ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57628— 2017

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по разработке профилей защиты и заданий по безопасности

(ISO/IEC TR 15446:2009, NEQ)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ»)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 августа 2017 г. № 967-ст

4 Настоящий стандарт разработан с учетом основных положений международного стандарта ISO/IEC TR 15446:2009 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности» (ISO/IEC TR 15446:2004 «Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets», NEQ)

5 ВЗАМЕН ГОСТ Р ИСО/МЭК ТО 15446—2008

Правила применения настоящего стандарта установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Предназначение профиля защиты (далее — ПЗ) состоит в том, чтобы изложить проблему безопасности для определенной совокупности продуктов (изделий) информационных технологий (далее — ИТ), называемых объектами оценки (далее — ОО), и сформулировать требования безопасности для решения данной проблемы. При этом ПЗ не регламентирует то, каким образом данные требования будут выполнены, обеспечивая таким образом независимое от реализации описание требований безопасности.

Профиль защиты содержит взаимосвязанную информацию, имеющую отношение к безопасности ИТ, в том числе:

а) формулировку потребности в безопасности, соответствующую проблеме безопасности и выраженную в терминах, ориентированных на пользователей ИТ;

б) описание проблемы безопасности, уточняющее формулировку потребности в безопасности с учетом порождаемых средой угроз безопасности информации, которым нужно противостоять, политики безопасности организации, которая должна выполняться, и сделанных предположений;

в) цели безопасности ОО, основанные на описании проблемы безопасности и предоставляющие информацию относительно того, как и в какой мере должны быть удовлетворены потребности в безопасности. Предназначение целей безопасности заключается в том, чтобы снизить риск реализации угроз безопасности информации и обеспечить поддержание политики безопасности организации, в интересах которой ведется разработка ПЗ;

г) функциональные требования безопасности и требования доверия к безопасности, которые направлены на решение проблемы безопасности в соответствии с описанием проблемы безопасности и целями безопасности для ОО. Функциональные требования безопасности выражают то, что должно выполняться ОО для удовлетворения целей безопасности. Требования доверия к безопасности определяют степень уверенности в правильности реализации функций безопасности ОО;

д) обоснование, показывающее, что функциональные требования и требования доверия к безопасности являются соответствующими для удовлетворения сформулированной потребности в безопасности. Посредством целей безопасности должно быть показано, что необходимо сделать для решения проблемы безопасности. Функциональные требования безопасности должны удовлетворять целям безопасности.

Задание по безопасности (ЗБ) во многом похоже на ПЗ, но содержит дополнительную информацию, ориентированную на конкретную реализацию продукта ИТ и разъясняющую, каким образом требования ПЗ реализуются в конкретном продукте ИТ. Задание по безопасности содержит следующую дополнительную по отношению к ПЗ информацию:

а) краткую спецификацию ОО, которая представляет функции безопасности и меры доверия к безопасности для конкретного ОО;

б) утверждение о соответствии ЗБ одному или более ПЗ (если применимо);

в) материалы обоснования, устанавливающие, что краткая спецификация ОО обеспечивает удовлетворение требований безопасности, а любые утверждения о соответствия ПЗ действительны.

Профиль защиты может быть использован для определения типового набора требований безопасности, которым должны удовлетворять один или более продуктов ИТ. Профиль защиты может быть применен к определенному виду или типу продуктов (например, операционным системам, системам управления базами данных, межсетевым экранам, средствам антивирусной защиты, средствам контроля съемных машинных носителей информации, системам обнаружения вторжений и т. д.).

Поставщики продукта ИТ в соответствии с потребностями безопасности, сформулированными в ПЗ, могут разработать ЗБ, которое будет демонстрировать то, как их продукт ИТ удовлетворяет потребностям безопасности. Тем не менее соответствие задания по безопасности профилю защиты не всегда является обязательным (если не требуется при сертификации).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по разработке профилей защиты и заданий по безопасности

Information technology. Security techniques.
Guide for the production of Protection Profiles and Security Targets

Дата введения — 2018—01—01

1 Область применения

Настоящий стандарт представляет собой руководство по разработке профилей защиты (ПЗ) и заданий по безопасности (ЗБ) в соответствии с комплексом стандартов ГОСТ Р ИСО/МЭК 15408.

Настоящий стандарт не предназначен для использования в качестве вводного материала по оценке безопасности продуктов ИТ в соответствии с ГОСТ Р ИСО/МЭК 15408. Для получения такой информации следует использовать ГОСТ Р ИСО/МЭК 15408-1.

В настоящем стандарте не рассматриваются вопросы, не связанные непосредственно со спецификацией ПЗ и ЗБ, например, такие как регистрация ПЗ и обращение с защищаемой интеллектуальной собственностью.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-1—2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ГОСТ Р ИСО/МЭК 15408-2—2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности

ГОСТ Р ИСО/МЭК 15408-3—2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который

Издание официальное

дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 15408-1.

4 Сокращения

В настоящем стандарте применены следующие обозначения:

БИТ — безопасность информационных технологий;
ЗБ — задание по безопасности;
ЗИ — защита информации;
ИТ — информационная технология;
ИФБО — интерфейс ФБО;
НДВ — недекларированные возможности;
ОО — объект оценки;
ОПБ — определение проблемы безопасности;
ОУД — оценочный уровень доверия;
ПБОр — политика безопасности организации;
ПЗ — профиль защиты;
ПО — программное обеспечение;
РД — руководящий документ;
САВЗ — средство антивирусной защиты;
СВТ — средство вычислительной техники;
СКН — средство контроля съемных машинных носителей информации;
СОВ — система обнаружения вторжений;
СУБД — система управления базами данных;
ТДБ — требование доверия к безопасности;
ФБО — функциональные возможности безопасности ОО;
ФТБ — функциональное требование безопасности.

5 Назначение и структура стандарта

Настоящий стандарт предназначен для использования при разработке профилей защиты (ПЗ) или заданий по безопасности (ЗБ), используемых при оценке продуктов ИТ в соответствии с комплексом стандартов ГОСТ Р ИСО/МЭК 15408. Настоящий стандарт представляет собой детальное руководство по разработке различных частей ПЗ или ЗБ и их взаимосвязи.

Настоящий стандарт предназначен в первую очередь для разработчиков ПЗ и ЗБ, а также может представлять интерес для потребителей и пользователей ПЗ и ЗБ, позволяя им понять, чем руководствовались разработчики ПЗ и (или) ЗБ при их разработке, и подтвердить актуальность и точность содержащейся в ПЗ и ЗБ информации. Также настоящий стандарт полезен для оценщиков ПЗ или ЗБ и для ответственных за контроль оценки ПЗ и ЗБ.

Предполагается, что пользователи настоящего стандарта ознакомлены с ГОСТ Р ИСО/МЭК 15408-1, в частности с приложениями А и В, в которых приведены спецификации ЗБ и ПЗ соответственно. Разработчикам ПЗ и ЗБ необходимо также быть ознакомленными и с другими частями ГОСТ Р ИСО/МЭК 15408, включая вводный материал, такой как парадигма функциональных требований безопасности, описанная в ГОСТ Р ИСО/МЭК 15408-2, раздел 5.

Предполагается, что настоящий стандарт полностью соответствует ГОСТ Р ИСО/МЭК 15408, тем не менее в случае любого несоответствия между настоящим стандартом и ГОСТ Р ИСО/МЭК 15408 последнему в качестве нормативного следует отдавать предпочтение.

Разделы 1—4 содержат вводные и ссылочные материалы.

В разделе 5 приведен обзор структуры и назначения настоящего стандарта.

Раздел 6 содержит вводную информацию по ПЗ и ЗБ; в нем дается общее представление о ПЗ и ЗБ и о том, в каких случаях и для чего они могут использоваться. В разделе 6 также рассмотрены взаимосвязь между ПЗ и ЗБ и вопросы, связанные с процессом их разработки.

В разделах 7—13 приведена информация по спецификации обязательных разделов ПЗ или ЗБ согласно структуре ПЗ и ЗБ, установленной в разделах А.2 и В.2 ГОСТ Р ИСО/МЭК 15408-1.

В разделе 14 рассмотрены вопросы разработки ПЗ и ЗБ для составных ОО, то есть ОО, которые состоят из двух или более ОО-компонентов, для каждого из которых имеются собственные ПЗ и (или) ЗБ.

Раздел 15 посвящен некоторым отдельным вопросам, а именно содержанию сокращенных ПЗ и ЗБ для низкого уровня доверия к безопасности, соответствию национальным ограничениям и интерпретациям, а также использованию функциональных пакетов и пакетов доверия к безопасности.

В приложении А приведен пример определения расширенного (по отношению к ГОСТ Р ИСО/МЭК 15408-2) компонента.

В приложении Б приведены примеры угроз, политики безопасности организации, предположений и целей безопасности, а также установлено соответствие между общими функциональными требованиями и соответствующими функциональными компонентами из ГОСТ Р ИСО/МЭК 15408-2.

6 Краткий обзор профилей защиты и заданий по безопасности

6.1 Введение

В данном разделе приведен краткий обзор роли ПЗ и ЗБ в процессе оценки безопасности продуктов ИТ в соответствии с комплексом стандартов ГОСТ Р ИСО/МЭК 15408.

6.2 Целевая аудитория

Настоящий стандарт предназначен для использования следующими категориями пользователей:

а) специалистами ИТ, обладающими знаниями в области защиты информации (например, ответственными за защиту информации или архитекторами по вопросам защиты информации, у которых есть знание и понимание требований безопасности), но которые не являются экспертами в области оценки безопасности продуктов ИТ и не имеют предварительных знаний по ГОСТ Р ИСО/МЭК 15408;

б) экспертами в области защиты информации, которые обладают хорошим знаниями ГОСТ Р ИСО/МЭК 15408 и занимаются разработкой ПЗ и ЗБ в рамках профессиональной деятельности.

Если пользователь настоящего стандарта относится к первой категории, настоящий раздел предоставит информацию, необходимую для понимания назначения и структуры ПЗ и ЗБ. В данном разделе представлена справочная информация, необходимая для восприятия и понимания ПЗ и ЗБ, а также для определения их применимости в конкретных случаях. В последующих разделах приведено детальное пояснение содержания каждого раздела ПЗ и ЗБ, но они ориентированы уже на практическую разработку ПЗ и ЗБ и предполагают знание положений ГОСТ Р ИСО/МЭК 15408.

Если пользователь настоящего стандарта является экспертом в области защиты информации, то информация, представленная в данном разделе, должна быть в целом ему известна. В последующих разделах для таких экспертов приведены методические подходы и практические рекомендации, которые могут быть использованы при разработке ПЗ и ЗБ.

Также настоящий стандарт полезен и в случае, если от лица, не являющегося экспертом в области защиты информации, требуется разработать ПЗ или ЗБ. Однако для этого потребуется найти и изучить опубликованные примеры ПЗ или ЗБ, подобные тем, которые требуется разработать. Также в этом случае следует рассмотреть возможность привлечения к разработке ПЗ или ЗБ организаций, у которых имеются специалисты с соответствующей компетенцией и опыт разработки ПЗ и ЗБ.

6.3 Использование профилей защиты и заданий по безопасности

6.3.1 Введение

Основной областью применения ГОСТ Р ИСО/МЭК 15408 является оценка безопасности продуктов ИТ. Для термина «продукт ИТ» в ГОСТ Р ИСО/МЭК 15408 не приведено однозначного определения, под ним может пониматься любой тип сущностей, построенных с использованием ИТ, будь то полная система ИТ (не путать с «информационной системой» или «автоматизированной системой»), используемая одной организацией, или линейка готовых к использованию продуктов, созданных разработчиком (производителем) продукта ИТ для реализации (поставки) различным заказчикам.

В качестве примера системы ИТ можно, например, привести средства контроля отчуждения (переноса) информации со съемных машинных носителей информации, в состав которых входят следующие компоненты, распределенные по компонентам информационной системы или сами являющиеся законченными изделиями:

- специализированные съемные машинные носители информации;
- программное обеспечение инициализации;
- программное обеспечение управления;
- программное обеспечение взаимодействия со съемными машинными носителями информации.

В настоящем стандарте рекомендации, относящиеся к «продуктам ИТ» или просто «продуктам», применимы ко всем таким сущностям. В случаях, когда область применения рекомендации ограничена определенным типом продукта ИТ, в настоящем стандарте применены термины «система», «готовый к использованию продукт» или иная конкретная формулировка.

Так как продукты ИТ могут использоваться различным образом и во многих типах среды функционирования, понятие безопасности будет различаться в зависимости от продукта ИТ. Поэтому конечным результатом оценки по ГОСТ Р ИСО/МЭК 15408 никогда не может быть вывод «данный продукт ИТ является безопасным», вместо этого утверждается, что «данный продукт ИТ соответствует данной спецификации безопасности».

В ГОСТ Р ИСО/МЭК 15408 приведены стандартизированные спецификации безопасности для (помимо прочего):

- определения специфического контента, необходимого для оценки продукта ИТ на соответствие спецификации безопасности;
- создания условий для сравнения спецификаций безопасности различных продуктов ИТ.

В ГОСТ Р ИСО/МЭК 15408 вводятся два различных типа спецификаций безопасности: профили защиты (ПЗ) и задания по безопасности (ЗБ). Разница между ними определяется их предназначением в типовом процессе разработки, оценки продукта ИТ и его приобретения заказчиком.

В целях настоящего стандарта используются термины «заказчик», «разработчик», «производитель», «заявитель», «продукт». Заказчиком является сторона, которая планирует приобрести продукт ИТ. Это может быть физическое лицо, организация, группа организаций, орган государственной власти и т. д. Разработчиком (производителем) является сторона, которая разрабатывает, производит и планирует поставку продукта ИТ заказчику. Это может быть малая или крупная организация, группа совместно работающих организаций и т. д. Заявителем является сторона, которая представляет продукт ИТ и соответствующие документированные материалы для оценки (сертификационных испытаний). Продуктом ИТ может быть средство защиты определенного вида и (или) типа, прикладное программное обеспечение, смарт-карта, операционная система, компьютерная система, содержащая сотни различных компонентов, и др.

Когда заказчику необходимо приобрести продукт ИТ, у него фактически имеются две возможности:

- связаться с разработчиком и изложить свои потребности, а разработчик затем создаст (разработает) продукт ИТ, который будет предназначен конкретно для этого заказчика и будет точно соответствовать требованиям этого заказчика. Это достаточно дорогостоящий вариант организации процесса приобретения, но заказчик при этом получает готовое требуемое изделие. Далее в настоящем стандарте подобный процесс будет называться процессом приобретения на основе спецификации;
- выбрать продукт из числа существующих продуктов ИТ. Такой способ менее затратный, но приобретенный продукт может соответствовать, а может и не соответствовать потребностям заказчика. Далее в настоящем стандарте подобный процесс будет называться процессом приобретения на основе выбора.

Процесс приобретения усложняется необходимостью учитывать вопросы безопасности ИТ. Среднестатистическому заказчику достаточно сложно:

- определить, какой уровень безопасности ИТ (функционал безопасности ИТ, класс защиты и т. п.) ему необходим;
- сделать заключение о том, необходим и достаточен ли тот уровень безопасности ИТ, который заявлен для данного продукта ИТ, для удовлетворения потребностей заказчика;
- сделать заключение о том, что утверждения о наличии в продукте ИТ характеристик безопасности являются корректными.

Для оказания содействия заказчику в процессе приобретения и в преодолении сложностей, перечисленных выше, целесообразным является проведение оценки продукта ИТ с использованием ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. И в этом случае профили защиты и задания по безопасности играют важную роль. В 6.3.2 и 6.3.3 продемонстрировано, каким образом проведение оценки помогает при каждом типе процесса приобретения на основе спецификации и на основе выбора.

Продукты ИТ не функционируют изолированно. Продукт используется заказчиком в среде функционирования, в которой могут применяться собственные меры защиты. Иногда для продукта делаются предположения о том, что в среде функционирования выполняются определенные типы функциональных возможностей безопасности. Эти предположения также включаются в ПЗ или ЗБ.

6.3.2 Процесс приобретения на основе спецификации

6.3.2.1 Краткий обзор

В процессе приобретения на основе спецификации заказчик разрабатывает спецификацию, предоставляет ее разработчику, а затем разработчик создает (разрабатывает) продукт ИТ на основании этой спецификации. При этом необходимо выполнить следующие шаги:

а) заказчик должен определить требования безопасности в неформализованном виде;

б) заказчик должен преобразовать эти неформализованные требования безопасности в спецификацию более формального стиля изложения, подходящую для использования разработчиком;

в) разработчик должен создать (разработать) продукт ИТ на основе данной спецификации.

В заключение заказчику потребуется убедиться, что продукт ИТ ему подходит. Поэтому очень важное значение имеет качество выполнения каждого из этих шагов.

6.3.2.2 Неформализованные требования безопасности

Процесс определения неформализованных требований безопасности, который определяет, «что является проблемой безопасности и как следует ее решать», находится вне области применения ГОСТ Р ИСО/МЭК 15408 и, соответственно, вне области рассмотрения настоящего стандарта. Тем не менее это не означает, что этот процесс простой или не является важным.

ГОСТ Р ИСО/МЭК 15408 предполагает, что заказчик способен определить неформализованные требования безопасности. Если неформализованные требования будут определены неправильно, то приобретаемый продукт ИТ может не отвечать фактически существующим требованиям безопасности.

В изложенных заказчиком требованиях часто присутствует ряд проблем, в частности связанных с вопросами безопасности. Требования заказчика, как правило, являются:

а) неполными (присутствуют не все требования). Например, могут быть не рассмотрены важные угрозы, которым должен противостоять продукт;

б) не связанными со средой: требования могут в недостаточной степени согласовываться с конкретной средой, в которой должен функционировать продукт ИТ, или в требованиях может быть изложено недостаточно четкое описание этой среды;

в) неявными: у некоторых требований к продукту ИТ могут иметься связанные с ними требования, не включенные в требования заказчика. Разработчик может не учесть эти неявные требования;

г) не пригодными для тестирования: требования могут быть сформулированы неоднозначным образом, из-за чего не представляется возможным верифицировать, соответствует ли продукт ИТ требованиям;

д) излишне детализированными: возможен случай, когда реализация подробно расписана и документирована, но не документирована причина выбора данной реализации. Если в дальнейшем требования изменятся, зачастую неясно, каким образом следует вносить эти изменения;

е) насыщенными расплывчатыми формулировками: например, в требованиях может быть указано, что связь должна осуществляться по защищенным каналам, при этом нет определения того, что считать «защищенным» каналом;

ж) несогласованными: требования могут быть внутренне противоречивыми.

