характеристик безопасности ИТ для объектов оценки, они также могут 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 ОК:

а) лица, ответственные за техническое состояние оборудования, и сотрудники служб безопас-

ности, ответственные за определение и выполнение политики и требований безопасности организации в области ИТ;

б) аудиторы как внутренние, так и внешние, ответственные за оценку адекватности безопасности системы;

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

г) аттестующие, ответственные за приемку системы ИТ в эксплуатацию в конкретной среде;

д) заявители, заказывающие оценку и обеспечивающие ее проведение;

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

3.3 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 ОК не излагаются требования к правовой базе. Однако согласованность правовой базы различных органов оценки является необходимым условием достижения взаимного признания результатов оценок. На рисунке 3.1 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 сертификация 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 ОК.

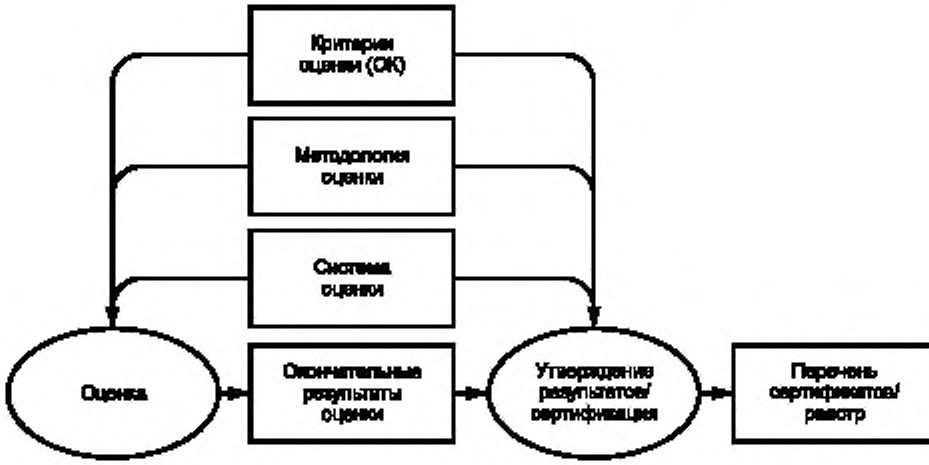

Рисунок 3.1 — Контекст оценки

3.4 Структура ОК

ОК состоит из нескольких отдельных, но взаимосвязанных частей, перечисленных ниже. Термины, используемые при описании отдельных частей ОК, приведены в разделе 4.

а) **Часть 1 «Введение и общая модель»** является введением в ОК. 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 ОК применительно к каждой из основных групп пользователей ОК.

б) **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.

в) **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 ОК шкалу ранжирования доверия к ОО.

Предполагается, что в поддержку частей ОК, перечисленных выше, будут опубликованы и документы других типов, включая нормативно-методические материалы и руководства.

В таблице 3.1 показано, в каком качестве различные части ОК будут представлять интерес для каждой из трех основных групп пользователей ОК.

Таблица 3.1 — Путеводитель по Общим критериям

Часть ОК	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 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

4 Общая модель

В этом разделе представлены общие понятия, используемые во всех частях ОК, включая контекст использования этих понятий, и подход ОК к их применению. Части 2 и 3 ОК 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 ОК с использованием совокупности понятий безопасности и терминологии. Их понимание является предпосылкой эффективного использования ОК. Однако сами по себе эти понятия имеют самый общий характер и не должны ограничивать класс проблем безопасности ИТ, к которым применимы ОК.

4.1 Контекст безопасности

4.1.1 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 4.1 иллюстрирует высокоуровневые понятия безопасности и их взаимосвязь.

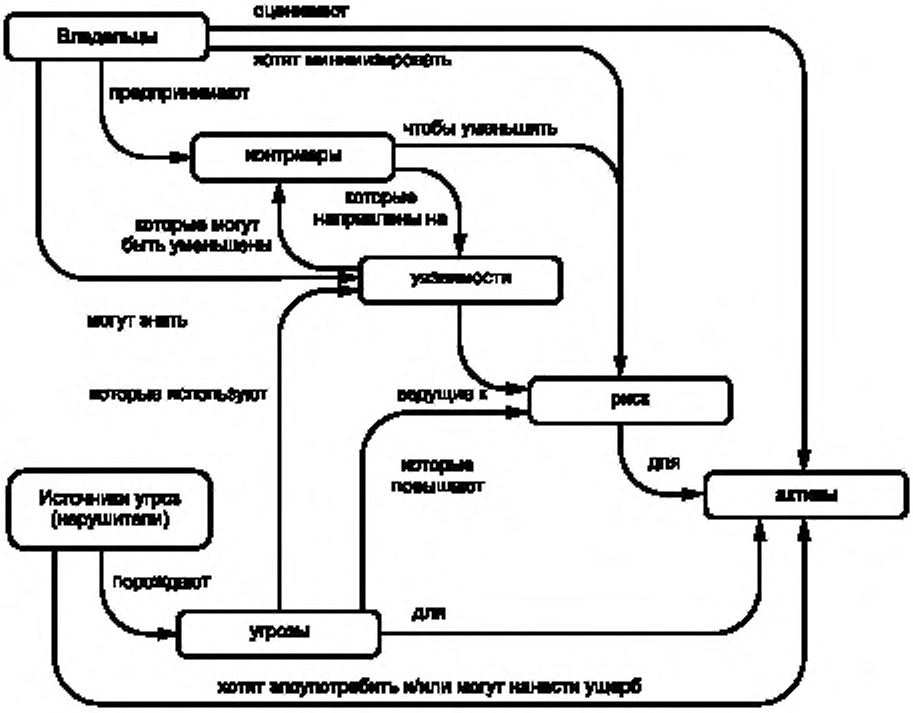

Рисунок 4.1 — Понятия безопасности и их взаимосвязь

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 получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Владельцы активов будут анализировать возможные угрозы, чтобы решить, какие из них действительно присущи их среде. В результате анализа определяются 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, задавая дополнительные ограничения.

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 4.2 иллюстрирует эту взаимосвязь.