При представлении требований заказчика разработчику в таком виде, как правило, возникают проблемы, так как разработчик может неверно интерпретировать предоставленные ему требования. При оценке безопасности продукта ИТ оценщики могут также интерпретировать неформализованные требования по-своему, отлично от того, как их интерпретируют и заказчик, и разработчик, что приведет к усугублению проблем.

По этим причинам важным шагом в процессе приобретения на основе спецификации является формализация требований заказчика. Для требований безопасности на основе ГОСТ Р ИСО/МЭК 15408 такая формализация происходит с использованием так называемого профиля защиты (ПЗ). Профиль защиты, по сути, является документом, в котором требования безопасности заказчика изложены в формализованном, стандартизированном виде.

6.3.2.3 Использование профилей защиты в качестве спецификаций

Профили защиты, как правило, разрабатываются уполномоченным федеральным органом исполнительной власти (ФСТЭК России), крупными организациями, группами организаций, ведомствами и т. д., поскольку их разработка требует значительных усилий.

Профиль защиты содержит несколько разделов, но для использования в качестве спецификации безопасности наиболее важным является раздел «Функциональные требования безопасности». Используя ГОСТ Р ИСО/МЭК 15408, необходимо составить эти требования на специальном языке, определенном в рамках этого комплекса стандартов. Использование специального языка обеспечивает, что ПЗ:

а) будет однозначно интерпретируемым: в языке ГОСТ Р ИСО/МЭК 15408 содержатся полные и однозначные определения терминов, достаточные для того, чтобы разработчик мог понять требования и правильно их интерпретировать;

б) даст возможность тестирования продукта ИТ: язык ГОСТ Р ИСО/МЭК 15408 определен таким образом, что содержит только элементы, которые можно протестировать. Таким образом, на последующих этапах можно будет оценить, соответствует ли конкретный продукт ИТ профилю защиты;

в) не будет излишне детализированным: язык ГОСТ Р ИСО/МЭК 15408 обеспечивает определенный уровень абстракции, необходимый для выражения требований заказчика;

г) будет достаточно полным: язык ГОСТ Р ИСО/МЭК 15408 содержит несколько конструкций («если необходима конкретная функциональная возможность, то требуется также и следующая функциональная возможность»), которые помогают удостовериться, что неявные требования учтены.

6.3.2.4 Разработка продукта по профилю защиты

Далее заказчик может предоставить ПЗ, то есть формализованные требования заказчика, одному или нескольким разработчикам. Разработчик использует предоставленный ПЗ в качестве отправной точки для создания (разработки) продукта ИТ. В качестве первого шага в этом процессе он разрабатывает задание по безопасности (ЗБ).

Задание по безопасности, используемое для создания (разработки) продукта ИТ, очень похоже на ПЗ, но тогда как ПЗ определяет требования заказчика и теоретически разрабатывается заказчиком, ЗБ представляет собой спецификацию продукта ИТ и составляется разработчиком.

Разработчик не может в ответ на ПЗ, полученный от заказчика, представить ЗБ произвольного содержания: ЗБ должно соответствовать ПЗ. Это означает, что продукт должен удовлетворять всем требованиям заказчика, но:

- в ЗБ может быть специфицировано больше, чем в ПЗ: в продукте может быть реализовано больше функциональных возможностей безопасности, чем предусматривалось требованиями заказчика (эти дополнительные функциональные возможности не должны противоречить ПЗ). Например, потому что продукт будет поставляться нескольким заказчикам со сходными, но не полностью совпадающими требованиями, или потому, что продукт является производным от существующего (стандартного) продукта ИТ;
- задание по безопасности может быть более детализированным, чем ПЗ: если в ПЗ объясняется, «что» должно быть защищено, то в ЗБ указывается и «каким образом»: разработчик обобщенно излагает, каким образом он реализует требования заказчика.

Профиль защиты может предоставить разработчику ЗБ достаточную гибкость для того, чтобы предложить эквивалентное, но отличное от указанного в ПЗ решение по предоставляемым функциональным возможностям безопасности (подробнее см. 6.5.6).

Задание по безопасности определяет для разработчика функциональные возможности безопасности, которые должен реализовывать продукт ИТ, и служит «спецификацией требований безопасности» для дальнейшего выполнения процесса разработки.

Результатом процесса разработки должен стать продукт ИТ, который может быть поставлен заказчику, установлен и использован заказчиком по назначению. Подразумевается, что этот продукт ИТ должен функционировать согласно описанию в ЗБ.

6.3.2.5 Роль оценки в процессе приобретения на основе спецификации

В предыдущих пунктах были рассмотрены только роли заказчика и разработчика. Разработчик может просто заявить заказчику (без представления дополнительных свидетельств — документированных материалов), что:

а) ЗБ соответствует ПЗ;

б) продукт ИТ соответствует ЗБ;

в) следовательно, продукт ИТ соответствует ПЗ и отвечает требованиям заказчика.

Если заказчик принимает эти утверждения, процесс завершается.

Однако если заказчик потребует независимого подтверждения этих утверждений, он может обратиться к третьей стороне (испытательной лаборатории) для проверки этих утверждений о соответствии путем проведения оценки (сертификационных испытаний) по ГОСТ Р ИСО/МЭК 15408. При этом испытательная лаборатория использует ПЗ, ЗБ, продукт ИТ и ГОСТ Р ИСО/МЭК 15408 для оценки двух утверждений:

а) ЗБ соответствует ПЗ;

б) продукт ИТ соответствует ЗБ.

Следует отметить, что несмотря на проведение оценки, два вопроса по-прежнему останутся открытыми:

а) преобразование неформализованных требований безопасности заказчика в профиль защиты. Как было указано ранее, этот процесс находится вне области применения ГОСТ Р ИСО/МЭК 15408, но если он будет проведен неправильно, то не будет достигнуто соответствие между ПЗ и требованиями заказчика. Таким образом, разрабатываемый продукт, скорее всего, также не будет соответствовать требованиям заказчика;

б) оценка не является способом «доказать» соответствие. Оценка в соответствии с ГОСТ Р ИСО/МЭК 15408 не предоставляет абсолютной гарантии того, что продукт отвечает требованиям ПЗ; оценка может только предоставить определенную степень доверия в зависимости от глубины и области охвата оценки, которые определены в ПЗ или ЗБ.

6.3.3 Процесс приобретения на основе выбора

6.3.3.1 Краткий обзор

В предыдущем пункте был рассмотрен процесс, когда заказчик предоставляет разработчику спецификацию, а затем разработчик осуществляет реализацию этой спецификации. В данном пункте рассматривается ситуация, при которой заказчик выбирает из уже существующих готовых продуктов ИТ, а не заказывает уникальный продукт. Таким образом, процесс приобретения при этом основывается не на соответствии продукта ИТ формализованному изложению требований заказчика (то есть ПЗ), а на сравнении существующих продуктов ИТ, которое выполняется заказчиком.

В процессе приобретения продукта ИТ на основе выбора:

а) разработчик должен создать (разработать) продукт ИТ, разработать спецификацию продукта и предоставить спецификацию заказчику;

б) заказчик на основе полученной спецификации (возможно, на основе сравнения спецификаций различных разработчиков) должен сделать заключение о том, является ли специфицированный продукт ИТ наиболее подходящим для приобретения.

6.3.3.2 Использование предоставленной разработчиком спецификации

В процессе приобретения на основе выбора заказчику приходится использовать спецификацию, предоставленную разработчиком.

Если эта спецификация представлена в неформальном стиле изложения, для нее характерны те же перечисленные в 6.3.2.2 потенциально возможные недостатки, что и для неформализованных требований заказчиков. По этой причине спецификация разработчика также подлежит формализации. Для этой цели в ГОСТ Р ИСО/МЭК 15408 используется задание по безопасности (ЗБ), как отмечалось ранее в 6.3.2.4. Задание по безопасности в данном случае используется аналогично описанию использования ЗБ в 6.3.2.4, с одной очевидной разницей: поскольку оно не основано на ПЗ заказчика, нельзя утверждать о соответствии ЗБ такому профилю защиты (но можно утверждать о соответствии другим ПЗ — см. 6.3.4).

Поскольку разработчик не знает специфических требований заказчика, ему придется провести оценку актуальных требований рынка и отразить соответствие этим требованиям в ЗБ. Они не обязательно будут совпадать со специфическими требованиями конкретного заказчика.

Разработчик создает (разрабатывает) свой продукт в соответствии с ЗБ: этот процесс аналогичен процессу приобретения на основе спецификации.

6.3.3.3 Сравнение заданий по безопасности разных разработчиков

Впоследствии заказчик может сравнить ЗБ для ряда продуктов ИТ и выбрать продукт ИТ, который наилучшим образом соответствует его требованиям (в том числе с учетом требований, не связанных с вопросами безопасности, например, с учетом требований к стоимости продукта ИТ). Это означает, что ему придется определить соответствующие неформализованные требования безопасности (см. 6.3.2.2) и сравнить с предоставленными ему ЗБ. Если один или несколько продуктов соответствуют его требованиям, то выбор завершен. Если это не так, заказчик должен либо выбрать наиболее «близкий» по требованиям продукт, либо найти другое решение (то есть изменить свои требования).

Как уже было указано в 6.3.2, процесс получения неформализованных требований безопасности заказчиков находится вне области применения ГОСТ Р ИСО/МЭК 15408 и настоящего стандарта. Сравнение неформализованных требований заказчика с ЗБ также находится вне области применения ГОСТ Р ИСО/МЭК 15408, хотя некоторые рекомендации по этому вопросу можно найти в последующих разделах настоящего стандарта.

6.3.3.4 Роль оценки в процессе приобретения на основе выбора

Как и для процесса приобретения на основе спецификации, разработчик может просто утверждать, что его продукт соответствует ЗБ. Если заказчик принимает эти утверждения, то процесс завершается.

Однако обычно разработчик предоставляет сертификат, подтверждающий, что независимая третья сторона (испытательная лаборатория) подтвердила правильность ЗБ, а затем провела оценку безопасности (сертификацию по требованиям безопасности информации) по ГОСТ Р ИСО/МЭК 15408 для подтверждения того, что продукт действительно соответствует ЗБ. Заказчик может также заказать проведение такой оценки (сертификацию по требованиям безопасности информации), если он считает, что оценка важна, а разработчик не провел ее.

Следует отметить, что при использовании оцененных (сертифицированных) продуктов два вопроса по-прежнему останутся открытыми:

а) доказательство соответствия неформализованных требований безопасности заказчика и задания по безопасности. Как было указано ранее, этот процесс находится вне области применения ГОСТ Р ИСО/МЭК 15408, но если этот процесс будет проведен неправильно, то не будет достигнуто соответствие между ЗБ и требованиями заказчика. Таким образом, и разрабатываемый продукт также может не соответствовать фактическим требованиям заказчика;

б) оценка не является способом «доказать» соответствие. Оценка по ГОСТ Р ИСО/МЭК 15408 не предоставляет абсолютной гарантии того, что продукт отвечает требованиям ПЗ; она может только предоставить определенную степень доверия в зависимости от глубины и области охвата оценки, которые определены в ЗБ.

6.3.4 Другие возможности использования профилей защиты

У профилей защиты есть и другие возможности для применения. Например, органы по стандартизации и ассоциации поставщиков могут специфицировать ПЗ в качестве лучшей практики задания минимальных норм по безопасности для определенных типов продуктов ИТ. Уполномоченные федеральные органы исполнительной власти (ФСТЭК России) могут требовать соответствия профилям защиты в рамках своих полномочий (например, для продуктов ИТ, применяемых в государственных информационных системах). В этих случаях заказчики и разработчики, скорее всего, будут требовать соответствия таким ПЗ, а также будут требовать или предлагать дополнительные функциональные возможности безопасности для удовлетворения конкретных потребностей.

Организации, специфицирующие ПЗ для использования в таких целях, должны удостовериться, что специфицированные ПЗ содержат минимум необходимых требований и не содержат требований с нереализуемыми функциональными возможностями или недостижимыми для разработчиков уровнями доверия.

Профили защиты также могут быть разработаны для выражения потребности в определенном типе продуктов ИТ.

Примерами таких профилей защиты являются профили защиты ФСТЭК России для средств контроля отчуждения (переноса) информации со съемных машинных носителей информации, средств доверенной загрузки уровня базовой системы ввода-вывода и другие.

6.4 Процесс разработки профилей защиты и заданий по безопасности

Анализ порядка представления требований для ПЗ и ЗБ в ГОСТ Р ИСО/МЭК 15408-1 (приложения А и В) и предыдущих подразделах данного раздела показывает, что разработка ПЗ или ЗБ осуществляется в следующей (нисходящей) последовательности (например, для случая разработки ЗБ):

а) первоначальное определение проблемы безопасности;

б) идентификация целей безопасности, направленных на решение проблемы безопасности;

в) формирование требований безопасности, направленных на удовлетворение целей безопасности для ОО;

г) выбор конкретных функциональных возможностей безопасности, направленных на выполнение требований безопасности.

В общем случае, хотя и с учетом данной последовательности действий, процесс разработки ПЗ и ЗБ чаще всего носит итеративный характер. Например, формирование требований безопасности может способствовать корректировке целей безопасности или даже проблемы безопасности. Может потребоваться целый ряд итераций для наиболее полного учета взаимосвязей между угрозами, ПБОр, целями и требованиями безопасности, а также функциями безопасности, в частности при формировании обо-

снований. При этом только когда все проблемы формирования обоснований решены, процесс разработки ПЗ или ЗБ можно считать завершенным.

Процесс разработки ПЗ или ЗБ может также включать в себя внесение изменений в документ при появлении новой информации в рамках проблемы безопасности, чтобы отразить изменения условий применения, например:

а) идентификацию новых угроз;

б) изменение ПБОр;

в) изменения в распределении задач по обеспечению безопасности информации, возлагаемой соответственно на ОО и среду ОО, связанные со стоимостными и временными ограничениями;

г) корректировку проблемы безопасности для ОО вследствие изменения предполагаемого потенциала нападения нарушителя.

Также возможно (в особенности для случая, когда объектом оценки является уже существующий продукт ИТ), что разработчики ПЗ или ЗБ имеют четкое представление относительно функциональных возможностей безопасности, которые предоставляет ОО (даже если эти требования еще не были выражены в стиле функциональных требований безопасности по ГОСТ Р ИСО/МЭК 15408). В таких случаях на определение проблемы безопасности и целей безопасности будут влиять сведения о том, каким образом ОО решает проблему безопасности. Процесс разработки ПЗ или ЗБ в таком случае будет в некоторой степени «восходящим».

6.5 Вопросы восприятия и понимания профилей защиты и заданий по безопасности

6.5.1 Введение

Данный пункт не предназначен для специалистов, ознакомленных с ГОСТ Р ИСО/МЭК 15408. Он предназначен для той части пользователей настоящего стандарта, которая мало знает о разработке ПЗ или ЗБ, но которой необходимо изучить один или несколько ПЗ или одно или несколько ЗБ для понимания возможностей безопасности соответствующих продуктов ИТ.

Для детального понимания содержания ПЗ и ЗБ следует изучить ГОСТ Р ИСО/МЭК 15408-1, в частности приложения А и В, в которых представлена детальная информация относительно заданий по безопасности и профилей защиты соответственно. Также необходимо изучить опубликованные ПЗ и ЗБ, находящиеся в открытом доступе. Профили защиты, выпущенные ФСТЭК России для целого ряда видов и типов средств защиты информации (например, средств антивирусной защиты, систем обнаружения вторжений, средств доверенной загрузки, средств контроля использования съемных машинных носителей информации, межсетевых экранов), представлены на официальном сайте ФСТЭК России (www.fstec.ru). Существует целый ряд международных реестров, из которых можно получить ПЗ и ЗБ. Самым известным является портал Common Criteria («Общие критерии») [1]. Этот реестр признан ИСО и МЭК в качестве официального реестра JTC 1 для профилей защиты и пакетов, сформированных в соответствии с ГОСТ Р ИСО/МЭК 15408. Он функционирует в соответствии с [2].

В последующих пунктах данного подраздела определены подразделы ПЗ и ЗБ, которые содержат ключевую информацию для понимания характеристик безопасности, отражаемых в ПЗ или ЗБ для продукта ИТ.

К таким подразделам относятся:

а) «Аннотация ОО»;

б) «Описание ОО»;

в) «Цели безопасности для среды функционирования»;

г) «Утверждения о соответствии».

6.5.2 Подраздел «Аннотация ОО»

С подразделом «Аннотация ОО» в ПЗ или ЗБ следует ознакомиться в первую очередь, так как он нацелен «на потенциальных потребителей ОО, просматривающих списки оцененных ОО/продуктов ИТ, чтобы найти ОО, которые могут удовлетворить их потребности в безопасности и поддерживаться их аппаратным, программным и программно-аппаратным обеспечением» (ГОСТ Р ИСО/МЭК 15408-1, пункт А.4.2). Аннотация ОО состоит из трех пунктов:

а) использование и основные характеристики безопасности ОО;

б) тип ОО;

в) требуемые аппаратные средства/программное обеспечение/программно-аппаратные средства, не входящие в ОО.

Простые примеры изложения этих пунктов приведены в ГОСТ Р ИСО/МЭК 15408-1, пункт А.4.2.

Пункт «Описание использования и основных характеристик безопасности ОО» предназначен для того, чтобы дать общее представление о возможностях ОО с точки зрения безопасности и о том, для чего можно использовать ОО в контексте безопасности.

Этот пункт должен быть достаточно кратким, чтобы его изучение и понимание не требовало больших усилий. Так как этот пункт нацелен на потребителей, он не должен быть сугубо техническим. Предполагается, что он служит для получения общего представления об ОО и не является исчерпывающим.

Ниже приведен фрагмент содержания пункта «Описание использования и основных характеристик безопасности ОО» на примере профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации [3].

«Объект оценки представляет собой программное или программно-техническое средство, которое предназначено для обеспечения контроля использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации.

Объект оценки должен обеспечивать нейтрализацию угроз безопасности информации, связанных с подключением к информационной системе внутренними и внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы или загрузкой в информационную систему с этих съемных машинных носителей информации вредоносного программного обеспечения.

В состав средства контроля подключения съемных машинных носителей информации (СКН) входят следующие компоненты:

- программное обеспечение, устанавливаемое на средствах вычислительной техники и обеспечивающее взаимодействие с подключаемыми съемными машинными носителями информации;
- программное обеспечение управления (локального и (или) централизованного) средствами контроля подключения съемных машинных носителей информации.

В СКН должны быть реализованы следующие функции безопасности:

- разграничение доступа к управлению СКН;
- управление работой СКН;
- управление параметрами СКН;
- контроль подключения съемных машинных носителей информации;
- аудит безопасности СКН;
- сигнализация СКН.

В среде, в которой СКН функционирует, должны быть реализованы следующие функции безопасности среды:

- физическая защита средств вычислительной техники, на которых используются компоненты СКН;
- обеспечение условий безопасного функционирования СКН;
- управление атрибутами безопасности компонентов СКН.

Функции безопасности СКН должны обладать составом функциональных возможностей (функциональных требований безопасности), обеспечивающих реализацию этих функций.

В ПЗ изложены следующие виды требований безопасности, предъявляемые к средствам контроля подключения съемных машинных носителей информации:

- функциональные требования безопасности;
- требования доверия к безопасности.

Функциональные требования безопасности СКН, изложенные в ПЗ, включают:

- требования к разграничению доступа к управлению СКН;
- требования к управлению работой (режимами выполнения функций безопасности) СКН;
- требования к управлению параметрами СКН, которые влияют на выполнение функций безопасности СКН;
- требования к контролю подключения съемных машинных носителей информации;
- требования по предупреждению о событиях, связанных с нарушением безопасности;
- требования к аудиту безопасности СКН.

Состав функциональных требований безопасности (ФТБ), включенных в настоящий ПЗ, обеспечивает следующие функциональные возможности СКН:

- реализация политики управления использованием подключаемых съемных машинных носителей информации по отношению к подключаемым произвольным съемным машинным носителям информации;

- возможность управления использованием подключаемых произвольных съемных машинных носителей информации на основе анализа разрешений на подключение к конкретным интерфейсам ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств, конкретных съемных машинных носителей информации;

- возможность со стороны администраторов СКН управлять данными (данными средства контроля подключения съемных машинных носителей информации), используемыми функциями безопасности средства контроля подключения съемных машинных носителей информации;

- поддержка определенных ролей для средства контроля подключения съемных машинных носителей информации и их ассоциации с конкретными администраторами СКН и пользователями информационной системы;

- возможность защиты от несанкционированной модификации данных средства контроля подключения съемных машинных носителей информации при передаче между программным обеспечением управления средствами контроля подключения съемных машинных носителей информации и программным обеспечением взаимодействия с подключаемыми съемными машинными носителями информации;

- возможность регистрации событий, связанных с изменениями конфигурации функций безопасности средства контроля подключения съемных машинных носителей информации;

- возможность чтения информации из записей аудита уполномоченным администраторам СКН;

- возможность реагирования при обнаружении событий, указывающих на возможное нарушение безопасности;

- возможность выборочного просмотра данных аудита.

Требования доверия к безопасности средств контроля подключения съемных машинных носителей информации сформированы на основе компонентов требований ГОСТ Р ИСО/МЭК 15408-3.

В целях обеспечения условий для безопасного функционирования СКН в настоящем ПЗ определены цели и требования для среды функционирования СКН».

В пункте «Тип ОО» приводится описание общей категории продуктов ИТ, к которым относится ОО (например, операционная система, межсетевой экран, средство антивирусной защиты, средство обнаружения вторжений, средство доверенной загрузки и т. д.).

Типы ОО могут быть определены в нормативных правовых актах уполномоченных федеральных органов исполнительной власти (ФСТЭК России) для видов средств защиты информации. Так, например, в нормативном правовом акте ФСТЭК России для средств контроля съемных машинных носителей информации определены следующие типы этих средств:

- средства контроля подключения съемных машинных носителей информации;

- средства контроля отчуждения (переноса) информации со съемных машинных носителей информации.

Ниже приведен фрагмент содержания пункта «Тип ОО» на примере профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации.

«Объектом оценки в настоящем ПЗ является средство контроля подключения съемных машинных носителей информации.

Объект оценки обеспечивает контроль использования интерфейсов ввода (вывода) средств вычислительной техники, типов подключаемых внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации путем реализации следующих процессов:

- проверка наличия разрешения или запрета на использование интерфейса ввода (вывода) средства вычислительной техники при попытке подключения съемного машинного носителя информации;

- проверка наличия разрешения или запрета на использование соответствующего типа подключаемых внешних программно-аппаратных устройств при наличии разрешения (отсутствия запрета) на использование интерфейса ввода (вывода) средства вычислительной техники;

- проверка наличия разрешения или запрета на подключение конкретного съемного машинного носителя информации при наличии разрешения (отсутствия запрета) на подключение соответствующего типа внешних программно-аппаратных устройств;

- разрешение или запрет использования подключаемого съемного машинного носителя информации по результатам выполненных проверок;

- регистрация событий безопасности и запись информации аудита безопасности средства контроля подключения съемных машинных носителей информации».

В ГОСТ Р ИСО/МЭК 15408 также установлено, что в «Аннотации ОО» перечисляются любые обоснованные ожидания, которые могут иметься в отношении этого типа ОО, но которые не поддерживаются ОО. В частности:

а) если от ОО (с учетом его типа) могут ожидаться определенные функциональные возможности, в то время как у данного ОО эти функциональные возможности отсутствуют, то в «Аннотации ОО» эти функциональные возможности должны быть перечислены как отсутствующие;

б) если от ОО (с учетом его типа) может ожидаться возможность его функционирования в определенной среде, в то время как для данного ОО такая возможность отсутствует, то это должно быть указано в «Аннотации ОО».

Следует отметить, что указанные предупреждения требуется приводить в пункте ПЗ или ЗБ «Тип ОО». При этом разработчик ПЗ или ЗБ может продублировать эту информацию и в других частях (разделах, подразделах, пунктах) ПЗ или ЗБ посредством примечаний (замечаний по применению).

Если эти предупреждения предоставлены и могут влиять на предполагаемое использование продукта ИТ, то следует внимательно рассмотреть возможность использования данного ОО с этими ограничениями.

Многие ОО (особенно программные ОО) зависят от дополнительных аппаратных средств, программного обеспечения и (или) программно-аппаратных средств, не входящих в ОО. В таком случае в «Аннотации ОО» требуется идентифицировать соответствующие аппаратные средства/программное обеспечение и (или) программно-аппаратные средства, не входящие в ОО.

В ПЗ или ЗБ не требуется полной и абсолютно детальной идентификации дополнительных аппаратных средств, программного обеспечения и (или) программно-аппаратных средств, но при этом необходима полнота и детализация идентификации, достаточная для определения потенциальными потребителями основных аппаратных средств, программного обеспечения и (или) программно-аппаратных средств, необходимых для использования ОО.

Следует тщательно оценить, существуют ли какие-либо нестандартные компоненты, на которые полагается ОО, и подходят ли эти компоненты к существующей инфраструктуре, бюджету, политикам организации и т. д.

6.5.3 Подраздел «Описание ОО»

В процессе оценки по ГОСТ Р ИСО/МЭК 15408 важно помнить, что если некий широко известный продукт ИТ подвергался оценке, это не означает, что все функциональные возможности безопасности (или хотя бы большая часть функциональных возможностей безопасности) данного продукта подвергались оценке. Возможен случай, когда фактически были рассмотрены только некоторые характеристики функциональных возможностей безопасности, а остальные не рассматривались как часть оцениваемых функциональных возможностей безопасности. В пункте А.4.1 ГОСТ Р ИСО/МЭК 15408 запрещается использование вводящих в заблуждение ссылок на ОО, однако разработчики могут обойти это ограничение, используя в ссылке наименование продукта. Необходимо проверить, что оцененные функции отвечают потребностям потенциального заказчика. Если некоторые функциональные возможности безопасности, которые потенциальный заказчик собирается использовать, были исключены из рассмотрения при оценивании, следует задаться вопросом, по какой причине это было сделано.

Самая важная цель описания ОО заключается в том, чтобы предоставить потенциальным потребителям общее понимание функциональных возможностей безопасности ОО. С этой целью в описании ОО детально рассматриваются физические и логические границы ОО.

В отношении физических границ в ГОСТ Р ИСО/МЭК 15408 указано, что «в описании ОО рассматривают физические границы ОО: список всех аппаратных, программно-аппаратных, программных частей и руководств, которые составляют ОО. Этот список должен быть описан на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих частей» (ГОСТ Р ИСО/МЭК 15408-1, пункт А.4.3).

Следует рассмотреть этот список на предмет наличия в нем частей продукта, которые не предполагались в составе ОО, а также на предмет отсутствия каких-либо частей продукта, которые потенциальный потребитель ожидал обнаружить в составе ОО. Если соответствующие части продукта в список частей ОО не включены, то они и не подвергались оценке. Это следует учитывать потребителю при эксплуатации продукта.

В отношении логических границ в ГОСТ Р ИСО/МЭК 15408 указано, что «в описании ОО следует также рассмотреть логические границы ОО: логические характеристики безопасности, обеспечиваемые ОО, на уровне детализации, достаточном, чтобы обеспечить пользователю ЗБ общее понимание этих

характеристик. Предполагается, что данное описание будет более подробным, чем описание общих характеристик безопасности в аннотации ОО» (ГОСТ Р ИСО/МЭК 15408-1, пункт А.4.3).

В описании физических границ приводится список частей ОО, а в описании логических границ следует рассмотреть, что именно выполняет ОО. Краткое обсуждение этого вопроса приводилось в пункте «Использование и основные характеристики безопасности ОО» (см. 6.5.2), но там оно занимает лишь несколько абзацев, а в «Описании ОО» может занимать несколько страниц. Наиболее важная особенность этого раздела в том, что если от продукта ИТ ожидается наличие определенной функциональной возможности, например удаленного управления (например, потому что при рекламе продукта в отраслевом журнале описывалось наличие этой функциональной возможности), но в логических границах не упоминается удаленное управление, то функция удаленного управления, вероятнее всего, не подвергалась оценке и, следовательно, удаленное управление не следует учитывать, если потребитель планирует использовать продукт в оцененной конфигурации.

Поэтому важно тщательно изучить этот раздел для определения того, все ли требуемые характеристики продукта ИТ, относящиеся к безопасности, фактически подвергались оценке. Если это не так, то проведение оценки продукта ИТ не будет способствовать приобретению доверия к его функционированию в части таких характеристик.

6.5.4 Цели безопасности для среды функционирования

Среда функционирования представляет собой общее месторасположение, в котором будет размещен ОО (место размещения ОО). Для правильного функционирования ОО в этой среде функционирования должны быть реализованы определенные ограничения. Например, если ОО представляет собой межсетевой экран, этот ОО должен быть защищен от возможности физического доступа нарушителей. Такая защита может быть обеспечена самим ОО (например, защита от вскрытия), но в общем случае эту проблему следует решать именно в среде функционирования путем указания требований к размещению межсетевого экрана в изолированном защищенном серверном помещении.

Подобные требования к среде функционирования рассматриваются в ПЗ или ЗБ в разделе «Цели безопасности для среды функционирования». Цели безопасности для среды функционирования описывают, чего необходимо достичь в рамках среды функционирования ОО, чтобы ОО отвечал требованиям безопасности. Примеры целей безопасности для среды функционирования приведены в ГОСТ Р ИСО/МЭК 15408-1, пункт А.7.2.2.

Очень важное понимать, что цели — это не рекомендации, а необходимые условия для функционирования ОО согласно спецификации. Все эти цели (задачи) должны быть достигнуты в полной мере, и ответственность за их достижение возлагается на пользователя ОО или его организацию (например, оператора информационной системы); сам ОО не будет достигать этих целей. Если хотя бы одна из этих целей не достигается, может возникнуть ситуация, когда ОО будет функционировать в небезопасном режиме. Поэтому крайне важно сделать заключение о том, являются ли цели безопасности для среды достижимыми в организации пользователя ОО (у оператора информационной системы), и если хотя бы одна из целей недостижима, этот ОО не подходит для использования данным пользователем ОО (оператором информационной системы).

6.5.5 Подраздел «Утверждение о соответствии»

«Утверждение о соответствии» обычно находится в начале ПЗ или ЗБ. В раздел обычно включается одно предложение следующего вида:

Настоящий ПЗ (настоящее ЗБ):

- соответствует ГОСТ Р ИСО/МЭК 15408;
- соответствует ГОСТ Р ИСО/МЭК 15408-2 или является расширенным по отношению к ГОСТ Р ИСО/МЭК 15408-2;

В этой части «Утверждения о соответствии» определяется, каким образом составлены функциональные требования безопасности. С точки зрения потребителя оба варианта соответствия являются приемлемыми.

- соответствует ГОСТ Р ИСО/МЭК 15408-3 или является расширенным по отношению к ГОСТ Р ИСО/МЭК 15408-3;

В этой части «Утверждения о соответствии» определяется, каким образом сформированы требования доверия к безопасности. Для случая, когда ПЗ или ЗБ является расширенным по отношению к ГОСТ Р ИСО/МЭК 15408-3, разработчик ПЗ или ЗБ разрабатывает действия и шаги оценивания для соответствующих расширенных компонентов доверия к безопасности, а с точки зрения потребителя следует задаться вопросом, почему это было необходимо.

- соответствует перечню пакетов, о соответствии которым утверждается для ОО;

Наиболее распространенным является использование пакета ОУД1, ОУД2, ..., ОУД6 или ОУД7, часто с пометкой «усиленный» и (или) «расширенный». Более подробно ОУД рассмотрены в 6.5.7.

- соответствует перечню профилей защиты, о соответствии которым утверждается в ПЗ или ЗБ.

Более подробно это соответствие рассмотрено в 6.5.6.

6.5.6 Соответствие профилям защиты

Как было указано в 6.3.2.4, в ЗБ может утверждаться о соответствии ПЗ (хотя это и необязательно). Кроме того, в ПЗ может утверждаться о соответствии другим ПЗ. В случае подобных утверждений в рассматриваемом подразделе ПЗ или ЗБ приводится список ПЗ, о соответствии которым утверждается. Согласно ГОСТ Р ИСО/МЭК 15408 не допускается какая-либо форма частичного соответствия, таким образом, если в ПЗ или ЗБ заявлено о соответствии ПЗ, то ПЗ или ЗБ должен(но) полностью соответствовать профилю защиты (профилям защиты), на который(ые) имеется ссылка.

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

В ПЗ может содержаться утверждение о «строгом» или «демонстрируемом» соответствии ПЗ или ЗБ.

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

Строгое соответствие используется только для тех случаев, когда не допускается никаких различий между ПЗ и ЗБ, например, при процессе приобретения на основе выбора (см. 6.3.3). В ЗБ, подтверждающем строгое соответствие некоторому ПЗ, могут вводиться дополнительные ограничения по отношению к ограничениям, введенным в ПЗ.

В профилях защиты, утвержденных ФСТЭК России, устанавливаются следующие типы соответствия рассматриваемому ПЗ при разработке ЗБ на основе данного ПЗ:

- «строгое» соответствие — если рассматриваемый ПЗ является единственным ПЗ, утверждение о соответствии которому включено в ЗБ;
- «демонстрируемое» соответствие — если ОО является комплексным продуктом (изделием), и в ЗБ включено утверждение о соответствии (помимо настоящему ПЗ) другому (другим) ПЗ.

6.5.7 Оценочные уровни доверия и другие вопросы доверия

Разделы «Аннотация ОО» и «Описание ОО» позволяют получить сведения о том, что способен выполнять ОО, то есть о функциональных возможностях, которые он предоставляет. Однако невозможно в полной мере составить представление о продукте ИТ только на основании сведений о его функциональных возможностях. Продукты ИТ с одинаковыми общими функциональными возможностями могут использоваться в различных контекстах. Например, конструктивно одна и та же смарт-карта может быть использована как:

- билет на некоторое число поездок в транспорте;
- кредитная карта с кредитным лимитом в 500 000 рублей;
- средство контроля доступа на объект.

В первом случае достаточно и небольших усилий по обеспечению безопасности смарт-карты. Даже если нарушитель сможет обойти защиту смарт-карты, использующуюся для проезда на транспорте, то он сможет только некоторое время бесплатно совершать поездки, пока не будут изменены параметры карты. Риск недополучения доходов (при условии, что другие карты не были взломаны таким же образом) не будет иметь существенного значения для транспортной компании.

Во втором и третьем случаях требуется гораздо больше уверенности в правильности реализации функциональных возможностей карты, так как последствия обхода защиты даже одной такой карты могут быть значительными.

В ГОСТ Р ИСО/МЭК 15408 качество, которое дает основу для уверенности в том, что продукт ИТ отвечает целям безопасности, называется «доверие». Согласно ГОСТ Р ИСО/МЭК 15408 доверие оценивается с использованием активного исследования многих аспектов разработки продукта: процессов разработки и производства, проектов, руководств, объема испытаний (тестов), выполненных разработчиком продукта ИТ, и др.

ГОСТ Р ИСО/МЭК 15408 систематизирует доверие по двадцати семи категориям (так называемым «семействам доверия»). В каждой такой категории ГОСТ Р ИСО/МЭК 15408 определяет различные уровни соответствия.

Например, продукт ИТ может получить следующую оценку в зависимости от покрытия тестами разработчика:

- «0»: неизвестно, выполнял ли разработчик тестирование продукта;
- «1»: разработчик выполнил некоторое число тестов по отношению к отдельным интерфейсам продукта ИТ;
- «2»: разработчик выполнил некоторое число тестов по отношению ко всем интерфейсам продукта ИТ;
- «3»: разработчик выполнил очень большое число тестов по отношению ко всем интерфейсам продукта ИТ.