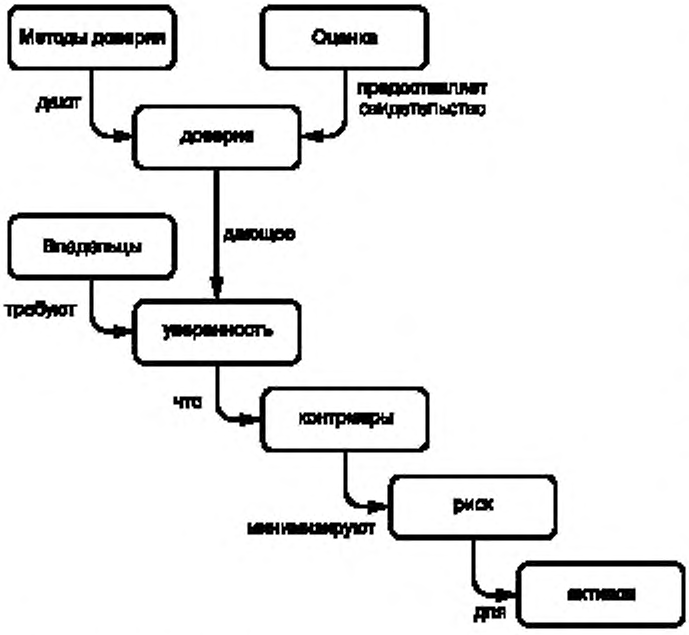

Рисунок 4.2 — Понятия, используемые при оценке, и их взаимосвязь

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 правомерными. Следовательно, оценка должна приводить к объективным и повторяемым результатам, что позволит использовать их в качестве свидетельства.

4.1.2 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 специальные средства контроля для противостояния угрозам данным как часть всей совокупности контрмер безопасности.

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.

4.2 Подход Общих критериев

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

4.2.1 Разработка

ОК не предписывают конкретную методологию разработки или модель жизненного цикла. На рисунке 4.3 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.

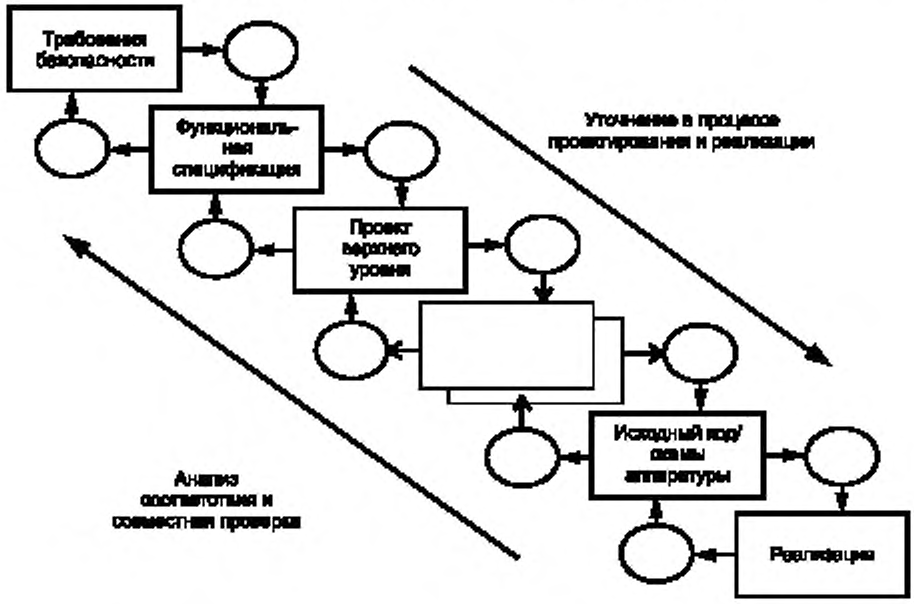

Рисунок 4.3 — Модель разработки ОО

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.

ОК не предписывают конкретную совокупность представлений проекта. В ОК требуется, чтобы имелось достаточное число представлений с достаточным уровнем детализации для демонстрации, если потребуется, того, что:

а) каждый уровень уточнения полностью отображает более высокие уровни (все функции, характеристики и режимы безопасности ОО, которые определены на более высоком уровне абстракции, необходимо наглядно представить на более низком уровне);

б) каждый уровень уточнения точно отображает более высокие уровни (не следует иметь 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 ОК 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 ОК.

4.2.2 Оценка ОО

Процесс оценки ОО, как показано на рисунке 4.4, может проводиться параллельно с разработкой или следом за ней. Основными исходными материалами для оценки ОО являются:

а) совокупность свидетельств, характеризующих ОО, включая прошедшее оценку ЗБ в качестве основы оценки ОО;

б) ОО, безопасность которого требуется оценить;

в) критерии, методология и система оценки.

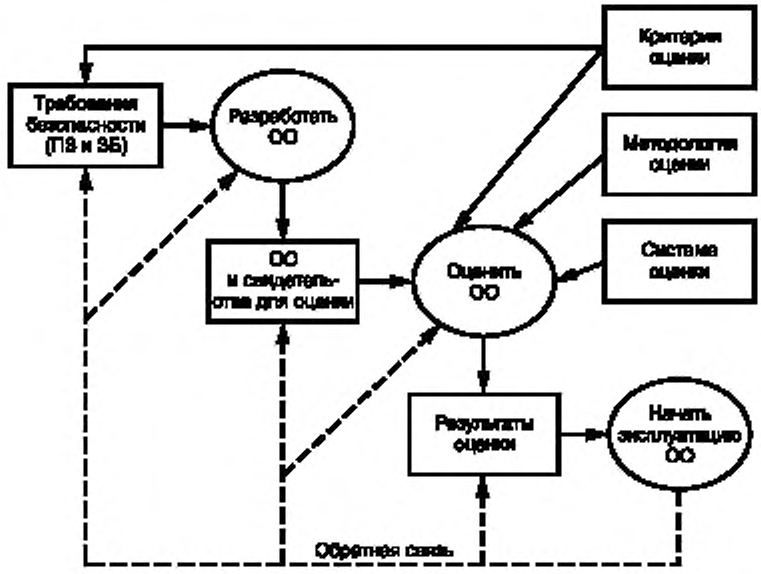

Рисунок 4.4 — Процесс оценки ОО

Кроме того, в качестве исходных материалов для оценки возможно также использование вспомогательных материалов (таких, как замечания по применению ОК) и специальных знаний в области безопасности ИТ, которыми располагают 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 эксплуатации. Кроме того, готовясь к строгой оценке, разработчик, возможно, более внимательно отнесется к проектированию и разработке ОО. Поэтому процесс оценки может оказывать значительное, хотя и косвенное, положительное влияние на начальные требования, процесс разработки, конечный продукт и условия его эксплуатации.

4.2.3 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. Хотя ОК содержат критерии, предусматривающие поддержку доверия, детальное описание процедур переоценки, включая использование результатов ранее проведенных оценок, выходит за рамки ОК.

4.3 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 могли бы применяться ОК.

ОК применимы, 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 ОК требуется, чтобы определенные уровни представления содержали логическое 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 логического обоснования, демонстрирующее согласованность со смежным более высоким уровнем представления, приводится как довод корректности ОО. Логическое обоснование, непосредственно демонстрирующее соответствие целям безопасности, поддерживает доводы об эффективности ОО в противостоянии угрозам и осуществлении политики безопасности организации.

В ОК используются различные формы представления, что показано на рисунке 4.5, 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.

4.3.1 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:

а) 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;

б) 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;

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

На основании исследования политик безопасности, угроз и рисков следует сформировать материалы, относящиеся к безопасности ОО;

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

д) изложение угроз безопасности активов, в котором были бы идентифицированы все угрозы, прогнозируемые на основе анализа безопасности как относящиеся к ОО. В ОК 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;

е) 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.

4.3.2 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. Необходимо,

чтобы цели безопасности были согласованы с определенными ранее целями применения или предназначением ОО как продукта, а также со всеми известными сведениями о физической среде ОО.

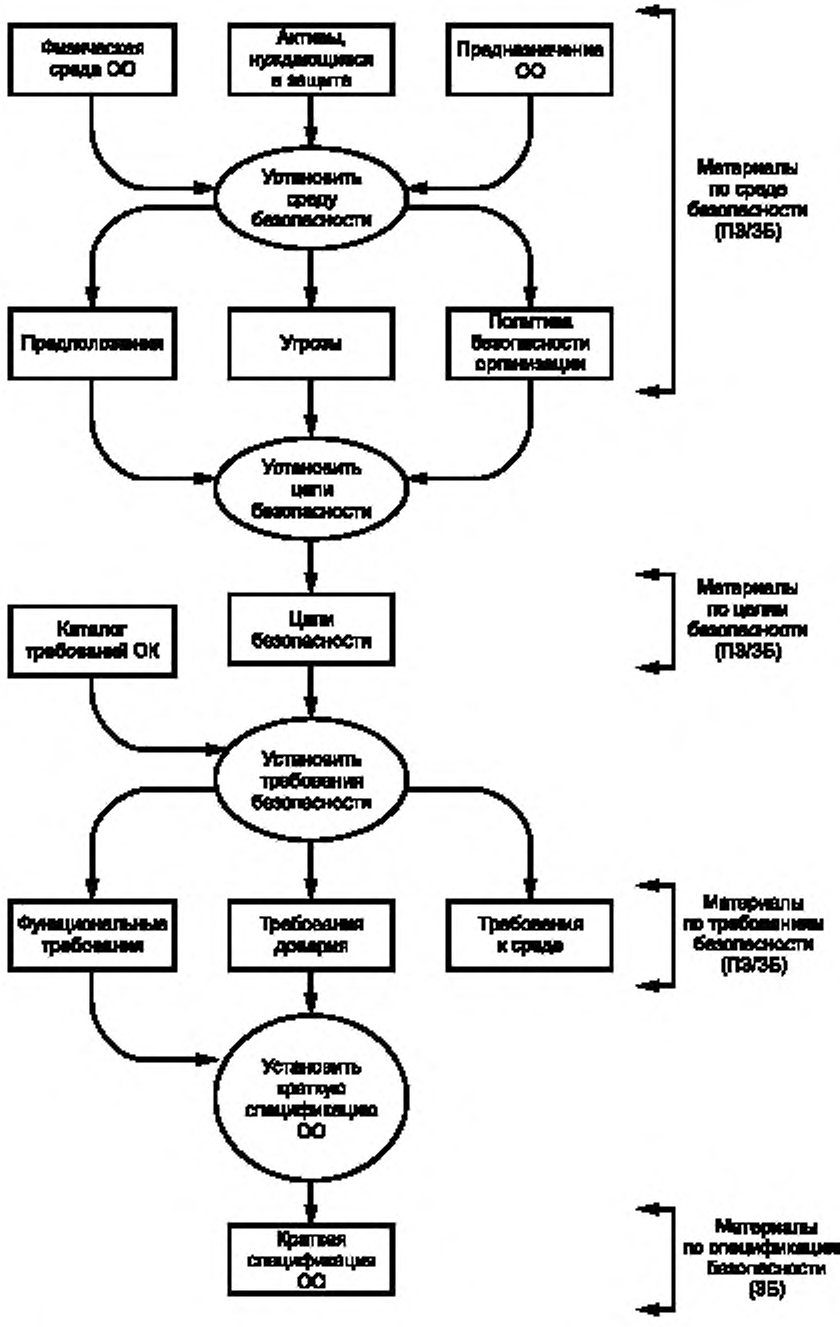

Рисунок 4.5 — Последовательное формирование требований и спецификаций

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 ООО 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.

4.3.3 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 ОК 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 части 2 ОК. 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. Часть 3 ОК 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:

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

б) 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 логического обоснования представляет дополнительную поддержку утверждению об отсутствии нежелательного режима.

4.3.4 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.

4.3.5 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.

4.4 Описательные возможности ОК

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

4.4.1 Представление требований безопасности

ОК определяют 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 4.6.

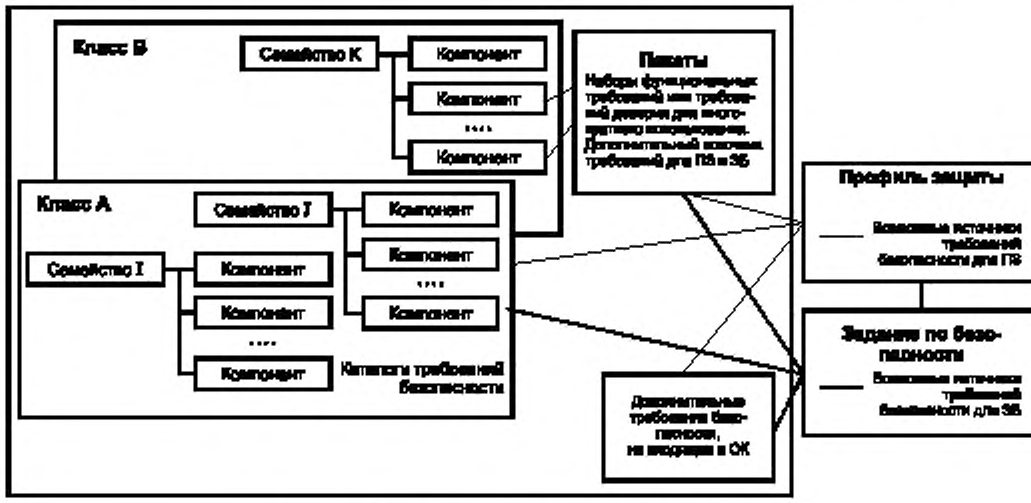

Рисунок 4.6 — Организация и структура требований

Организация требований безопасности в ОК в виде иерархии класс — семейство — компонент призвана помочь потребителям в поиске конкретных требований безопасности.