Из примера видно, что с каждым уровнем увеличивается степень прилагаемых усилий, а степень неопределенности уменьшается.

Для лица, не являющегося экспертом в области защиты информации, достаточно сложно правильно интерпретировать систему показателей, состоящую из индивидуальных показателей для всех двадцати семи категорий. Для того чтобы позволить лицам, не являющимся экспертами в области защиты информации, оценить доверие к продукту ИТ, в ГОСТ Р ИСО/МЭК 15408 имеются семь предопределенных уровней, называемых оценочными уровнями доверия (ОУД). Им присвоены идентификаторы по порядку от ОУД1 до ОУД7, где ОУД1 является самым низким уровнем доверия, а ОУД7 — самым высоким.

Каждый ОУД можно рассматривать как набор из двадцати семи чисел, по одному числу на каждую подкатегорию. Например, ОУД1 присваивает «1» тринадцати подкатегориям и «0» — остальным четырнадцати, в то время как ОУД2 присваивает «2» семи подкатегориям, «1» — одиннадцати подкатегориям, а оставшимся девяти — «0».

Все ОУД являются строго иерархическими, то есть если ОУД (*n*) присваивает определенный рейтинг доверия определенной подкатегории, то в ОУД (*n+1*) этой подкатегории будет присвоен такой же или более высокий рейтинг. Таким образом, ОУД (*n+1*) обеспечивает в целом больший уровень доверия, чем ОУД (*n*).

Приобретение более высокого уровня доверия в общем случае требует увеличения затрат. Если рассматривать покрытие тестами, как в приведенном выше примере, то «0» не будет означать отсутствие затрат, но для каждого более высокого показателя разработчик должен будет выполнять и документировать тесты, а оценщик должен будет определить, правильно ли разработчик провел и задокументировал эти тесты и т. д. С одной стороны, повышение уровня доверия почти всегда означает увеличение затрат, с другой стороны, большее доверие уменьшает риск того, что заявленная функциональная возможность не реализуется должным образом или содержит потенциальные пригодные для использования уязвимости.

В профилях защиты, утвержденных ФСТЭК России, оценочные уровни доверия используются с дополнениями:

- усиливаются компонентами не использовавшейся в данном ОУД категории (семейства);
- усиливаются заменой компонентов на более высокие по иерархии компоненты одной подкатегории (семейства);
- расширяются с использованием компонентов, не входящих в ГОСТ Р ИСО/МЭК 15408-3, то есть расширенных (специальных) компонентов.

При этом итоговые наборы требований доверия (усиленные и расширенные ОУД) применяются для соответствующих классов защиты, устанавливаемых в нормативных правовых актах ФСТЭК России. Типовой состав компонентов доверия в зависимости от класса защиты средств защиты информации представлен в 12.4.1.

7 Спецификация раздела «Введение» в профилях защиты и заданиях по безопасности

В данном разделе представлены рекомендации по спецификации раздела «Введение» в ПЗ и ЗБ.

«Введение» в ПЗ состоит из следующих элементов:

а) ссылка на ПЗ;

б) аннотация ОО.

«Введение» в ЗБ состоит из следующих элементов:

а) ссылка на ЗБ;

б) ссылка на ОО;

в) аннотация ОО;

г) описание ОО.

Разработчику ПЗ или ЗБ может быть не сразу очевидно, какую информацию включать в пункт «Использование и основные характеристики безопасности ОО» подраздела «Аннотация ОО». Лучшее понимание «использования ОО» может быть получено путем обобщения определения проблемы безопасности из ПЗ или ЗБ (см. раздел 9), в то время как большинство «характеристик безопасности ОО» описываются лучше всего путем обобщения целей безопасности для ОО. Такой подход обеспечивает согласованность раздела «Введение» с другими, более детальными частями ПЗ или ЗБ.

Разработчикам ПЗ или ЗБ проще всего окончательно оформить раздел «Введение» после того, как будут написаны остальные разделы ПЗ или ЗБ.

В ГОСТ Р ИСО/МЭК 15408-1 (подразделы А.4 и В.4) вопросы разработки раздела «Введение» в ПЗ и ЗБ рассматриваются достаточно подробно.

8 Спецификация раздела «Утверждения о соответствии»

В данном разделе представлены рекомендации по спецификации раздела «Утверждения о соответствии» в ПЗ или ЗБ. Раздел ЗБ «Утверждения о соответствии» описывается в ГОСТ Р ИСО/МЭК 15408-1 (подраздел А.5), а отличия раздела ПЗ «Утверждения о соответствии» от аналогичного раздела ЗБ описываются в ГОСТ Р ИСО/МЭК 15408-1 (подраздел В.5).

В разделе «Утверждения о соответствии» в ПЗ или ЗБ описывается соответствие профиля защиты или задания по безопасности:

а) ГОСТ Р ИСО/МЭК 15408. В текст раздела включается указание точной редакции ГОСТ Р ИСО/МЭК 15408, которая была использована для разработки (и, возможно, также для оценки) ПЗ или ЗБ. Если использовался отличный от национального стандарта ГОСТ Р ИСО/МЭК 15408 перевод ISO/IEC 15408 (например, РД БИТ [5]), это также должно быть указано. Если были использованы редакции ГОСТ Р ИСО/МЭК 15408 с какими-либо внесенными исправлениями или иные сопутствующие документы, информация об этом должна быть указана;

б) профилям защиты. В текст раздела включается перечисление профилей защиты, о соответствии которым утверждается в ПЗ или ЗБ. Достаточно привести список ПЗ. Приводить дополнительную информацию в данном разделе не требуется;

в) пакетам требований безопасности. В текст раздела включается перечисление пакетов требований безопасности, на которые даны ссылки в ПЗ или ЗБ. Обычной практикой является утверждение соответствия одному из пакетов доверия (ОУД), определенному в ГОСТ Р ИСО/МЭК 15408-3, возможно, с усилением и расширением. Использование пакетов рассмотрено далее в 15.3. В данном случае также просто достаточно списка; приводить дополнительную информацию в данном разделе не требуется.

Указанные утверждения также применимы к ОО, основанному на соответствующем ПЗ или ЗБ.

Современные продукты ИТ могут быть комплексными изделиями. Например, один продукт ИТ может реализовывать функциональность системы обнаружения вторжений и средства антивирусной защиты. В этом случае разработчик (заявитель) может быть заинтересован в проведении сертификации продукта ИТ как по требованиям для систем обнаружения вторжений, так и по требованиям для средств антивирусной защиты. Для этого заявитель может включить в задание по безопасности утверждения о соответствии сразу двум профилям защиты (для СОВ и САВЗ).

При разработке ПЗ следует определить, каким образом другие ПЗ и ЗБ должны соответствовать данному ПЗ. Возможны два типа соответствия:

а) строгое. По сути, оно означает, что ПЗ или ЗБ, соответствующие рассматриваемому ПЗ, должны полностью соответствовать ему по содержанию. Подробные требования по этому вопросу приведены в ГОСТ Р ИСО/МЭК 15408-1 (подраздел 8.3);

б) демонстрируемое. По сути, оно означает, что ПЗ или ЗБ, соответствующие рассматриваемому ПЗ, должны быть «эквивалентны» ему. Подробные требования и для этого случая приведены в ГОСТ Р ИСО/МЭК 15408-1 (подраздел 8.3).

Разработчикам ПЗ, которые разрабатывают его в качестве точной и полной спецификации продукта ИТ, приобретаемого или создаваемого (разрабатываемого) для собственного использования,

следует требовать строгого соответствия. При разработке ПЗ с другой целью допускается использовать и «демонстрируемое» соответствие.

Если утверждается о соответствии функциональному пакету или другому ПЗ, то определение проблемы безопасности, цели безопасности и требования безопасности должны быть совместимы с этим пакетом или ПЗ.

Если разработчики ПЗ или ЗБ включают дополнительные требования к приведенным в ПЗ, на который дана ссылка, то им следует удостовериться, что не возникает таких противоречий между требованиями, в результате которых ни один ОО не сможет реализовать все требования одновременно.

В ПЗ, утвержденных ФСТЭК России, принят следующий подход к определению типов соответствия при разработке ЗБ и (или) других ПЗ на основе утвержденного профиля защиты:

- требуется «строгое» соответствие профилю защиты — если рассматриваемый ПЗ является единственным ПЗ, утверждение о соответствии которому включено в ЗБ;
- допускается «демонстрируемое» соответствие профилю защиты — если ОО является комплексным продуктом (изделием) и в ЗБ включено утверждение о соответствии (помимо рассматриваемому ПЗ) другому (другим) ПЗ.

В настоящее время действуют различные типы нормативных и методических документов ФСТЭК России, определяющие требования к средствам защиты информации:

- нормативные правовые акты и профили защиты (например, для средств контроля съемных машинных носителей информации, межсетевых экранов, операционных систем), разработанные в соответствии с действующей редакцией ГОСТ Р ИСО/МЭК 15408 (2012, 2013 гг.);
- нормативные правовые акты и профили защиты (например, для средств антивирусной защиты, систем обнаружения вторжения, средств доверенной загрузки), разработанные в соответствии с редакцией ГОСТ Р ИСО/МЭК 15408 (2008 г.);
- руководящие документы ФСТЭК (Гостехкомиссии) России, такие как «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (1992 г.), «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» (1999 г.);
- другие документы, определяющие в том числе требования к техническим мерам и средствам защиты информации, такие как «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [6], «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [7], «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [8].

Формат, структура и стиль изложения требований к средствам защиты информации в этих документах могут отличаться. В этих условиях при подготовке к сертификации комплексного изделия, которое должно соответствовать требованиям сразу нескольких нормативных и (или) методических документов, наиболее подходящим способом объединения требований всех этих документов представляется разработка единого задания по безопасности на изделие.

При этом целесообразно руководствоваться следующими правилами:

1) При необходимости соответствия нескольким ПЗ, разработанным в соответствии с разными редакциями ГОСТ Р ИСО/МЭК 15408, следует разрабатывать ЗБ в соответствии с действующей редакцией ГОСТ Р ИСО/МЭК 15408.

Примечание — Необходимо учитывать, что впоследствии оценка ЗБ будет проводиться по требованиям класса ASE действующей редакции ГОСТ Р ИСО/МЭК 15408. В отдельных случаях возможна разработка единого задания по безопасности в соответствии с РД БИТ.

2) При необходимости соответствия ПЗ разным редакциям ГОСТ Р ИСО/МЭК 15408 требования доверия к безопасности в ЗБ можно определить следующим способом.

За основу следует взять пакет доверия из ПЗ, разработанного в соответствии с действующей редакцией ГОСТ Р ИСО/МЭК 15408. При этом автоматически обеспечивается покрытие требований других пакетов доверия из ранее выпущенных ПЗ для соответствующего класса защиты. Например, если необходимо соответствие изделия профилю защиты для САВЗ (по ГОСТ Р ИСО/МЭК 15408—2008)

и профилю защиты для СКН (по ГОСТ Р ИСО/МЭК 15408—2012, 2013), то необходимо в качестве основы требований доверия в ЗБ использовать пакет доверия из ПЗ для СКН.

Примечание — Необходимо учитывать, что впоследствии оценка ОО будет осуществляться в соответствии с действующей редакцией ГОСТ Р ИСО/МЭК 18045 (в частности, для приведенного выше примера по ГОСТ Р ИСО/МЭК 18045—2013).

Затем в ЗБ следует добавить в пакет доверия требования доверия (расширенные компоненты, уточнения стандартных компонентов) из ПЗ, разработанного по предыдущей редакции ГОСТ Р ИСО/МЭК 15408, для отражения специфики доверия к соответствующим механизмам ЗИ. Для приведенного выше примера с ПЗ для САВЗ и ПЗ для СКН в состав требований доверия в ЗБ комплексного изделия необходимо включить компоненты доверия ALC_UPV_EXT.1 «Процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов)» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства антивирусной защиты» из ПЗ для САВЗ (по ГОСТ Р ИСО/МЭК 15408—2008);

3) Если в состав комплексного изделия включены механизмы, требования к которым изложены в форме, отличной от ПЗ, то соответствующие требования излагаются в стиле компонентов требований по ГОСТ Р ИСО/МЭК 15408-2 и (или) ГОСТ Р ИСО/МЭК 15408-3 и включаются в задание по безопасности.

9 Спецификация раздела «Определение проблемы безопасности»

9.1 Введение

В данном разделе приведено руководство по спецификации раздела «Определение проблемы безопасности» (ОПБ) в ПЗ или ЗБ. В ГОСТ Р ИСО/МЭК 15408-1 (подразделы А.6 и В.6) описывается спецификация раздела «Определение проблемы безопасности» для ЗБ и ПЗ соответственно. При этом в подразделе В.6 просто приводится ссылка на подраздел А.6, что можно считать подтверждением того, что ожидаемое содержание раздела «Определение проблемы безопасности» одинаково для ПЗ и ЗБ. Действительно, формулировки соответствующих критериев оценки в ГОСТ Р ИСО/МЭК 15408-3 идентичны.

Целью определения проблемы безопасности является формализованное определение характера и масштаба проблемы безопасности, которую должен решать ОО (см. рисунок 1).

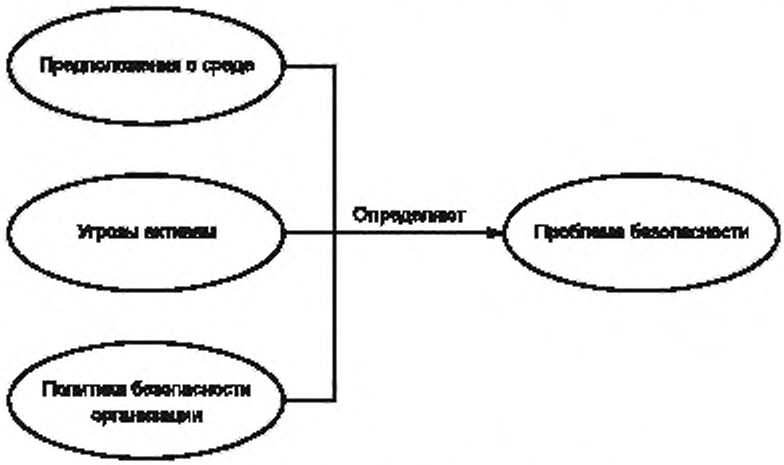

Рисунок 1 — Определение проблемы безопасности

В тех ПЗ и ЗБ, в структуре которых предусмотрен раздел «Определение проблемы безопасности», данный раздел является одним из наиболее важных разделов. Ниже приведен соответствующий фрагмент из ГОСТ Р ИСО/МЭК 15408-1 (пункт А.6.1):

«Полноценность результатов оценки в существенной степени зависит от ЗБ, а полноценность ЗБ в существенной степени зависит от качества определения проблемы безопасности. Поэтому зачастую

необходимо потратить существенные ресурсы и использовать четкие процессы и процедуры анализа, чтобы получить соответствующее определение проблемы безопасности».

Если проблема определена неправильно или описана нечетко, то остальные части ПЗ или ЗБ также будут являться неправильными. Что еще хуже, на основании технически правильной, но неподходящей спецификации может быть выбран или приобретен продукт не тот, который нужен. Поэтому в настоящем стандарте раздел 9 является одним из самых объемных и наиболее подробных, хотя описанным в нем критериям в ГОСТ Р ИСО/МЭК 15408 отведено только две или три страницы текста. Для разработчика и для заказчика независимо от того, будет ли ПЗ или ЗБ использоваться в процессе приобретения на основе спецификации или в процессе приобретения на основе выбора, правильное определение проблемы безопасности имеет первостепенное значение.

В последующих разделах ПЗ и ЗБ демонстрируется, каким образом ОО совместно с его средой функционирования будет решать проблему безопасности. Поэтому важно удостовериться, что определение проблемы безопасности является четким, кратким и внутренне непротиворечивым.

ГОСТ Р ИСО/МЭК 15408 не предполагает и не предписывает использование какого-либо конкретного процесса или методического подхода к определению проблемы безопасности. В данном разделе настоящего стандарта представлено подробное описание простого методического подхода, который был опробован и испытан на практике и показал свою работоспособность в различных организациях и средах функционирования. Он основан на выполнении ряда последовательных шагов:

а) идентификация и подтверждение неформализованных требований безопасности;

б) идентификация и спецификация актуальных угроз на основе выполнения формализованного анализа угроз;

в) документирование применимых политик;

г) документирование применимых предположений;

д) доработка и проверка спецификации определения проблемы безопасности.

Независимо от используемого методического подхода настоящий стандарт предполагает, что определение проблемы безопасности представляет формализованное описание существующих неформализованных требований безопасности. На практике неформализованные требования безопасности могут и не быть отражены в одном-единственном документе; такого документа может и вовсе не существовать. Таким образом, первым шагом (согласно рекомендуемому методическому подходу) являются идентификация и подтверждение неформализованных требований безопасности, даже если они не приводятся в ПЗ или ЗБ. Неформализованные требования могут быть очевидными и полностью определенными. В других случаях значительной частью деятельности по разработке определения проблемы безопасности может быть идентификация неформализованных требований и получение подтверждения со стороны руководства и других заинтересованных сторон, что данные неформализованные требования безопасности являются корректным и полным представлением потребностей в безопасности для данной организации.

В предложенном методическом подходе рассматриваются также два других аспекта, которые не требуются в обязательном порядке согласно ГОСТ Р ИСО/МЭК 15408, но которые, как показала практика, позволяют сэкономить время и избежать противоречий на последующих стадиях разработки ПЗ или ЗБ, а именно:

а) документирование угроз, которым может противостоять ОО (угроз, которым изначально противостоять не планировалось);

б) разработка обоснования для прослеживания определения проблемы безопасности к неформализованным требованиям безопасности.

Оба этих аспекта подробно рассматриваются в соответствующих пунктах методического подхода. Угрозы, не рассматриваемые как применимые — это угрозы, которые могут быть применимыми либо неприменимыми для данного продукта, но которым в случае, если они применимы, противостоят функциональные возможности безопасности, уже включенные в ОО по иным причинам. Если такие угрозы не документируются в определении проблемы безопасности, то они, вероятнее всего, вызовут вопросы при анализе ПЗ или ЗБ. Более того, в случае изменения требования некоторая функциональная возможность может быть исключена без учета ее значения для покрытия угроз, не рассматривавшихся как применимые.