Функциональные требования и требования доверия представлены в ОК в едином стиле с использованием одной и той же структуры и терминологии.

4.4.1.1 *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.

4.4.1.2 *Семейство*

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

Составляющие семейства называются компонентами.

4.4.1.3 *Компонент*

Компонент описывает специфический набор требований безопасности, который является наименьшим выбираемым набором требований безопасности для включения в структуры, определенные в ОК. 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.

4.4.1.4 *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 ОК. Чтобы обеспечить полноту требований к ОО, следует удовлетворить, где это необходимо, зависимости всех компонентов при их включении в ПЗ и ЗБ.

4.4.1.5 *Разрешенные операции на компонентах*

Компоненты ОК можно использовать точно так, как они сформулированы в ОК, или же можно их конкретизировать, применяя разрешенные операции для выполнения определенной политики безопасности или для противостояния определенной угрозе. Для каждого компонента ОК идентифицируют и определяют все разрешенные операции назначения и выбора, условия применения операции к компоненту и возможные результаты применения операции. Операции итерации и уточнения могут выполняться для любого компонента. Указанные четыре операции определены следующим образом:

а) **итерация** (iteration), позволяющая неоднократно использовать компонент при различном выполнении в нем операций;

б) **назначение** (assignment), позволяющее специфицировать параметр, устанавливаемый при использовании компонента;

в) **выбор** (selection), позволяющий специфицировать пункты, которые выбираются из перечня, приведенного в компоненте;

г) **уточнение** (refinement), позволяющее осуществлять дополнительную детализацию при использовании компонента.

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

4.4.2 Использование требований безопасности

В ОК определены три типа конструкций требований: пакет, ПЗ и ЗБ. Помимо этого, в ОК определена совокупность критериев безопасности ИТ, которые могут отвечать потребностям многих сообществ пользователей и поэтому служат основным исходным материалом для создания этих конструкций. Центральной идеей ОК является концепция максимально широкого использования определенных в ОК компонентов, которые представляют хорошо известную и понятную сферу применимости. Рисунок 4.7 показывает взаимосвязь между различными конструкциями.

4.4.2.1 *Пакет*

Промежуточная комбинация компонентов называется пакетом. Пакет позволяет выразить

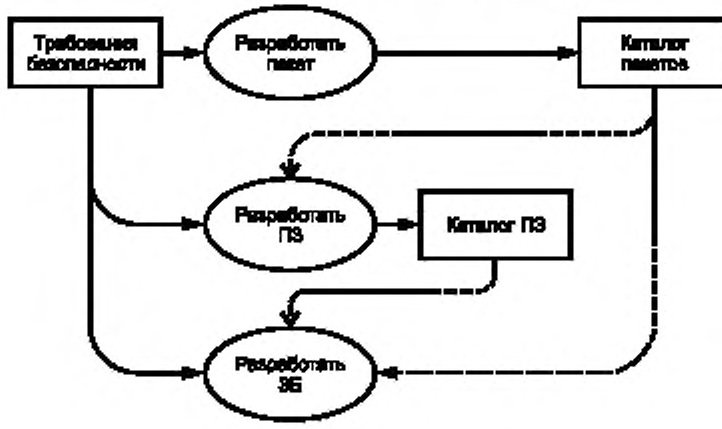

Рисунок 4.7 — Использование требований безопасности

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 части 3 ОК. ОУД является базовым набором требований доверия для оценки. Каждый ОУД определяет непротиворечивый набор требований доверия. Совместно ОУД формируют упорядоченное множество, которое является предопределенной в ОК шкалой доверия.

4.4.2.2 *Профиль защиты*

ПЗ содержит совокупность требований безопасности, взятых из ОК 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 логическое обоснование требований и целей безопасности.

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

4.4.2.3 *Задание по безопасности*

ЗБ содержит совокупность требований безопасности, которые могут быть определены ссылками на ПЗ, непосредственно на функциональные компоненты или компоненты доверия из ОК 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 логическим обоснованием для каждого из них. ЗБ является основой для соглашения между всеми сторонами относительно того, какую безопасность предлагает ОО.

4.4.3 Источники требований безопасности

Требования безопасности ОО могут быть скомпонованы с использованием следующих источников:

а) существующих ПЗ: требования безопасности ОО в ЗБ могут быть адекватно выражены непосредственно через требования, содержащиеся в существующем ПЗ, или предполагать согласованные с ними;

Существующие ПЗ можно использовать как основу для создания нового ПЗ;

б) 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 части 3 ОК. В требования доверия к ОО, входящие в ПЗ или ЗБ, следует включить какой-либо ОУД из этой части;

в) существующих компонентов функциональных требований или требований доверия: функциональные требования или требования доверия в ПЗ или ЗБ могут быть выражены непосредственно через компоненты, приведенные в частях 2 или 3 ОК;

г) расширенных требований: в ПЗ или ЗБ могут быть использованы дополнительные функциональные требования, не содержащиеся в части 2 ОК, и/или дополнительные требования доверия, не содержащиеся в части 3 ОК.

Материалы имеющихся требований из частей 2 и 3 ОК следует использовать всюду, где только возможно. Использование существующего ПЗ поможет обеспечить выполнение объектом оценки апробированной совокупности требований известной полезности и, как следствие, более широкое признание ОО.

4.5 Виды оценок

4.5.1 Оценка ПЗ

Оценка ПЗ выполняется согласно критериям оценки ПЗ, содержащимся в части 3 ОК. Целью такой оценки является продемонстрировать, что профиль полон, непротиворечив, технически правилен и пригоден для использования при изложении требований к ОО, предполагаемому для оценки.

4.5.2 Оценка ЗБ

Оценка ЗБ для ОО выполняется согласно критериям оценки ЗБ, содержащимся в части 3 ОК. 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.

4.5.3 Оценка ОО

Оценка ОО производится согласно критериям оценки, содержащимся в части 3 ОК, с использованием в качестве основы ЗБ, прошедшего оценку. Цель такой оценки — продемонстрировать, что ОО отвечает требованиям безопасности, содержащимся в ЗБ.

4.6 Поддержка доверия

Поддержка доверия к ОО осуществляется в соответствии с критериями оценки из части 3 ОК с использованием предварительно оцененного ОО в качестве основы. Цель состоит в том, чтобы убедиться, что доверие к ОО, установленное ранее, поддерживается и что ОО будет продолжать отвечать требованиям безопасности после внесения изменений в него или в его среду.

5 Требования общих критериев и результаты оценки

5.1 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. Однако ЗБ дает промежуточные результаты, которые затем используются при оценке ОО.

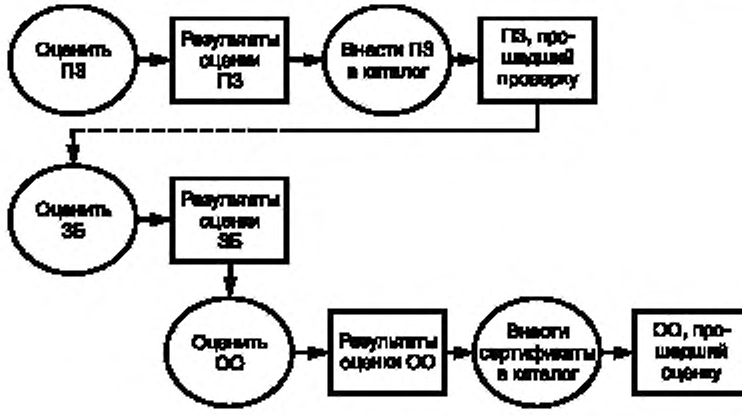

Рисунок 5.1 — Результаты оценки

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 ОК, 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.

5.2 Требования, включаемые в ПЗ и ЗБ

В ОК определена совокупность критериев безопасности ИТ, которая может отвечать потребностям многих сообществ пользователей. ОК разработаны, 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 части 2 ОК, ОУД и компонентов доверия из части 3 ОК, поскольку они представляют хорошо известную и понятную сферу применимости.

В ОК допускается возможность, 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:

а) 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 ОК;

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

в) включение, при необходимости, в состав ПЗ или ЗБ расширенных функциональных требований или требований доверия должно соответствовать требованиям классов APE или ASE из части 3 ОК.

5.2.1 Результаты оценки ПЗ

ОК содержат критерии оценки, позволяющие оценщику установить, является ли ПЗ полным, непротиворечивым, технически правильным и, следовательно, пригодным для изложения требований к ОО, предполагаемому для оценки.

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

5.3 Требования к ОО

ОК содержат критерии оценки, которые позволяют оценщику решить, удовлетворяет ли ОО требованиям безопасности, выраженным в ЗБ. Используя ОК при оценке ОО, оценщик сможет прийти к выводам:

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

б) правильно ли реализованы специфицированные функции безопасности ОО.

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

Однако может возникнуть потребность, чтобы ОО отвечал требованиям безопасности, непосредственно не выраженным в ОК. В ОК признается необходимость оценки подобных ОО, но, поскольку дополнительные требования лежат вне известной сферы применимости ОК, 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 ОК. Описание безопасности ОО в терминах ОК дает возможность сравнения характеристик безопасности различных ОО.

5.3.1 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.

5.4 Пояснение результатов оценки

При положительном результате оценки должна быть указана степень, с которой можно доверять тому, что ПЗ или ОО соответствуют требованиям ОК. Должно поясняться соотношение с функциональными требованиями из части 2 ОК, требованиями доверия из части 3 ОК или же непосредственно с ПЗ, как это указано ниже:

а) **соответствие части 2** — ПЗ или ОО соответствует части 2, если функциональные требования основаны только на функциональных компонентах из части 2;

б) **расширение части 2** — ПЗ или ОО соответствует расширению части 2, если функциональные требования включают функциональные компоненты, не содержащиеся в части 2;

в) **соответствие части 3** — ПЗ или ОО соответствует части 3, если требования доверия представлены в виде **ОУД** из части 3 или **пакета требований доверия**, включающего только компоненты доверия из части 3;

г) **усиление части 3** — ПЗ или ОО соответствует усилению части 3, если требования доверия представлены в виде **ОУД** или **пакета требований доверия** и включают другие компоненты доверия из части 3;

д) **расширение части 3** — ПЗ или ОО соответствует расширению части 3, если требования доверия представлены в виде **ОУД**, дополненного требованиями доверия не из части 3, или **пакета требований доверия,** который включает требования доверия, не содержащиеся в части 3, или полностью состоит из них;

е) **соответствие ПЗ** — ОО соответствует ПЗ только в том случае, если он соответствует всем частям этого ПЗ.

5.5 Использование результатов оценки ОО

Продукты и системы ИТ отличаются в отношении использования результатов оценки. На рисунке 5.2 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.

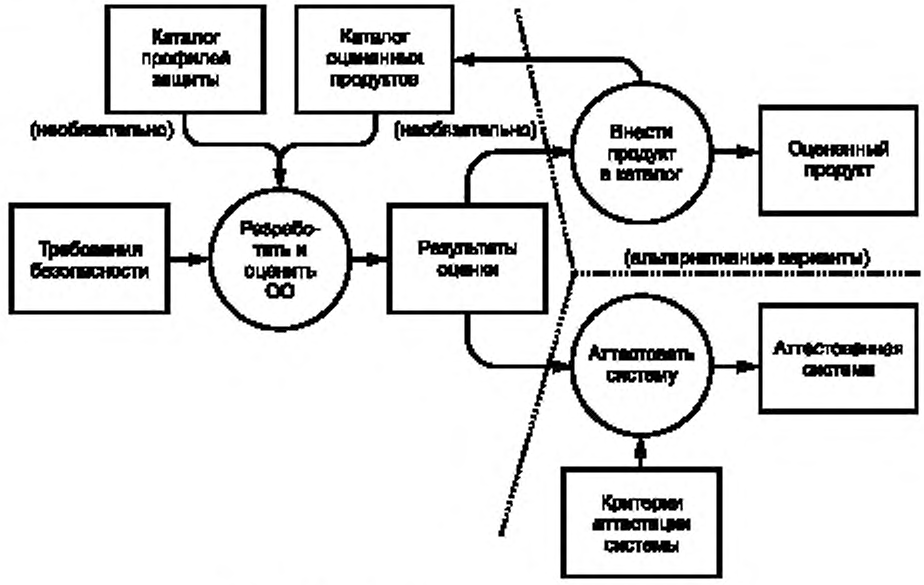

Рисунок 5.2 — Использование результатов оценки ОО

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 (аннотация) 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 ОК, могут быть учтены аттестующим при применении принятых в организации критериев аттестации, требующих оценки по ОК. Результаты оценки по ОК являются частью исходных данных для процесса аттестации, ведущего к принятию решения о приемлемости риска эксплуатации системы.

ПРИЛОЖЕНИЕ А
(справочное)

Проект Общих критериев

А.1 Предыстория

ОК представляют собой результат последовательных усилий по разработке критериев оценки безопасности ИТ, которые были бы полезны международному сообществу. В начале 80-х годов в США были разработаны «Критерии оценки доверенных компьютерных систем» (TCSEC). В следующем десятилетии различные страны проявили инициативу по разработке критериев оценки, которые строились на концепциях TCSEC, но были более гибки и адаптируемы к природе эволюции ИТ в целом.