С точки зрения оценки определение проблемы безопасности рассматривается как не требующее доказательств: не предпринимается попыток прослеживания определения проблемы безопасности к фактическим потребностям в безопасности. В случае если не приводится никакого обоснования определения проблемы безопасности, существует риск того, что в процессе формирования определения

проблемы безопасности могут быть упущены некоторые аспекты неформализованных требований, и это не будет обнаружено до начала использования продукта, когда выяснится, что продукт не соответствует предназначению. Следовательно, обоснование представляет собой важный критерий проверки согласованности и полноты.

Общий принцип состоит в том, что при определении проблемы безопасности следует по возможности избегать рассмотрения характеристик ОО, направленных на удовлетворение требований, например, подробностей, связанных с функциями безопасности ОО. Соблюдение этого принципа помогает сконцентрировать внимание пользователя документа на важных аспектах проблемы безопасности. Рассмотрение того, каким образом ОО будет решать проблему безопасности, следует приводить в последующих частях ПЗ или ЗБ. Когда конкретное решение предписывается как часть неформализованного требования безопасности, то такое решение должно быть указано как часть определения проблемы безопасности для того, чтобы обеспечить его документирование, а также для обоснования ограничений последующих проектных решений.

9.2 Определение неформализованных требований безопасности

9.2.1 Введение

В отношении проблемы безопасности и ее предполагаемого решения всегда существует ряд аспектов, которые зафиксированы и известны до начала определения проблемы безопасности. Такие требования и ограничения составляют неформализованные требования безопасности. Идентифицировать и документировать такие аспекты всегда достаточно проблематично. Поэтому именно это является первым шагом рекомендуемого методического подхода.

9.2.2 Источники информации

9.2.2.1 Аннотация

Существует множество способов идентификации описанных выше аспектов неформализованных требований безопасности. В следующих пунктах рассматриваются некоторые из них. Для конкретной организации могут существовать и другие аспекты, которые невозможно идентифицировать по общему методическому подходу в соответствии с описанием в настоящем стандарте. Необходимо, чтобы потребности в безопасности были внимательно и тщательно обдуманы. Предложенные в данном пункте возможные источники информации должны в этом помочь.

9.2.2.2 Требуемые функциональные возможности

Функциональные возможности безопасности могут быть частью предназначения рассматриваемого продукта. Особенно это относится к готовым к использованию продуктам, где службы и сервисы безопасности, которые должны быть доступны покупателю через интерфейсы прикладных программ (API) или человекомашинные интерфейсы, могут быть значимой частью спецификации продукта.

Если функциональные возможности безопасности являются частью документированного требования пользователей, то их предоставление является частью проблемы, учитываемой при определении проблемы безопасности.

9.2.2.3 Оценка риска

Оценка рисков безопасности могла быть проведена с учетом предполагаемой системы и даже готового к использованию продукта, и могли заранее быть идентифицированы риски, которые подлежат снижению посредством применения мер обеспечения безопасности. Эти риски представляют часть проблемы безопасности.

Существуют различные методические подходы к оценке рисков. Обычно согласно этим методическим подходам предполагается, что для существования риска должны иметься в наличии: имеющий ценность актив, которому может быть нанесен некоторый ущерб, угроза (источник угрозы) — что-либо или кто-либо, что (кто) может нанести ущерб активу, и уязвимость — аспект, посредством которого может быть нанесен ущерб активу. Если какое-либо из указанных трех условий отсутствует, то риск отсутствует. Такой вид модели предполагается в ГОСТ Р ИСО/МЭК 15408. Если в действительности при оценке рисков была использована иная модель рисков, то могут возникнуть проблемы с отражением результатов оценки рисков в подходящую для использования в определении проблемы безопасности форму.

9.2.2.4 Оценка угроз

Оценка угроз представляет собой упрощенную форму оценки рисков, когда предполагается, что если существует угроза, то активы могут быть повреждены и, таким образом, риск тоже будет существовать. В этом случае идентифицированные угрозы представляют собой часть проблемы безопасности.

Оценка угроз особенно уместна, когда лицо, пытающееся идентифицировать и специфицировать проблему безопасности, не является владельцем активов, которые подлежат защите и, следовательно, не в состоянии выполнить оценку рисков или определить ценность активов.

9.2.2.5 Политика руководства

Требование безопасности может вытекать из политики, принятой решением руководства, например, что во всех системах в конкретной организации должны применяться определенные стандартизированные меры обеспечения безопасности ИТ. Такой процесс называют иногда «политикой минимальных стандартов» или «уклонением от рисков». Политика может быть выбранной произвольно, например, соответствовать примеру аналогичных организаций, или может быть логически обоснованной, например, с целью удовлетворения требований законодательства или договорных условий, установленных заказчиками.

9.2.2.6 Презентационная политика

Требование безопасности может появиться как результат стремления продемонстрировать, что организация или готовый к использованию продукт реализует определенные меры обеспечения безопасности ИТ. Такая политика может возникнуть вследствие потребностей рынка или из желания следовать передовой практике.

Проблемы безопасности такого типа хорошо согласуются с оценкой по ГОСТ Р ИСО/МЭК 15408, так как успешная оценка с привлечением аккредитованной испытательной лаборатории позволяет получить официальный сертификат, обеспечивающий независимое подтверждение наличия мер обеспечения безопасности. Для идентификации мер могут использоваться опубликованные ПЗ.

Недостатком политик такого типа является то, что они основаны на стремлении получить сертификат или продемонстрировать соответствие, а не на выборе мер обеспечения безопасности, соответствующих рассматриваемому продукту. Это может привести к возникновению проблем в процессе поиска причин, включаемых в определение проблемы безопасности и обосновывающих потребности в тех или иных мерах обеспечения безопасности. Такие политики, возможно, придется рассматривать как «политические» решения, причем лицо, принимающее решение, может неохотно признавать истинную причину их выбора.

9.2.2.7 Политика оценки

В организации может быть принята политика, согласно которой продукты ИТ оцениваются в системе сертификации в соответствии с ГОСТ Р ИСО/МЭК 15408, РД БИТ или документами, на них основанными, независимо от того, какие меры безопасности реализуются в продуктах ИТ.

9.2.3 Документирование неформализованных требований

Лучшим источником информации относительно проблемы безопасности являются результаты оценки рисков безопасности. При возможности доступа к результатам оценки рисков следует учитывать, что они, скорее всего, будут всесторонними, к тому же большинство методических подходов к оценке рисков вводят понятие пропорциональности, что означает, что некоторые риски могут быть приемлемы в случаях, когда вероятность ущерба очень низка или последствия ущерба не являются значимыми. Выявление как приемлемых, так и неприемлемых рисков позволит в дальнейшем уточнить проблему безопасности в ходе разработки проекта.

При оценке рисков третьей стороной ее отношение к риску может отличаться от принятого в организации заказчика. В подобных случаях такие результаты следует использовать с осторожностью.

Если описание части проблемы в терминах риска невозможно, то оно почти наверняка будет иметь произвольную основу, которая не может быть изменена или усовершенствована. Важно, чтобы это было четко отражено в неформализованном описании.

Рассматриваемая информация может касаться не только продукта ИТ, но также и его среды функционирования. Среда функционирования определяет уровень доверия, который может быть установлен для организационных и физических мер обеспечения безопасности. Потребности в безопасности для мест общего доступа значительно отличаются от потребностей в безопасности для изолированного серверного помещения. Если было установлено, что предполагается наличие некоторых организационных и физических мер обеспечения безопасности, то это должно быть важной частью определения проблемы безопасности.

Наряду со сведениями о рисках и мерах обеспечения безопасности могут быть приняты определенные проектные решения в отношении того, каким образом предполагается реализовать конкретные функциональные возможности безопасности: например, может быть принято решение использовать биометрическую аутентификацию, а не аутентификацию на основе ввода пароля, или использовать конкретные протоколы передачи данных, которые определяют характеристики безопасности.

Некоторые части проблемы безопасности могут быть нерешаемыми техническими средствами; для решения этих частей проблемы могут быть использованы только имеющие отношения к персоналу организационные и физические меры обеспечения безопасности. Но, несмотря на это, они являются частью проблемы безопасности и должны быть документированы. На самом деле любой аспект проблемы безопасности, в отношении которого было принято решение, должен быть документирован как часть неформализованного требования безопасности.

После идентификации, упорядочивания и проверки на внутреннюю непротиворечивость всей доступной информации ее следует классифицировать по трем областям:

а) потенциально возможные атаки, которым должен противостоять продукт ИТ;

б) атрибуты безопасности или характеристики безопасности, которыми должен обладать продукт ИТ;

в) атрибуты или характеристики безопасности, которые не являются необходимыми для продукта ИТ.

Такая классификация необходима для организации дальнейшего анализа полученной информации. Потенциально возможные атаки должны рассматриваться как угрозы для ОО, и он должен им противостоять. Атрибуты безопасности и характеристики безопасности, которыми должен обладать продукт, в том числе предписанные решения по безопасности, соотносятся с политиками безопасности организации. Атрибуты и характеристики, которые не являются необходимыми для продукта, соотносятся с предположениями. Эти категории будут рассмотрены подробнее.

Различные части неформализованного требования, полученные из разных источников, могут перекрываться или даже быть противоречивыми. Атрибуты и характеристики безопасности могут определяться в качестве подсознательной реакции на идентифицированные потенциальные атаки. Аналогично определенные типы атак могут подсознательно быть сочтены слишком сложными или требующими слишком больших затрат для эффективного противостояния им, вследствие чего связанные с ними характеристики безопасности объявляются необязательными. Такие несоответствия необходимо устранить до продолжения работы с неформализованной спецификацией. Следует стремиться к изложению каждого аспекта неформализованного требования один и только один раз.

9.3 Идентификация и спецификация угроз

9.3.1 Введение

После документирования неформализованного требования безопасности и идентификации атак и атрибутов безопасности следующим логическим шагом подготовки определения проблемы безопасности является проведение анализа угроз для идентификации угроз, представленных потенциальными атаками. ГОСТ Р ИСО/МЭК 15408 не предписывает какого-либо конкретного методического подхода к идентификации применимых угроз. Однако используемый методический подход должен идентифицировать все угрозы, значимые для рассматриваемого ОО.

Анализ и спецификация угроз обычно являются более сложными и трудными, чем определение политики и предположений, поэтому целесообразнее проводить их в первую очередь. С другой стороны, если неформализованные требования были в основном получены как производные от решений по поводу политик или предписанных требований (см. 9.2), то может быть проще вначале разработать проект политик и предположений (см. 9.4 и 9.5), затем выполнить описываемый в данном разделе анализ угроз, пересмотреть и завершить разработку политик и предположений. Если политики и предположения могут быть легко идентифицированы, в таком случае они могут быть использованы для исключения угроз из дальнейшего рассмотрения, что значительно упростит анализ угроз.

Для проведения анализа угроз необходимо:

а) принять решение, какой методический подход к проведению анализа будет использоваться;

б) идентифицировать аспекты угроз согласно выбранному методическому подходу;

в) применить методический подход.

В последующих пунктах данного подраздела в порядке очередности рассматриваются эти виды деятельности.

9.3.2 Выбор методологии анализа угроз

Выбор методического подхода к идентификации применимых угроз будет зависеть от того, каким образом было получено неформализованное требование безопасности. Если требование было специфицировано в терминах результатов оценки рисков, то список угроз может быть уже доступен как один из результатов оценки рисков. Даже в ином случае есть возможность идентифицировать значимые угрозы на основании другой доступной информации.

В ряде случаев информация в необходимом и достаточном объеме не будет доступна, и возникнет необходимость в проведении дополнительного анализа угроз.

Существуют различные методические подходы, которые могут быть использованы для проведения анализа угроз. Однако большинство разработчиков ПЗ и ЗБ используют один из трех методов:

а) анализ дерева угроз;

б) поиск по базе данных угроз;

в) специальная идентификация.

Из перечисленных методических подходов анализ дерева угроз является наиболее документированным и отработанным методом. Он основан на построении деревьев решений, хорошо известном методе декомпозиции проблемы, который широко используется в процессах управления рисками и технике обеспечения надежности.

Вследствие того, что это отработанный и хорошо документированный метод, в настоящем стандарте анализ дерева угроз не будет подробно описываться. Однако, если говорить простыми терминами, он предусматривает вначале очень общее, абстрактное описание полного набора потенциальных угроз, применимых для данного типа продукта ИТ, а затем итерационное увеличение детализации, с уточнением описания угроз на каждом этапе. Такой метод называется деревом угроз, так как первоначальное абстрактное описание рассматривается как корень дерева, а каждый новый уровень последовательного уточнения создает набор новых, более детализированных узлов, связанных с этим корнем. Каждый из узлов затем становится корнем нового поддерева. В итоге описания конечных узлов будут достаточно конкретными и не требующими дальнейшего уточнения и будут использоваться как реальные угрозы, специфицируемые в ПЗ или ЗБ. Такой метод предоставляет также обоснование выбора угроз, включаемых в ПЗ или ЗБ, и дает уверенность в том, что никакие из значимых угроз не были пропущены.

Следует учитывать, что лицам, не являющимся экспертами в области безопасности, может быть достаточно трудно строить точные и внутренне непротиворечивые деревья угроз.

Второй вариант — поиск по базе данных — основан на исчерпывающем анализе одной или нескольких предопределенных баз данных общих угроз для того, чтобы рассмотреть, какие элементы из базы данных соответствуют атакам для рассматриваемого продукта ИТ. Базы данных, подходящие для выполнения этой задачи, могут быть получены из различных источников. Большинство национальных систем оценки предоставляют информацию относительно общих угроз по запросу, и, как правило, это делается в форме базы данных с возможностью поиска по ней.

В настоящее время ФСТЭК России разработана и поддерживается национальная база данных угроз безопасности информации с помещением информации на общедоступном ресурсе.

Поиск по базе данных имеет ряд преимуществ и недостатков. Преимуществом является то, что при этом может быть рассмотрен достаточно большой диапазон угроз, а также то, что все они определены в унифицированной форме. Одним из ограничений является возможность наличия специфических угроз для конкретного продукта, которые не охватываются базой данных и, следовательно, не будут идентифицированы при использовании данного метода. Кроме того, описания угроз в базе данных могут быть слишком общими для применения их к рассматриваемому продукту с целью идентификации угроз. Также может выясниться, что применимо окажется слишком большое число угроз, что приводит к возникновению определенной степени произвольности выбора.

Третий вариант — специальная идентификация — состоит в выявлении угроз неструктурированным образом на основе изучения рассматриваемого продукта ИТ. Этого лучше избегать — разработчику или лицу, ответственному за решение проблемы, трудно мыслить нестандартно. У нарушителя может быть больше опыта или изобретательности при поиске применимых реализуемых угроз.

Если и проблема безопасности, и среда четко определены, то построение дерева угроз обычно является наиболее эффективным методом. Если проблема определена в общих терминах либо среда является неопределенной или произвольно определенной, то простой последовательный поиск угроз по базе данных будет более эффективным при предложении применимых угроз, чем методический нисходящий анализ. В особенности это относится к разработчикам готовых к использованию (широко тиражируемых) продуктов. Они, как правило, не обладают достаточными знаниями о фактических условиях, в которых будут использоваться их продукты ИТ.

Если неформализованное требование безопасности было обусловлено прежде всего политикой или предписанными характеристиками безопасности, то анализ может не выявить никаких применимых угроз, которым еще не противостоят требуемые атрибуты безопасности.

В зависимости от используемого методического подхода к проведению анализа угроз, а также происхождения неформализованного требования безопасности, угрозы могут быть идентифицированы,

но исключены из рассмотрения, или идентифицированы как дубликаты других требований (например, политик). ГОСТ Р ИСО/МЭК 15408 не требует, чтобы такие угрозы были документированы каким-либо образом, но затем может быть очень трудно понять определение проблемы безопасности в целом, в частности трудно будет модифицировать его так, чтобы отразить последние изменения. Настоящим стандартом настоятельно рекомендуется документировать даже признанные несущественными и исключенные из рассмотрения угрозы. Обычно это делается в рамках раздела предположений определения проблемы безопасности (см. 9.5).

9.3.3 Идентификация аспектов угроз

9.3.3.1 Введение

Результаты анализа рисков или угроз, а также другие формы описаний атак и векторов атак не всегда описываются в терминах источников угрозы, активов и негативных действий, вследствие чего необходимо разработать описание, требуемое согласно ГОСТ Р ИСО/МЭК 15408, на основе первоисточников с использованием доступной информации об угрозах и атаках.

9.3.3.2 Источники угроз

Согласно определению в ГОСТ Р ИСО/МЭК 15408, источники угроз — «сущности, которые негативно воздействуют на активы». При этом отсутствует какое-либо руководство по спецификации источников угроз или требуемому уровню детализации и точности описаний. При описании угроз в ПЗ и ЗБ целесообразно придерживаться как можно более простого описания источников угроз. Один из общепринятых методов, рекомендуемый рассматриваемым методическим подходом, состоит в том, чтобы использовать фиксированный список, содержащий пять типов источников угроз:

а) нарушители;

б) уполномоченные пользователи;

в) привилегированные пользователи;

г) администраторы;

д) владельцы и разработчики системы.

Нарушитель — это лицо, которому не разрешен доступ к активам, защищаемым продуктом ИТ. К этой же категории относятся лица, которые являются уполномоченными пользователями, но не прошли идентификацию и аутентификацию. Поскольку они неизвестны владельцу системы, их мало что удерживает от вредоносных действий, за исключением того случая, когда атака обнаружена и увязывается с идентифицированным лицом, например, с помощью отслеживания по телефону или визуальной идентификации сотрудниками службы охраны.

Уполномоченный пользователь — это лицо, которому разрешено использовать продукт ИТ в соответствии с политикой безопасности и которое может получить доступ к активам, защищаемым продуктом, с разрешения владельца этих активов. Уполномоченные пользователи известны владельцу информационной системы, что удерживает их от нанесения ущерба активам, так как они несут ответственность за свои действия.