В Европе в 1991 г. Европейской Комиссией были опубликованы «Критерии оценки безопасности информационных технологий» (ITSEC) версии 1.2, разработанные совместно Францией, Германией, Нидерландами и Великобританией. В Канаде на основе сочетания подходов TCSEC и ITSEC в начале 1993 г. были созданы «Канадские критерии оценки доверенных компьютерных продуктов» (CTCPEC) версии 3.0. В США в это же время был издан проект стандарта «Федеральные критерии безопасности информационных технологий» (FC) версии 1.0, использовавший другой подход к объединению североамериканской и европейской концепций критериев оценки.

В 1990 г. Международной организацией по стандартизации (ISO) была начата разработка международного стандарта критериев оценки для общего использования. Новые критерии были призваны удовлетворить потребность взаимного признания результатов стандартизованной оценки безопасности на мировом рынке ИТ. Эта задача была поставлена перед Рабочей группой 3 (WG3) подкомитета 27 (SC27) Совместного технического комитета 1 (JTC1). Вначале работа WG3 шла медленно из-за большого объема и необходимости интенсивных многосторонних переговоров.

А.2 Разработка Общих критериев

В июне 1993 г. организации—спонсоры CTCPEC, FC, TCSEC и ITSEC (указанные в следующем подразделе) объединили свои усилия и начали действовать совместно, чтобы согласовать различающиеся между собой критерии и создать единую совокупность критериев безопасности ИТ, которые могли бы широко использоваться. Эта деятельность получила название «Проект ОК». Его целью являлось устранение концептуальных и технических различий между исходными критериями и представление в ISO полученных результатов для содействия разработке международного стандарта. Представители организаций-спонсоров сформировали Редакционный совет ОК (CCEB) для разработки ОК. Затем было установлено взаимодействие между CCEB и WG3, после чего CCEB представил в WG3 несколько ранних версий ОК. Начиная с 1994 г. в результате взаимодействия между WG3 и CCEB эти версии оформлялись как последовательные рабочие проекты различных частей критериев ISO.

Версия 1.0 ОК была завершена CCEB в январе 1996 г. и одобрена ISO в апреле 1996 г. для распространения в качестве Проекта комитета. Был проведен ряд экспериментальных оценок на основе версии 1.0 ОК, а также организовано широкое публичное обсуждение документа. Затем в рамках Проекта ОК была предпринята значительная переработка ОК на основе замечаний, полученных при его экспериментальном использовании, публичном обсуждении и взаимодействии с ISO. Переработка документа была выполнена преемником CCEB, который в настоящее время называется Советом по реализации ОК (CCIB).

CCIB завершил бета-версию 2.0 ОК в октябре 1997 г. и представил ее в WG3, которая одобрила ее как Второй проект комитета. Последующие промежуточные версии проекта предоставлялись неофициально экспертам WG3 по мере их подготовки в CCIB. CCIB учел ряд замечаний, которые были получены как непосредственно от экспертов WG3, так и от национальных органов ISO при обсуждении промежуточных версий проекта. Кульминацией этого процесса явилась публикация версии 2.0 ОК.

По историческим причинам и с целью обеспечения преемственности ISO/IEC/JTC1/SC27/WG3 приняла для дальнейшего использования термин «Общие критерии» (ОК) внутри документа, признавая, что его официальным названием, принятым в ISO, является «Критерии оценки безопасности информационных технологий».

А.3 Организации—спонсоры проекта Общих критериев

Семь перечисленных ниже европейских и североамериканских организаций являются спонсорами проекта ОК. Эти организации почти полностью обеспечили разработку ОК от ее начала до завершения. Эти организации являются также «органами оценки» для своих национальных правительств. Они обязались заменить свои аналогичные критерии версией 2.0 ОК, когда техническая работа над ней была завершена и наступила финальная стадия ее принятия в качестве международного стандарта.

КАНАДА

Communications Security Establishment
Criteria Coordinator
12A Computer and Network Security
P.O. Box 9703, Terminal Ottawa, Canada K1G 3Z4
Tel: +1.613.991.7882, Fax: +1.613.991.7455
E-mail: gost.e-ecolog.ru
WWW:gost.e-ecolog.ru
FTP: ftp://ftp.cse-cst.gc.ca/pub/criteria/CC2.0

ФРАНЦИЯ

Service Central de la Sécurité des Systémes
d'Information (SCSSI)
Centre de Certification de la Sécurité des Technologies
de l'Information
18, rue du docteur Zamenhof
F-92131 Issy les Moulineaux France
Tel: +33.1.41463784, Fax: +33.1.41463701
E-mail: gost.e-ecolog.ru

ГЕРМАНИЯ

Bundesamt für Sicherheit in der Informationstechnik
(BSI)
German Information Security Agency (GISA)
Abteilung V
Postfach 20 03 63 D-53133 Bonn Germany
Tel: +49.228.9582.300, Fax: +49.228.9582.427
E-mail: gost.e-ecolog.ru
WWW: gost.e-ecolog.ru

НИДЕРЛАНДЫ

Netherlands National Communications Security Agency
P.O. Box 20061
NL 2500 EB The Hague The Netherlands
Tel: +31.70.3485637, Fax: +31.70.3486503
E-mail: gost.e-ecolog.ru
WWW: gost.e-ecolog.ru

ВЕЛИКОБРИТАНИЯ

Communications-Electronics Security Group
Compusec Evaluation Methodology
P.O. Box 144 Cheltenham GL52 5UE United Kingdom
Tel: +44.1242.221.491 ext. 5257, Fax: +44.1242.252.291
E-mail: gost.e-ecolog.ru
WWW: gost.e-ecolog.ru
FTP: ftp://ftp.cesg.gov.uk/pub

США (Национальный институт стандартов и технологий)

National Institute of Standards and Technology Computer
Security Division
820 Diamond, MS: NN426
Gaithersburg, Maryland 20899 U.S.A.
Tel: +1.301.975.2934, Fax: +1.301.948.0279
E-mail:gost.e-ecolog.ru
WWW: gost.e-ecolog.ru

США (Агентство национальной безопасности)

National Security Agency
Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755-6740 U.S.A.
Tel: +1.410.859.4458, Fax: +1.410.684.7512
E-mail: gost.e-ecolog.ru
WWW: gost.e-ecolog.ru

ПРИЛОЖЕНИЕ Б
(обязательное)

Спецификация профилей защиты

Б.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 4 ГОСТ Р ИСО/МЭК 15408-3 эти требования приведены в форме компонентов доверия, которые следует использовать при оценке ПЗ.

Б.2 Содержание профиля защиты

Б.2.1 Содержание и представление

ПЗ должен соответствовать требованиям к содержанию, изложенным в данном приложении. ПЗ следует представить как ориентированный на пользователя документ с минимумом ссылок на другие материалы, которые могут быть недоступны пользователю этого ПЗ. Логическое обоснование, при необходимости, может быть оформлено отдельно.

Содержание ПЗ представлено на рисунке Б.1, который следует использовать при создании структурной схемы разрабатываемого ПЗ.

Б.2.2 Введение ПЗ

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

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

б) **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.

Б.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.

Б.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 в себя следующее.

а) 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.

б) 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 описать через такие аспекты, как компетентность, доступные ресурсы и мотивация. Нападение следует описать 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.

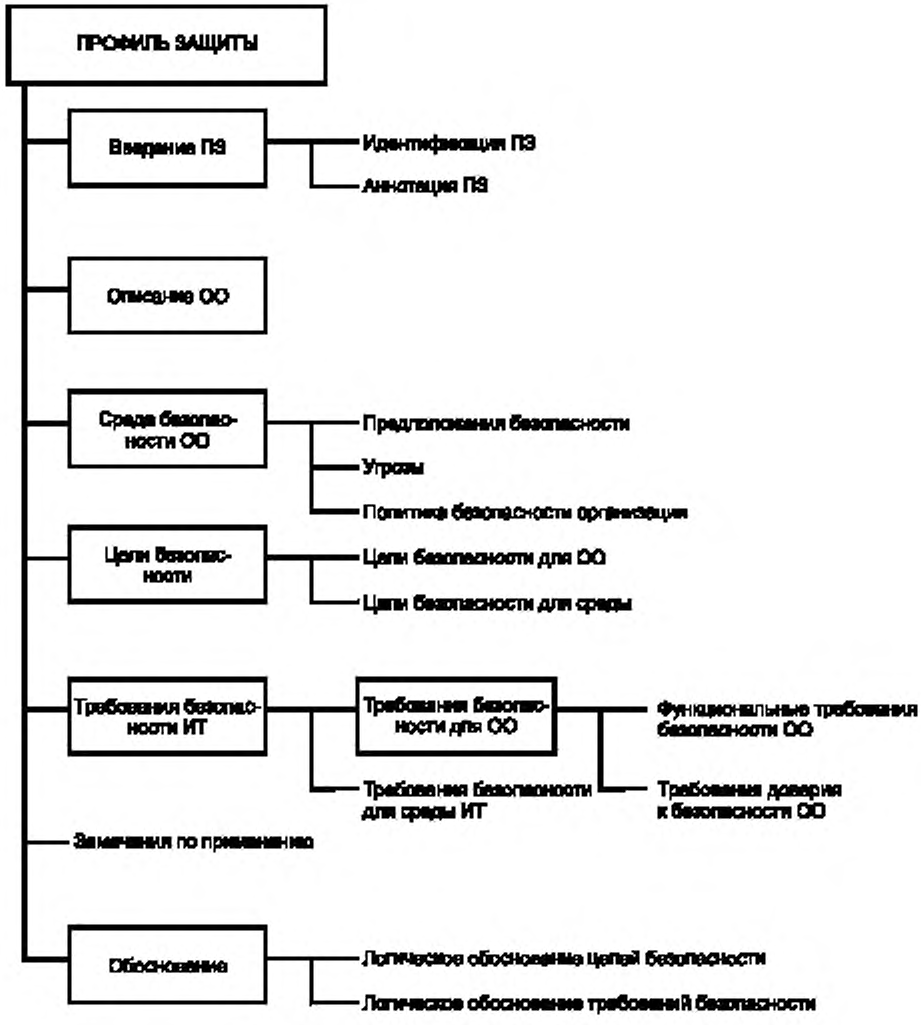

Рисунок Б.1 — Содержание профиля защиты

в) 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.

Б.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. 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.

а) **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.

б) **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.

Б.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.

а) 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, как функциональные компоненты, выбираемые из части 2 ОК.

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 части 2 ОК (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 определить их как один из ОУД, возможно, усиленный другими компонентами доверия из части 3 ОК. Расширение ОУД в ПЗ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в этой части.

б) Необязательное изложение **требований безопасности для среды ИТ** должно определять требования безопасности ИТ, которым должна отвечать среда ИТ этого ОО. 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 ПЗ, поскольку они не связаны непосредственно с реализацией ОО.

в) 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 частей 2 и 3 ОК. Если при формировании всех либо части требований не применимы компоненты из частей 2 или 3, то в ПЗ допускается сформулировать необходимые требования безопасности явным образом, без ссылки на содержание ОК.

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 ОК, должны 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.

Б.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.

Б.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 в себя следующее.

а) **Логическое обоснование целей безопасности**, демонстрирующее, что изложенные цели безопасности сопоставлены со всеми идентифицированными аспектами среды безопасности ОО и пригодны для их охвата.

б) **Логическое 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 строго обоснован. Каждое из перечисленных ниже условий должно быть строго обосновано:

- выбор требований, не содержащихся в частях 2 или 3 ОК,
- 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 5 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

ЗБ должно соответствовать требованиям к содержанию, изложенным в данном приложении. ЗБ следует представить в виде ориентированного на пользователя документа с минимумом ссылок на другие материалы, которые могут быть недоступны пользователю этого ЗБ. Логическое обоснование, при необходимости, может быть оформлено отдельно.

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

В.2.2 Введение ЗБ

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

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

б) **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;

в) **утверждение о соответствии ОК** должно изложить каждое поддающееся оценке утверждение о соответствии ОО общим критериям, как указано в подразделе 5.4.

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 в себя следующее.

а) 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.