Привилегированный пользователь — это лицо, которому разрешено использовать продукт ИТ вопреки общей политике безопасности и которое может получить доступ к информационным активам без явного разрешения владельца активов. К таким привилегированным пользователям относятся, например, системные администраторы. Однако существуют и другие типы привилегированных пользователей — например, инженеры по техническому обслуживанию аппаратного и программного обеспечения. Продукт ИТ не может противостоять попыткам привилегированного пользователя нанести ущерб информационному активу, но впоследствии пользователь может быть привлечен к ответственности за свои действия.

Под администратором понимается лицо, на которое возложена ответственность за обеспечение правильного функционирования продукта ИТ после его установки в среду функционирования. Администраторы несут ответственность за внедрение мер, предотвращающих и обнаруживающих попытки нанесения ущерба активам. Администраторы могут быть ограничены в своих действиях, но при неправильном выполнении ими своих обязанностей другие лица могут нанести ущерб информационным активам.

Под владельцем системы и разработчиком понимаются лица, которые несут ответственность за спецификацию, проектирование и реализацию системы или готового к использованию продукта ИТ, но не обязательно используют продукт ИТ для доступа к защищаемым этим продуктом активам. Хотя в случае принятия неправильных решений эти лица не могут напрямую нанести ущерб активам, но продукт ИТ может при этом оказаться не способен в достаточной мере защитить активы.

В соответствии с этими определениями одно и то же лицо может в различное время быть отнесено к разным из перечисленных категорий. Это связано с тем, какой именно тип угроз они представляют, выступая в качестве источника угрозы.

Из приведенного выше списка исключен один из возможных типов источников угроз, который может быть значимым для некоторых проблем безопасности — стихийные бедствия (иногда называемые форс-мажорными обстоятельствами), например, землетрясения. При этом человек не выступает в качестве источника угроз. Общепринятый подход состоит в том, чтобы возложить ответственность за рассмотрение таких угроз на владельца или разработчика системы, хотя они не вовлечены при этом в подготовку или реализацию атак. В некоторых случаях предпочтительнее указать вместо источника угрозы «источник угрозы отсутствует» либо «стихийные факторы».

9.3.3.3 Типы активов

Активы имеют важное значение для анализа угроз, и их следует идентифицировать соответствующим образом. Большинство методических подходов к проведению анализа угроз могут успешно применяться даже с учетом недостаточной точности или частичного перекрытия описаний аспектов угроз (источников угроз) или негативных действий, но активы должны быть отделены друг от друга и подробно описаны. Далее предложен подробный методический подход к идентификации активов или типов активов, которые необходимо защищать с помощью конкретного продукта ИТ.

В большинстве случаев можно четко идентифицировать, какие активы подлежат защите, поскольку это составляет часть определения системы. Для случая готового к использованию продукта часто неизвестно фактическое использование продукта, и поэтому могут быть идентифицированы только типы активов, для защиты которых предназначен данный продукт.

Активы, связанные с системами ИТ, обычно относятся к одному из трех классов:

а) информационные активы;

б) процессы;

в) физические активы.

Информационные активы являются данными, представляющими ценность для организации — владельца активов (оператора). Примерами возможных типов информационных активов являются:

- данные общего характера;
- системные данные;
- специализированные базы данных;
- клиентские данные.

Базы данных специалистов обычно содержат информацию, представляющую ценность только для некоторых пользователей. Примерами может служить база данных по кадрам (представляющая ценность только для отдела кадров) или база данных по заказчикам (представляющая ценность только для отдела обработки заказов и коммерческого отдела). Клиентские данные могут представлять собой данные, не принадлежащие владельцу системы, и вследствие этого у них есть особая и значимая характеристика, заключающаяся в необходимости соблюдения требований по обеспечению защиты таких сведений, предусмотренных действующим законодательством.

Применительно к системе, как правило, имеется возможность идентифицировать наименования и характеристики существующих баз данных или других информационных активов, подлежащих защите.

В самом простом случае все данные можно рассматривать как равноценные, с одинаковым риском проведения атаки, представленные единым информационным активом, называемым, например, «пользовательские данные».

Однако часто необходимо различать системные данные, то есть данные, используемые функциональными возможностями безопасности ОО (ФБО), от других данных. В случае модификации или удаления системных данных ФБО могут функционировать неправильно и тем самым допускать проведение определенных типов атак, тогда как в случае модификации других данных будут скомпрометированы только эти данные, а ФБО продолжат функционировать и обеспечивать защиту других активов. Распространен случай, когда достаточно выделить следующие два типа информационных активов: данные ФБО и все остальные данные, защищаемые с использованием продукта ИТ.

В некоторых случаях разные типы данных ФБО могут быть уязвимы в отношении разных атак или их компрометация может приводить к разным последствиям, поэтому их требуется рассматривать раздельно. Примерами разных типов данных ФБО могут быть:

- данные конфигурации ФБО;
- база аутентификационных данных;
- записи аудита.

Активы процессов представляют собой приложения (прикладные ПО), в которых осуществляется преобразование или анализ данных. Отличие от информационных активов состоит в том, что связанные

с этими активами данные не представляют большой ценности без имеющихся у приложений возможностей по обработке. Примерами возможных типов активов процессов являются:

- финансовые;
- коммуникационные;
- логистические;
- производственные;
- процессы автоматизации офисной работы.

К финансовым приложениям могут относиться начисление заработной платы, управление инвестициями и расходами. Коммуникационные системы могут включать электронную почту или обработку информации внутри сети или полученной из сети Интернет. Логистические системы могут включать обработку заказов, контроль складов или планирование ресурсов. Производственные приложения могут включать управление процессами производства в режиме реального времени. Автоматизация офисной работы может охватывать обработку структурированного текста.

Применительно к системе, как правило, есть возможность идентифицировать наименования и характеристики процессов, подлежащих защите.

В общем случае активы процессов восприимчивы только к атакам модификации или отказа в обслуживании. Например, могут быть изменены функциональные возможности соответствующего прикладного программного обеспечения с целью удаления проверок авторизации или для изменения обработки финансовых данных. Одного актива, называемого, например, «прикладным программным обеспечением», обычно достаточно для охвата всех процессов.

Физические активы представляют собой реальное оборудование для обработки информации, используемое для поддержки информационных активов и активов процессов. Примерами возможных типов физических активов являются:

- важные элементы сетевой инфраструктуры;
- портативные персональные компьютеры;
- центры обработки данных.

Крайне редко сам ОО предоставляет защиту физических активов как часть решения проблемы безопасности — физическая защита либо исключается из рассмотрения, либо обеспечивается средой функционирования и регулируется посредством предположений. Вследствие этого физические активы не так часто упоминаются в ПЗ или ЗБ. Однако существуют применимые меры, например автоматическое прекращение работы в случае сбоя электропитания, которые могут обеспечить защиту физических активов. В таких случаях физические активы могут быть приведены в ПЗ или ЗБ.

Важно не идентифицировать слишком много активов или типов активов. Если для двух активов или двух типов активов существуют одинаковые возможности подвергнуться атаке и одинаковые последствия реализации атаки, то их следует сгруппировать в один составной тип актива. Многие ОО защищают только два типа активов, данные ФБО и пользовательские данные. Больше чем шесть типов рассматривать не рекомендуется для любого ОО, за исключением тех, которые, как ожидается, предоставляют комплексные или специфические возможности защиты.

В рамках определения проблемы безопасности определенные активы или типы активов могли быть исключены из числа подлежащих защите. В этом случае они должны быть перечислены отдельно: эта информация потребуется в дальнейшем для пояснения того, почему данные активы были исключены из анализа угроз.

9.3.3.4 Негативные действия

В ГОСТ Р ИСО/МЭК 15408 отсутствует руководство по поводу того, каким образом следует описывать негативные действия. Что касается источников угроз, лучше всего, чтобы перечень описаний негативных действий был по возможности как можно более простым. Пример простого, но при этом достаточного по области охвата перечня:

- несанкционированный доступ;
- несанкционированная передача прав доступа;
- отказ в доступе субъекту, имеющему право доступа;
- отсутствие подотчетности.

Этот простой перечень включает в себя почти все угрозы, которые могут быть выявлены на практике. Следует учесть, что иногда некоторые негативные действия могут иметь различные последствия, это следует изложить отдельно для достижения полноты и ясности изложения. Могут существовать также другие, особые типы негативных действий, которые не подпадают ни под одну из указанных выше категорий. Наличие таких негативных действий должно быть очевидным при рассмотрении

неформализованных требований безопасности. Такие негативные действия также должны быть изложены отдельно.

Альтернативный подход заключается в описании негативных действий в терминах последствий от успешной атаки, например, утраты конфиденциальности. Такой подход часто использовался ранее. Однако он может быть излишне специфическим и ограниченным по области применения. В настоящее время он используется реже.

9.3.4 Применение выбранного методического подхода к проведению анализа угроз

Следующий шаг (после выбора методического подхода и подготовки необходимой для его применения информации) состоит в том, чтобы сформировать список применимых угроз.

На практике многие возможные угрозы могут быть достаточно просто исключены из рассмотрения. Существуют два конкретных метода, которые весьма полезны — идентификация исключаемых из рассмотрения или принимаемых как допустимые угроз и идентификация уже охваченных политикой угроз.

Многие типы угроз будут исключены из рассмотрения уже в ходе определения неформализованного требования безопасности либо потому, что они были исключены из области применения продукта ИТ, либо вследствие принятия решения о том, что они принимаются как допустимые, так как последствия от реализации связанных с ними рисков являются незначительными, либо потому, что связанный с ними риск передан на рассмотрение третьей стороне (например, страховой организации).

Исключение угроз распространено в контексте использования готовых коммерческих продуктов: например, поставщик операционной системы может решить не включать антивирусную защиту в продукт, предполагая, что покупатель пожелает приобрести дополнительное специализированное антивирусное программное обеспечение или будет использовать продукт в среде функционирования, изолированной и защищенной от возможности заражения.

Принятие угроз как допустимых обычно реализуется в контексте системы, так как это требует оценки ценности и значимости активов, которую разработчик (производитель) готового к использованию продукта выполнить не может.

Информация относительно не принимаемых в расчет угроз обычно становится очевидной, исходя из перечня того, что продукт не должен делать. В противном случае ее необходимо подтвердить и затем добавить в этот перечень. Также следует зафиксировать эту информацию в форме предположения (см. 9.5).

Для многих продуктов ИТ независимо от анализа фактических угроз уже будет принято решение о включении в продукт ИТ функциональных возможностей безопасности. Этот вариант типичен для случая готовых к использованию продуктов: например, поставщик операционной системы обычно включает функции идентификации и аутентификации пользователей, даже если продукт предназначен для использования в однопользовательском режиме.

Если эта обязательная функциональная возможность безопасности будет противостоять конкретному типу угроз, то нет необходимости в дальнейшем изучении этой угрозы на предмет того, является ли она применимой; защита будет обеспечиваться в любом случае.

Информация, используемая для отказа от учета конкретных угроз, обычно становится очевидной, исходя из перечня характеристик, которыми должен обладать продукт ИТ. В противном случае ее необходимо подтвердить и затем добавить в этот перечень. Также следует зафиксировать эту информацию в форме изложения политики безопасности (см. 9.4).

Все остальные угрозы должны быть идентифицированы и рассмотрены, а затем должен быть составлен полный список применимых угроз, с описанием каждой угрозы в терминах источников угроз, активов и негативного действия.

Некоторые угрозы могут быть применимы для некоторой конкретной системы, но в ходе определения области проблемы безопасности было уже решено, что им будут противостоять меры обеспечения безопасности в среде функционирования. Некоторым угрозам можно противостоять только средствами среды функционирования (например, когда необходима физическая защита). Эти угрозы также должны быть перечислены, но необходимо указать, что они формулируют цели безопасности для среды; такая информация будет весьма полезна в дальнейшем.

Однако не следует заранее судить о том, каким образом следует противостоять угрозам, будет ли это осуществляться ОО или средой его функционирования. Это бы ограничило возможности проектирования при выборе мер обеспечения безопасности.

В предыдущих редакциях ГОСТ Р ИСО/МЭК 15408 в анализ угроз были включены угрозы, связанные с разработкой продукта ИТ (то есть угрозы для среды разработки). Однако в действующей редакции ГОСТ Р ИСО/МЭК 15408 этого не требуется.

9.3.5 Практические рекомендации

Угрозы указывают на возможные способы совершить атаку на продукт ИТ. Поэтому их следует формулировать соответствующим образом. Целесообразнее использовать глагол «может». Например:

«Неуполномоченное лицо может попытаться получить доступ и использовать ресурсы ОО».

Начинать описание каждой угрозы удобнее всего с идентификатора, чтобы можно было сослаться на него. Описание должно быть четким и кратким.

Ниже приведен пример описания угрозы безопасности на базе профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации.

«Угроза-1

1. Аннотация угрозы — подключение к информационной системе внутренними и (или) внешними нарушителями незарегистрированных (неучтенных) съемных машинных носителей информации с последующей несанкционированной записью (передачей) на эти носители защищаемой информации из информационной системы.

2. Источники угрозы — внутренний нарушитель (пользователь информационной системы), внешний нарушитель (лицо, не являющееся пользователем информационной системы).

3. Способ реализации угрозы — подключение к средству вычислительной техники съемных машинных носителей информации, незарегистрированных в информационной системе и (или) не предназначенных для использования на конкретном интерфейсе ввода (вывода) средства вычислительной техники, и (или) не отнесенных к разрешенному типу, и (или) не отнесенных к разрешенным; несанкционированная запись защищаемой информации на подключенный съемный машинный носитель информации.

4. Используемые уязвимости — отсутствие или недостаточность мер контроля за использованием съемных машинных носителей информации в информационной системе.

5. Вид информационных ресурсов, потенциально подверженных угрозе — защищаемая информация, обрабатываемая в информационной системе; другие информационные ресурсы информационной системы.

6. Нарушаемые свойства безопасности информационных ресурсов — конфиденциальность.

7. Возможные последствия реализации угрозы — несанкционированное ознакомление с защищаемой информацией, обрабатываемой в информационной системе; нарушение режимов функционирования информационной системы».

При применении описанного в настоящем стандарте методического подхода к анализу угроз допускается его при необходимости адаптировать и интерпретировать под потребности описания конкретной проблемы безопасности. Если конкретный вариант категорирования угроз на практике неэффективен, можно выполнить анализ заново, используя другой подход.

Угрозы можно комбинировать, если у них имеются схожие аспекты: источники угроз, активы и негативные действия. В дальнейшем это позволит сократить перечень угроз и временные затраты, так как для противодействия таким угрозам будут использоваться одни и те же меры обеспечения безопасности. Аналогично, если для какой-либо угрозы возможны существенно отличающиеся последствия ее реализации в зависимости от источника угрозы или затрагиваемых активов, то разбиение рассматриваемой угрозы на несколько более конкретно сформулированных угроз позволит добиться большей ясности изложения и сократить временные затраты в дальнейшем.

Информация, указывающая на то, что угрозу можно не принимать во внимание, часто выражается неявным образом. Например:

«Предполагается, что администраторы не относятся к злонамеренным пользователям, они являются доверенными и компетентными пользователями».

Подобная информация выражена в терминах источника угрозы и по существу позволяет не принимать во внимание большинство типов угроз, которые обычно связываются с этим источником угрозы. Некоторые из таких типов угроз специфичны для администраторов и, следовательно, могут быть полностью исключены из рассмотрения. Другие типы угроз все же будут применимы, но могут ограничиваться только другими применимыми источниками угроз, например, обычными пользователями. Не следует забывать о дополнении списка предположений предположением, которое сократит область таких угроз.

В некоторых случаях можно только установить то, что связанный с источниками угроз или негативными действиями риск является неприемлемым, при этом может оказаться невозможным определить сами источники угрозы или негативные действия. Примером такой ситуации является нарушение реализации базовой абстрактной машиной связанной с ней модели безопасности. В этих случаях нет необходимости определять характеристики, основанные на предположениях. Данная угроза является неприемлемой по определению проблемы безопасности, и ее следует идентифицировать и обосновывать как таковую.

После формирования окончательного перечня угроз его следует проверить на полноту и непротиворечивость. Если угроза была выделена, исходя из типов активов или типов источников угрозы, то целесообразно проверить, были ли охвачены все возможные варианты. Хотя противоречия и упущения обычно обнаруживаются на последующих стадиях разработки ПЗ или ЗБ, проведение проверки на данном этапе позволяет сэкономить затраты времени и избежать необходимости пересмотра и внесения существенных изменений.

Возможно, по результатам анализа угроз не будут идентифицированы угрозы, которые следовало бы перечислить в качестве применимых для ОО. Такая ситуация может возникнуть, например, в случае с ПЗ, которые разрабатываются исключительно для удовлетворения требований общей корпоративной или государственной политики в области защиты информации. Это является допустимым в контексте ГОСТ Р ИСО/МЭК 15408; в подобном случае раздел «Угрозы» следует оставить незаполненным с указанием, что угрозы не были идентифицированы.

9.4 Идентификация и спецификация политик

В определение проблемы безопасности кроме угроз включается также перечень применимых политик безопасности организации (ПБОр), которым должен соответствовать ОО. По сравнению с угрозами политики, как правило, гораздо легче идентифицировать и описать. При использовании рекомендуемого в настоящем стандарте методического подхода необходимо иметь перечень свойств или характеристик безопасности, которыми должен обладать продукт ИТ. Каждый элемент этого перечня может быть переформулирован как ПБОр.

Независимо от рассмотрения угроз или других обстоятельств политики представляют собой формулировки того, что должен выполнять продукт ИТ. При их формулировании часто используется глагол «должен». Например:

«Администраторы должны пройти аутентификацию до предоставления им доступа к каким-либо функциям или данным ОО».

Как и для описаний угроз, целесообразнее начать описание каждой политики с идентификатора, чтобы облегчить возможность ссылки на конкретную политику. Описание правил политики должно быть четким и кратким.

Ниже также приведены примеры изложения политик на базе профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации:

«Политика безопасности-1

Должно осуществляться разграничение доступа к управлению СКН на основе ролей уполномоченных лиц.

...

Политика безопасности-4

Должен обеспечиваться контроль использования интерфейсов ввода (вывода) в СВТ при подключении съемных машинных носителей информации.

Политика безопасности-5

Должен обеспечиваться контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации».

В ГОСТ Р ИСО/МЭК 15408 политики обычно называются политиками безопасности организации, или сокращенно ПБОр. Это может ввести в заблуждение, ведь некоторые ПБОр могут относиться только к одной системе, которая охватывается ПЗ или ЗБ, а не ко всем системам организации-владельца (оператора). В настоящем стандарте используется более простой термин «политики».

Большинство применяемых политик следует идентифицировать во время определения неформализованного требования безопасности или при проведении анализа угроз. Однако следует провести и окончательную проверку, чтобы идентифицировать любые другие политики, имеющие отношение к безопасности.

Политики используются для спецификации:

- обязательных функциональных возможностей безопасности, которые следует включить в состав ОО;
- обязательных технологий, методов и средств, которые следует использовать для реализации конкретных функциональных возможностей безопасности (что неявно потребует наличия соответствующих функциональных возможностей).

Политики могут также использоваться вместо соответствующих угроз. Это может оказаться целесообразным, если:

- уверенность в существовании конкретной угрозы отсутствует, но, несмотря на это, было принято «политическое» решение обеспечить соответствующую защиту;
- было принято «политическое» решение относительно того, как противостоять конкретной угрозе, например, специфицировав то, какие меры обеспечения безопасности должны предотвращать успешную реализацию атаки или что следует предпринять, если атака произойдет;
- было принято «политическое» решение о выборе конкретного подхода для противодействия ряду соответствующих угроз.

Однако нет практической ценности в замене угрозы на политику, если в политике отсутствует какая-либо информация, которой нет в явном виде в формулировке угрозы.

Политики, определенные в ходе заключительной проверки, могут потребовать внесения изменений или доработки разработанного ранее определения проблемы безопасности, например, может потребоваться исключить угрозы, которые теперь уже охвачены политиками.

На практике большую часть политик легко идентифицировать и четко сформулировать. Однако следует отметить наличие некоторых общих проблем.

Изложения политик иногда неправильно используются для выражения требований относительно тех функциональных возможностей безопасности, которые ОО не должен или не может выполнять и которые вместо этого должны реализовываться средой функционирования ОО. Если требование не может быть реализовано ОО, то правильно определить его как предположение относительно среды функционирования (см. 9.5). Если рассматриваемая политика не может быть осуществлена ОО, средой функционирования или ОО и средой его функционирования совместно, то изложение политики является либо не имеющим смысла, либо нереализуемым.

Во время определения проблемы безопасности и ее решения может возникнуть потребность в изменении границ ОО для передачи функций, возлагавшихся на ОО, его среде функционирования или наоборот. Это может привести к тому, что политики станут предположениями или предположения станут политиками либо потребуется повторная спецификация политик и предположений с учетом новых границ ОО. Аналогично для составных ОО, которые разбиваются на несколько компонентов, решающих различные проблемы безопасности, предположение для одного компонента часто реализуется другим компонентом как требование политики. В таких случаях тщательное формулирование при изложении правил политик позволит повторно использовать эти формулировки в других определения проблемы безопасности в качестве предположений, обеспечив совместимость и простоту проверки непротиворечивости.

Иногда во время разработки определения проблемы безопасности неясно, будет ли политика реализована ОО или средой его функционирования. И это допустимо; уточнить этот вопрос можно будет в процессе определения целей безопасности, когда требования к функциональным возможностям безопасности станут понятнее. Цели безопасности и для ОО, и для среды функционирования могут быть прослежены к политикам. Политика может даже частично реализовываться ОО, а частично — средой его функционирования.

Не для всех определений проблем безопасности требуется наличие политик. Это вполне допустимо и не противоречит ГОСТ Р ИСО/МЭК 15408. В таких случаях раздел «Политика безопасности организации» следует оставить незаполненным с указанием, что политики не были идентифицированы.

9.5 Идентификация и спецификация предположений

Кроме угроз и политик в определение проблемы безопасности включается перечень применимых предположений, которые ограничивают или исключают характеристики безопасности, требующиеся от ОО. При использовании рекомендуемого в настоящем стандарте методического подхода необходимо иметь перечень свойств безопасности или характеристик, которые не требуются от продукта ИТ. Каждый элемент такого перечня может быть переформулирован как предположение относительно среды функционирования либо предполагаемого использования ОО.

Независимо от результатов рассмотрения угроз или других обстоятельств предположения представляют собой изложение того, что не требуется от продукта ИТ. Следовательно, они должны быть сформулированы как констатация фактов. Пример ясно и четко сформулированного предположения:

«ОО будет размещен в месте, для которого обеспечивается физическая защита».

Предположения могут быть использованы двумя способами:

- для указания на то, что конкретная мера обеспечения информационной безопасности или тип мер будет предоставлена (представлен) средой функционирования, а не ОО;

- для указания на то, что конкретные угрозы или типы угроз можно не принимать во внимание, так как в контексте предполагаемой среды функционирования их либо не существует, либо они не являются важными.

В первом случае целесообразнее использовать глаголы в будущем времени: это позволит указать, что мера обеспечения безопасности должна предоставляться, пусть и не самим ОО. Во втором случае целесообразнее использовать глаголы в настоящем времени.

Следует отдельно рассматривать предположения о мерах обеспечения безопасности, предоставляемых средой, от предположений об угрозах, не принимающихся во внимание, так как первые требуются согласно ГОСТ Р ИСО/МЭК 15408, а вторые служат в качестве дополнительной информации и рекомендуются настоящим стандартом для упрощения демонстрации того, что цели безопасности охватывают все применимые угрозы. Этот вопрос подробно объясняется далее (см. 10.2).

Каждому предположению следует присвоить идентификатор для обеспечения возможности ссылки на него. Описание предположения должно быть четким и кратким.

В ГОСТ Р ИСО/МЭК 15408 установлено, что предположения «могут быть по отношению к физическим аспектам, персоналу и аспектам связности среды функционирования» (ГОСТ Р ИСО/МЭК 15408-1, пункт А.6.4).

Ниже также приведены примеры предположений на базе профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации:

«Предположения, связанные с физическими аспектами среды функционирования

Предположение-1

Обеспечивается невозможность осуществления действий, направленных на нарушение физической целостности СВТ, доступ к которым контролируется с применением СКН.

Предположения по отношению к аспектам связности среды функционирования

Предположение-2

Обеспечивается надежный источник меток времени для записи событий аудита безопасности СКН.

Предположение-3

Обеспечиваются условия совместимости ОО с СВТ для реализации своих функциональных возможностей.

Предположения, связанные с персоналом среды функционирования

Предположение-4

Персонал, ответственный за функционирование ОО, обеспечивает функционирование ОО в соответствии с эксплуатационной документацией».

Практический опыт показал, что часто возникает необходимость и в других предположениях, например, о технических функциональных возможностях обеспечения безопасности вне ОО:

«В среде функционирования ОО будут отсутствовать какие-либо инструментальные средства, позволяющие обычным пользователям добавлять новые функциональные возможности системы».

Во многих случаях реализация политик и противостояние угрозам частично осуществляются ОО, а частично — его средой функционирования. Например, для эффективной реализации технических мер обеспечения безопасности в ОО может потребоваться реализовать вспомогательные организационные или физические меры обеспечения безопасности. Потребность в таких вспомогательных мерах в среде функционирования следует идентифицировать и изложить в форме предположений.

В ходе оценки не выполняется тестирование предположений; считается, что они всегда правомочны и истины. Однако предположения полезны для демонстрации непротиворечивости и полноты. Если угрозы были определены с помощью ранее рассмотренного методического подхода, для демонстрации полноты охвата в обосновании могут потребоваться предположения. Угроза может частично не приниматься во внимание, а частично ей может оказываться противодействие. В данном случае потребуется соответствующее предположение для демонстрации полноты охвата при прослеживании целей безопасности к угрозе, которой оказывается частичное противодействие средствами ОО.

Многие предположения идентифицируются при спецификации неформализованного требования безопасности или в процессе анализа угроз. Однако для идентификации любых других значимых предположений следует провести всеохватывающий анализ в рамках выполнения рассматриваемого этапа

определения проблемы безопасности. В случае принятия решения о применении какой-либо политики или необходимости противостояния какой-либо угрозе средствами среды функционирования это решение всегда следует документировать в форме предположения.

Предположения следует формулировать таким образом, чтобы отражать рассматриваемые политики и угрозы, так как на их основе будут разработаны цели для среды функционирования, которые должны будут соответствовать этим политикам и угрозам.

Одно предположение часто может использоваться для противостояния нескольким угрозам, так или иначе связанным между собой. Если используется подход, основанный на дереве угроз, когда совокупность различных детально описанных угроз, которым должна противостоять среда функционирования, соответствует общему иерархическому узлу верхнего уровня, то предположение может быть выражено на уровне общего узла. Например, если все угрозы, являющиеся результатом противоправных действий администраторов, не принимаются во внимание, то это можно выразить одним предположением:

«Администраторы имеют необходимые навыки, квалификацию, время и ресурсы для выполнения всех назначенных им административных функций и правильно выполняют все эти функции».

При формулировке предположений можно проверить предположение на полноту и точность, а также на целесообразность использования данного предположения следующим образом: если данное предположение не выполняется, то в отношении ОО может быть успешно реализована атака.

Для идентификации и спецификации целей безопасности целесообразно разделять предположения по типам. В первую очередь следует разделить друг от друга предположения, связанные с физическими и организационными аспектами безопасности. Следующая категория должна включать в себя предположения, связанные с функциональными возможностями безопасности, предоставляемыми средой функционирования ИТ. Также следует выделить предположения об угрозах, не принимающихся во внимание. Такие предположения должны быть выделены в отдельную категорию, так как они не порождают целей безопасности.

Не для всех проблем безопасности требуется наличие предположений. Это вполне допустимо и не противоречит ГОСТ Р ИСО/МЭК 15408. В таких случаях подраздел «Предположения безопасности» следует оставить незаполненным, указав, что предположения не были идентифицированы.

9.6 Оформление раздела «Определение проблемы безопасности»

Заключительный этап формирования раздела «Определения проблемы безопасности» состоит в его окончательном оформлении и включает в себя решение следующих двух задач:

- подготовка полного перечня всех угроз, политик и предположений;
- выполнение проверок на непротиворечивость и полноту для подтверждения того, что определение проблемы безопасности достаточно точно представляет проблему или проблемы безопасности, которые присутствуют в неформализованном требовании безопасности.

В ГОСТ Р ИСО/МЭК 15408 отсутствуют какие-либо требования относительно предоставления обоснования определения проблемы безопасности; изложение угроз, политик и предположений, выраженных в определении проблемы безопасности, в целях оценки рассматривается как не требующее доказательств. Однако настоятельно рекомендуется, чтобы было приведено обоснование, в котором каждый элемент определения проблемы безопасности прослеживается к неформализованным требованиям безопасности и в котором демонстрируется, что покрытие является полным, без дублирования и избыточности. Если требования изменятся или возникнут какие-то сложности с восприятием, то такое обоснование упростит переработку определения проблемы безопасности и уменьшит риск внесения ошибок.

Также в ГОСТ Р ИСО/МЭК 15408 отсутствуют какие-либо требования относительно идентификации угроз, которые были исключены из состава актуальных. Эта информация очень полезна при изменении обстоятельств и необходимости переработки определения проблемы безопасности. Настоящим стандартом рекомендуется всегда включать соответствующие предположения относительно таких угроз. Однако их следует приводить в отдельном особо выделенном подразделе определения проблемы безопасности, отдельно от всех других предположений о среде функционирования. Данная информация будет служить для экспертов, оценивающих «Определение проблемы безопасности», индикатором того, что эти угрозы не должны учитываться при прослеживании к целям безопасности.

Проверка раздела на полноту и непротиворечивость включает также и проверку того, что все ограничения и требования, выявленные в ходе определения области проблемы безопасности, были отражены в политиках или предположениях и что для всех идентифицированных угроз либо определено

противостояние, либо эти угрозы исключены из рассмотрения. Аналогичным образом, все политики, угрозы и предположения, перечисленные в определении проблемы безопасности, должны прослеживаться к аспектам исходного неформализованного требования безопасности. Часто эффективным и простым способом демонстрации непротиворечивости и полноты является создание перекрестных таблиц.

Предположения и политики могут иногда конфликтовать (вступать в противоречие), например, требование политики «должен выполнять *X*» может вступать в противоречие с предположением «*X* выполнять не обязан». В ходе анализа обычно обнаруживается, что в действительности противоречие отсутствует: ожидается, что ОО решает лишь часть идентифицированной проблемы, а не всю проблему в целом. Необходимо дополнительное разъяснение и уточнение формулировок требования, что позволит разрешить возникшее противоречие. В случае наличия противоречия на самом деле его следует решать посредством повторного исследования неформализованного требования безопасности для установления того, что в действительности требовалось.

10 Спецификация раздела «Цели безопасности»

10.1 Введение

Данный раздел содержит рекомендации по идентификации и определению целей безопасности в ПЗ или ЗБ, требования к которым приведены в ГОСТ Р ИСО/МЭК 15408-1, подразделы А.7 и В.7 соответственно. Как и в случае с определением проблемы безопасности, подраздел В.7 состоит только из ссылки на подраздел А.7, что в явном виде указывает на то, что содержание этих разделов идентично. Как и в случае с определением проблемы безопасности, приведенные в ГОСТ Р ИСО/МЭК 15408-3 требования подтверждения правильности спецификации целей безопасности в обоих случаях идентичны.

Цели безопасности представляют собой краткое изложение предполагаемой реакции на проблему безопасности (см. ГОСТ Р ИСО/МЭК 15408-3, пункты 9.4.1 и 10.4.1). При этом не следует неправильно интерпретировать это утверждение, так как в действительности описание реакции является спецификацией функциональных требований безопасности (см. раздел 11). Лучше, когда цели безопасности выражают в виде аннотации и описания структуры требуемых функциональных возможностей безопасности, что обеспечивает связь между детализацией ФТБ и абстрактным определением проблемы безопасности. Иными словами, указав в определении проблемы безопасности, в чем состоят проблемы безопасности, следует указать и каким образом они будут решаться объектом оценки и его средой функционирования.

Согласно ГОСТ Р ИСО/МЭК 15408 требуются два различных типа целей безопасности, которые подлежат спецификации:

а) цели безопасности для ОО, которые должны достигаться путем применения технических (ИТ) мер защиты информации, реализуемых ОО;

б) цели безопасности для среды, которые должны достигаться путем применения технических мер, реализуемых ИТ-средой, или не-ИТ-мер (например, организационных, процедурных мер).

Указанные типы целей безопасности приведены на рисунке 2.

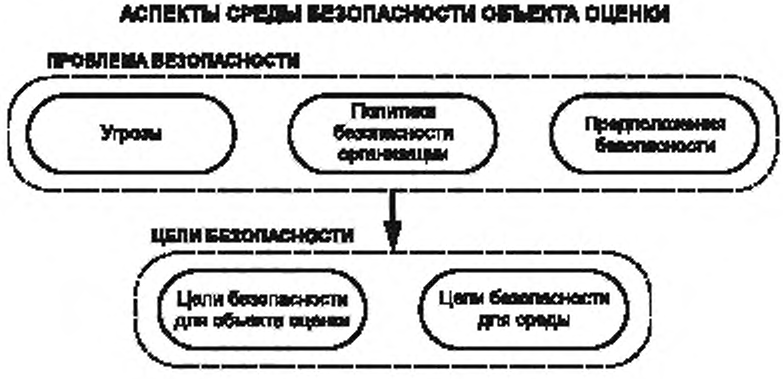

Рисунок 2 — Роль целей безопасности

Во всех ПЗ и ЗБ необходимо специфицировать цели безопасности для среды функционирования ОО. В ПЗ и ЗБ для низких уровней доверия (см. раздел 15) не требуется специфицировать цели безопасности для ОО, а цели безопасности для среды функционирования ОО принимаются как не требующие доказательства, то есть не требуется их прослеживание к определению проблемы безопасности.

В дальнейшем в данном разделе предполагается, что требуются оба типа целей безопасности, и они прослеживаются к определению проблемы безопасности.

Цели безопасности должны быть сформулированы в виде требований. Они должны представлять собой краткие и четкие формулировки, в совокупности определяющие решение верхнего уровня для проблемы безопасности, идентифицированной в соответствующем определении проблемы безопасности. При формулировании целей целесообразно использовать глагол «должен».

ГОСТ Р ИСО/МЭК 15408 не предполагает и не предписывает использование какого-либо конкретного процесса или методического подхода для разработки целей безопасности; можно выбрать любой подходящий метод. Это представляет определенные трудности для лиц, не обладающих опытом разработки ПЗ и ЗБ. Поэтому в данном разделе содержится подробное описание простого методического подхода, который был опробован и испытан на практике, и эффективность которого была подтверждена применением в различных организациях и средах функционирования. Он основан на выполнении последовательности следующих шагов:

а) структурирование перечня всех угроз, политик и предположений, которые должны охватываться целями безопасности;

б) идентификация целей безопасности для не-ИТ-среды функционирования;

в) идентификация целей безопасности для ИТ-среды функционирования;

г) идентификация целей безопасности для ОО;

д) разработка обоснования целей безопасности посредством обратного сопоставления целей безопасности и идентифицированных угроз, политик и предположений.

Каждый из этих шагов описан в последующих подразделах. В большинстве случаев эти шаги целесообразно выполнять в указанной выше последовательности.

Это всего лишь один из возможных подходов к идентификации целей безопасности. В некоторых конкретных случаях предложенный методический подход может быть не самым простым в реализации или требующим существенных затрат времени. Существуют и другие применимые подходы.

Учитывая центральную роль, которую играют цели безопасности в ПЗ и ЗБ, большое значение имеет вопрос о наиболее приемлемом уровне детализации при их (целей безопасности) изложении. Требование краткого изложения целей безопасности предполагает достижение равновесия между двумя следующими аспектами:

а) с одной стороны, цели безопасности должны помочь пользователю ПЗ или ЗБ без углубленного изучения деталей реализации (за исключением случаев, когда такая детализация предписана в определенной проблеме безопасности) понять, как аспекты проблемы безопасности, идентифицированные в определенной проблеме безопасности, решаются объектом оценки. В идеале цели безопасности для ОО должны быть независимы от реализации. Таким образом, основное внимание необходимо сосредоточить на том, *какое* решение предпочтительнее, а не на том, каким образом это решение достигается;

б) в то же время необходимо, чтобы формулировка целей безопасности не являлась простым повторением, хотя и в несколько другой форме, информации, содержащейся в описании угроз и ПБОр.