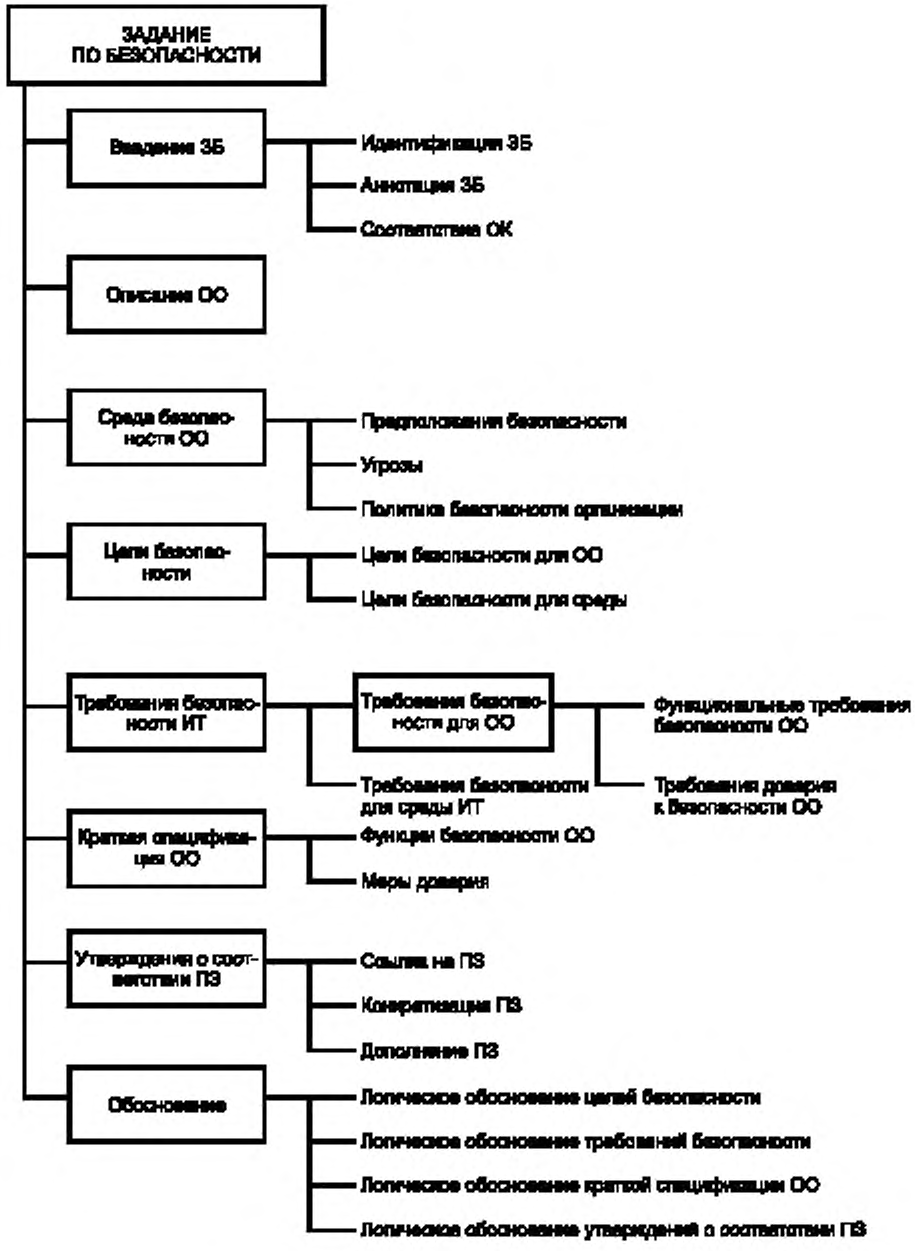

Рисунок В.1 — Содержание задания по безопасности

б) 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 описать через такие аспекты, как компетент-

ность, доступные ресурсы и мотивация. Нападение следует описать 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.

в) 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.

В.2.5 Цели безопасности

Изложение **целей безопасности** должно определять цели безопасности как для ОО, так и для его среды. Цели безопасности должны учитывать все установленные аспекты среды безопасности. Цели безопасности должны отражать изложенное намерение противостоять всем установленным угрозам и быть подходящими для этого, а также охватывать все предположения безопасности и установленную политику безопасности организации. 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.

а) **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.

б) **Цели безопасности для среды ОО** должны быть четко изложены и сопоставлены с аспектами установленных угроз, которым не полностью противоречит 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.

В.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.

а) 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, как функциональные компоненты, выбираемые из части 2 ОК;

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 части 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 определить их как один из ОУД, возможно, усиленный другими компонентами доверия из части 3 ОК. Расширение ОУД в ЗБ может осуществляться за счет явного включения дополнительных компонентов доверия, не содержащихся в этой части.

б) Необязательное изложение **требований безопасности для среды ИТ** должно определять требования безопасности ИТ, которым должна отвечать среда ИТ этого ОО. 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.

в) 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 частей 2 и 3 ОК. Если при формировании всех либо части требований не применимы компоненты из частей 2 или 3, то в ЗБ допускается необходимые требования безопасности сформулировать явным образом, без ссылки на содержание ОК.

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 ОК, 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.

В.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 в себя следующее.

а) **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.

б) **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.

В.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, строгое 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.

а) 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.

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

в) 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.

г) 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.

д) Случай, когда в ЗБ утверждается о частичном соответствии ПЗ, не приемлем для оценки в рамках ОК.

ОК не содержат 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 являлось приемлемой основой для оценки ОО, и четко прослеживалось соответствие каждому заявленному ПЗ.

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

е) **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.

ж) **Конкретизацию ПЗ**, идентифицирующую те требования безопасности ИТ, в которых выполняются операции, разрешенные в ПЗ, или дополнительно уточняются требования ПЗ.

и) **Дополнение ПЗ,** идентифицирующее цели и требования безопасности ОО, которые дополняют цели и требования ПЗ.

В.2.9 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 в себя следующее.

а) **Логическое обоснование целей безопасности,** демонстрирующее, что изложенные цели безопасности сопоставимы со всеми идентифицированными аспектами среды безопасности ОО и пригодны для их охвата.

б) **Логическое 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 строго обоснован. При этом должны быть строго обоснованы:

- выбор требований, не содержащихся в частях 2 или 3 ОК,
- 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.

в) **Логическое 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) строго обосновано утверждение, что изложенные меры доверия соответствуют требованиям доверия.

Уровень детализации логического обоснования должен соответствовать уровню детализации определения функций безопасности.

г) **Логическое 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.

ПРИЛОЖЕНИЕ Г
(справочное)

Библиография

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

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

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

[FC] 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.

[Gogu1] Goguen, J. A. and Meseguer, J., «Security Policies and Security Models», 1982 Symposium on Security and Privacy, pp. 11-20, IEEE, April 1982.

[Gogu2) Goguen, J. A. and Meseguer, J., «Unwinding and Inference Control», 1984 Symposium on Security and Privacy, pp. 75—85, IEEE, May 1984.

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

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

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

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

Редактор *В.П. Огурцов*
Технический редактор *В.Н. Прусакова*
Корректор *Н.Л. Рыбалко*
Компьютерная верстка *И.А. Налейкиной*

Изд. лиц. № 02354 от 14.07.2000. Сдано в набор 11.06.2002. Подписано в печать 16.07.2002. Усл. печ. л. 4,65. Уч.-изд.л. 4,50.
Тираж 380 экз. С 6608. Зак. 598.

ИПК Издательство стандартов, 107076 Москва, Колодезный пер., 14.
e-mail: info@standards.ru
Набрано в Издательстве на ПЭВМ
Филиал ИПК Издательство стандартов — тип. «Московский печатник», 103062 Москва, Лялин пер., 6.
Плр № 080102

gost.e-ecolog.ru