Одним из критериев правильности выбора уровня детализации формулировки целей безопасности, применяемым на этапах обоснования целей безопасности и требований безопасности, является следующий. Если обоснование одной цели безопасности (или требования) является слишком тривиальным, а другое обоснование — слишком объемным, сложным и трудным для понимания, то существует вероятность того, что формулировка целей безопасности является либо слишком детализированной, либо слишком абстрактной.

Сформированный соответствующим образом набор целей безопасности для ОО будет способствовать тому, что выбранные для удовлетворения целей функциональные требования безопасности не будут избыточными. Это, в свою очередь, позволит минимизировать стоимость и затраты времени на оценку (сертификационные испытания) ОО.

10.2 Структурирование угроз, политик и предположений

Первоочередной задачей является структурирование полного перечня всех применимых угроз, политик и предположений из определения проблемы безопасности.

Следует учитывать, что некоторые угрозы могут иметь отношение к ОО, но в результате анализа рисков или изучения среды функционирования может быть принято решение о том, что некоторые угрозы могут быть исключены из рассмотрения. При использовании рекомендуемого в настоящем стандарте методического подхода следует включить такие угрозы в определение проблемы безопасности, а также сформулировать предположения, в которых указывается, что они не являются применимыми. Такие угрозы не порождают целей безопасности, поэтому первый шаг состоит в том, чтобы идентифицировать их и связанные с ними предположения, а также исключить эти угрозы и предположения из дальнейшего рассмотрения. Следует убедиться в том, что из определения проблемы безопасности очевидно, что эти угрозы были исключены именно таким образом.

Остальные угрозы, политики и предположения следует затем разделить по следующим типам:

- относящиеся к не-ИТ-среде функционирования;
- относящиеся к ИТ-среде функционирования;
- относящиеся к функциональным возможностям ОО.

Обычно процесс такой классификации не представляет сложностей: политика, требующая применения средств физической защиты, может быть применима только к не-ИТ-среде функционирования; угроза, представляющая собой потенциально возможную атаку непосредственно на ОО, относится к функциональным возможностям ОО. Следует заметить, что предположения могут быть применимы только к элементам среды функционирования. В том случае, когда обнаруживается, что политика или угроза охватывают несколько вопросов, следует разделить их и поставить в соответствие каждому вопросу одну политику или угрозу.

Например, некоторую угрозу можно разделить на две части:

- часть угрозы, относящаяся к ИТ-среде функционирования;
- часть угрозы, относящаяся к функциональным возможностям ОО.

В случае сомнений следует разделить политику или соответствующую угрозу на несколько частей. Невостребованные элементы можно будет легко исключить в дальнейшем. При этом упущение каких-либо аспектов может привести к упущению целей безопасности, а эту проблему будет гораздо труднее обнаружить в ходе проверки правильности ПЗ или ЗБ.

10.3 Идентификация целей безопасности для не-ИТ-среды функционирования

Цели для среды функционирования определить легче, чем цели для ОО, а цели для не-ИТ-среды функционирования — легче, чем цели для ИТ-среды. Поэтому имеет смысл рассмотреть сначала цели для не-ИТ-среды функционирования.

Первым шагом в идентификации этих целей является рассмотрение всех предположений, определенных для не-ИТ-среды функционирования, и перефразирование их по принципу «один к одному» в соответствующие цели (далее в этом разделе приведено руководство по выполнению этого шага). Цели для среды не анализируются в дальнейшем в ПЗ и ЗБ или в процессе оценки, поэтому нет смысла в выявлении их совместимости, общности, перекрытии и т. д. в случае, если цели безопасности сформулированы ясно и четко.

Затем разрабатываются и добавляются любые другие цели, необходимые для учета аспектов угроз и политик, определенных для не-ИТ-среды функционирования, путем переформулирования этих угроз и политик в цели, но без детализации или пояснений. Определение соответствующих формулировок обычно также не представляет трудностей. В противном случае могут быть использованы методы категорирования, используемые для более сложной задачи — определение целей безопасности для ОО. Эти методы описаны в 10.5.

Иные цели безопасности для не-ИТ-среды могут включать:

а) цели, связанные с разработкой и реализацией процедур, обеспечивающих эксплуатацию ОО в безопасных режимах (в частности, соблюдаются все предположения о среде);

б) цели, связанные с обучением и подготовкой администраторов и пользователей по практическим вопросам обеспечения информационной безопасности.

На данной стадии эти цели может быть труднее идентифицировать, так как они поддерживают цели безопасности для ОО. Если они очевидны, то следует включить их на этой стадии. В ином случае на последующих стадиях предлагаемого методического подхода цели безопасности для среды могут быть пересмотрены и дополнены.

Целям для среды функционирования часто присваиваются идентификационные имена, помогающие отличать их от целей безопасности для ОО. В рассмотренных целях должно быть четко указано,

что они достигаются организационными (процедурными) или физическими мерами; при необходимости в описании цели следует явно указать на «не-ИТ-среду функционирования».

Цели для среды функционирования, полученные на основе предположений, целесообразнее формулировать аналогично предположениям, то есть как констатацию фактов. Например:

«При окончательном выводе из эксплуатации магнитные машинные носители информации размагничиваются или измельчаются».

Цели, полученные на основе угроз и политик, должны быть сформулированы в виде требований. Например:

«Ответственный за эксплуатацию персонал должен через регулярные интервалы времени просматривать записи аудита с целью обнаружения недопустимой и необычной деятельности».

Большинство целей для не-ИТ-среды функционирования формулируют на основе предположений.

Ниже приведены примеры изложения целей безопасности для ОО на базе профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации:

«Цель для среды функционирования ОО-1

Совместимость

Объект оценки должен быть совместим с СВТ (ИС), в котором (которой) он функционирует.

Цель для среды функционирования ОО-3

Физическая защита ОО

Должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, доступ к которым контролируется с применением СКН.

Цель для среды функционирования ОО-8

Требования к персоналу

Персонал, ответственный за функционирование объекта оценки, должен обеспечивать требуемое функционирование объекта оценки, руководствуясь эксплуатационной документацией».

Приведенные примеры целей безопасности для среды функционирования получены на основе примеров предположений, изложенных в 9.5.

Цели, полученные только на основе анализа угроз, могут свидетельствовать о том, что в определении проблемы безопасности пропущены соответствующие предположения. В этом случае следует проверить и при необходимости пересмотреть определение проблемы безопасности.

Для удобства могут быть определены отдельные цели, охватывающие несколько взаимосвязанных предположений, или предположение и связанные с ним угрозы, или политики и связанные с ними угрозы. Такие элементы полезно сочетать, если это позволит получить более понятный общий результат.

Ответственность за достижение целей для не-ИТ-среды функционирования возлагается на организацию, которая использует рассматриваемый продукт ИТ. На данной стадии определения целей очень важно убедиться в том, что сформулированные цели являются реалистичными и достижимыми. Лучше узнать об имеющихся проблемах на данной стадии, так как на данной стадии цели могут еще быть изменены или угрозы и политики могут быть учтены иными способами.

10.4 Идентификация целей безопасности для ИТ-среды функционирования

Методы, используемые для идентификации и определения целей для ИТ-среды функционирования, идентичны методам, описанным в 10.3 в отношении целей для не-ИТ-среды. Однако важно, чтобы цели для ИТ-среды излагались отдельно от целей для не-ИТ-среды, так как цели для ИТ-среды могут стать целями для ОО в случае последующего изменения границ ОО в процессе спецификации и проектирования ОО.

Поэтому в цели для ИТ-среды функционирования целесообразно включать текст «ИТ-среда функционирования» либо каким-то иным образом пояснять, что эти цели будут реализовываться программно-техническими средствами, находящимися за пределами границ ОО.

Ниже также приведены примеры изложения целей безопасности для ИТ-среды функционирования ОО на базе профиля защиты ФСТЭК России для средств контроля подключения съемных машинных носителей информации:

«Цель для среды функционирования ОО-4

Поддержка аудита

Должны быть обеспечены поддержка средств аудита, используемых в ОО (расширенные возможности по хранению и анализу информации аудита безопасности), и предоставление для них соответствующего источника меток времени.

Цель для среды функционирования ОО-5

Идентификация и аутентификация

Должна быть обеспечена возможность идентификации и аутентификации администратора СКН до предоставления ему возможности по управлению ОО, просмотру аудита безопасности и выполнения иных действий по администрированию ОО».

В предыдущих редакциях ГОСТ Р ИСО/МЭК 15408 допускалось специфицировать требования безопасности для удовлетворения целей для ИТ-среды, чтобы определить и объяснить, каким образом предполагается их достичь. В действующей редакции ГОСТ Р ИСО/МЭК 15408 это не допускается. Однако имеются и другие методы, например использование замечаний по применению, которые могут использоваться для указания ограничений по реализации целей.

В составном продукте цели для ИТ-среды одной части продукта становятся целями для ОО других частей. Такие цели следует формулировать очень тщательно для упрощения установления соответствия.

10.5 Идентификация целей безопасности для ОО

Цели безопасности для ОО являются наиболее важными и при этом их сложнее всего сформулировать достаточно полно и правильно. В отличие от целей для среды функционирования, они используются как обоснование функциональных требований безопасности. Поэтому важно, чтобы они были четко сформулированы с указанием их назначения и обеспечением хорошей прослеживаемости между детализированными требованиями безопасности и проблемой безопасности. При этом недостаточно только переформулировать проблему безопасности или перечислить конкретные требования безопасности.

Методический подход, предложенный в данном разделе, предполагает систематизацию цели для ОО на базе четких областей функциональных возможностей безопасности, выбранных для четкого сопоставления со структурой организации функциональных компонентов в семействах и классах в ГОСТ Р ИСО/МЭК 15408-2. Широта и глубина изложения целей в рамках каждой области функциональных возможностей связаны с использованием концепции основных и вспомогательных целей. Каждая основная цель устанавливает общую стратегию относительно рассмотрения аспекта безопасности («лучшую практику»). Вспомогательные цели детализируют конкретные специфичные вопросы, которые имеются в изложении любой проблемы безопасности.

При использовании этого методического подхода первый шаг определения целей для ОО состоит в переупорядочивании перечня применимых угроз, а также политик, назначенных для функциональных возможностей ОО с целью совместного группирования соответствующих угроз и политик. При этом не должно быть каких-либо предположений относительно функциональных возможностей ОО, так как предположения делаются только относительно среды функционирования. Если какие-либо предположения были сделаны для конкретной рубрики, их следует изучить и откорректировать.

Способ группирования для конкретных ПЗ и ЗБ зависит от вида (типа) рассматриваемого ОО. В любом случае для формирования функциональных требований безопасности будет полезно, чтобы проведенное группирование было связано с внутренней структурой ГОСТ Р ИСО/МЭК 15408-2.

Методический подход, предлагаемый в данном разделе, предполагает семь рубрик, под которыми группируются все угрозы и политики. Этот подход был опробован и протестирован на практике и оказался работоспособным для многих типов ОО.

Такими рубриками являются:

а) управление доступом (объекты, атрибуты, операции, правила доступа);

б) управление пользователями (типы пользователей, идентификация, аутентификация);

в) собственная защита ОО (обнаружение сбоев, доверенное восстановление и т. д.);

г) безопасное взаимодействие (установление соединений, свойства соединений, правила);

д) аудит (ведение журналов аудита, реагирование, управление инцидентами, анализ);

е) требования к архитектуре (требуемые свойства и ограничения);

ж) другие функции [сюда относится все, не попадающее очевидным образом под рубрики а)—е) — например, доверенный источник времени].

Существует тесная взаимосвязь между предложенными рубриками и предложенной в разделе 12 структурой для идентификации и спецификации функциональных требований безопасности.

Хотя у целей безопасности может быть любая структура и для их систематизации может использоваться любой метод, в общем случае предложенное выше группирование упростит процесс создания

перекрестных ссылок и формирования аргументов для последующего обоснования полноты и непротиворечивости. Могут существовать такие конкретные ОО, для которых в дальнейшем будет целесообразнее и проще использовать другой подход группирования. То есть важно обдумать структуру и выбрать подходящий подход.

Следующий шаг при определении целей для ОО состоит в том, чтобы привести простое определение типов сервисов безопасности или функций безопасности, требуемых для каждой из выбранных областей для удовлетворения всех потребностей, вытекающих из проблемы безопасности. Вместо того чтобы пытаться анализировать и обобщать определение проблемы безопасности, целесообразнее вернуться к неформализованному требованию безопасности, на основе которого было получено определение проблемы безопасности. Из неформализованного требования безопасности обычно очевидно, какие основные функции безопасности должны быть реализованы для каждой из областей. Некоторые области могут не упоминаться либо могут быть указаны как не значимые. На данном шаге эти области следует не рассматривать.

Полученный перечень сервисов (функций) затем следует сопоставить с систематизированным списком угроз и политик. Для каждого сервиса следует решить, к каким угрозам и политикам он относится. Все остальные угрозы и политики следует отнести к рубрике — «другие функции (сервисы)».

Затем следует разделить угрозы и политики, связанные с каждым сервисом, на общие и специфические требования. К общим следует относить требования, которые предъявляются ко всем аспектам определения сервиса, а специфические требования предъявляются к конкретным аспектам.

Далее следует переформулировать определение сервиса в утвердительное высказывание, в котором рассматривается общее требование. Оно станет основной целью для этого сервиса. Следует переформулировать все специфические требования в связанные, но отдельные вспомогательные цели для этого сервиса.

Ниже приведен пример изложения цели безопасности для ОО, направленной на противостояние угрозе, приведенной в качестве примера (Угроза-1) в 9.3.5:

«Цель безопасности-5

Контроль устройств

Объект оценки должен обеспечивать контроль типов подключаемых внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации».

На противостояние угрозам может быть направлена цель, которая предотвращает реализацию угрозы путем устранения или блокирования одного из ее необходимых компонентов: например, исключение возможности со стороны источника угрозы осуществить негативное воздействие; перемещение, изменение либо защита актива таким образом, что негативное воздействие становится неприменимым, устранение источника угрозы (например, путем определения цели для среды функционирования относительно мер контроля физического доступа). Угрозы могут также предотвращаться косвенным образом: например, реализация подотчетности через аудит, повышение уровня профессиональной подготовки с целью предотвращения ошибок пользователей, частое выполнение резервного копирования для упрощения восстановления утраченных либо поврежденных активов.

Таким образом, не от всех угроз можно обеспечить защиту. Иногда целесообразнее обнаружить связанный с угрозой инцидент и сгенерировать оповещение или запись в журнале аудита. Решение о такой обработке угроз необходимо принять на этапе проектирования. Если в качестве ответной реакции выбрано обнаружение, то это порождает потребность в сервисе аудита для реагирования на инциденты. Ниже приводится пример:

«Цель безопасности-6

Аудит безопасности СКН

Объект оценки должен обеспечивать соответствующие механизмы регистрации и предупреждения (сигнализации) о событиях, относящихся к возможным нарушениям безопасности. Механизмы регистрации должны предоставлять уполномоченным лицам с учетом их ролей возможность полного или выборочного ознакомления с информацией о произошедших событиях».

В ходе процесса спецификации целей безопасности для ОО может возникнуть потребность в переопределении угроз и политик. В результате более четкого определения сервисов конкретные угрозы или политики могут быть сопоставлены со вспомогательной, а не с основной целью или наоборот либо они будут больше подходить для рассмотрения в рамках другого сервиса. В ходе процесса спецификации целей безопасности для ОО часто идентифицируются соответствующие цели для среды функционирования, которые ранее были пропущены. Например, если в качестве реагирования на конкретные угрозы выбрано оповещение, то от администраторов потребуется реагировать на эти оповещения.

В некоторых случаях в результате принятых проектных решений конкретные угрозы или политики могут даже полностью перейти из рубрики целей для ОО под рубрику целей для среды функционирования или наоборот. Такие изменения возможны, поэтому необходимо проводить несколько итераций, пока не будет получен четкий список целей, покрывающий все рубрики.

Политики помимо выражения общих требований безопасности (сопоставляемых непосредственно с основной целью) иногда используются и для ограничения характеристик соответствующего технического решения. Такой тип ограничений должен быть выражен в виде вспомогательной цели, связанной с общим требованием.

Некоторые угрозы будут непосредственно сопоставимы с конкретной вспомогательной целью, которая направлена на противостояние только этой угрозе. В этом случае следует сформировать цель таким образом, чтобы она соответствовала первопричине. В дальнейшем это упростит прослеживание — в обосновании при сопоставлении целей с определением проблемы безопасности и для понимания ПЗ или ЗБ.

Вспомогательная цель может быть направлена на учет нескольких угроз и политик. Например, во многих ПЗ и ЗБ имеется цель, связанная с повторным использованием объекта, как вспомогательная цель для области управления ресурсами. Правильнее отделить ее от других аспектов управления ресурсами, так как у них обычно существует мало общего с точки зрения учитываемых угроз. Однако нет никакой необходимости в дальнейшем разбиении цели по различным типам ресурсов, хотя различные типы ресурсов могут обрабатываться разными способами, например, некоторые угрозы для оперативной памяти (RAM) не применимы к магнитным носителям. Различие становится ясным на стадии спецификации требований безопасности, когда в качестве механизмов для различных ресурсов будут выбираться различные ФТБ.

Еще одним важным различием в определении вспомогательных целей является тип требуемых мер обеспечения безопасности. Меры могут быть предупредительными (предотвращающими возникновение инцидента), обнаруживающими (распознающим факт возникновения инцидента) или корректирующим (устраняющим последствия инцидента). Если противостояние угрозам либо осуществление политик требует реализации более чем одного из этих типов реагирования, то целесообразно наличие различных вспомогательных целей для каждого такого типа. Подобная ситуация часто связана со случаем, когда описание проблемы безопасности требует глубокой защиты либо когда основная цель для сервиса будет состоять только в том, чтобы снизить или смягчить последствия реализации угрозы, а не блокировать ее.

Примером цели безопасности предупредительного характера может служить следующая цель, которая определяет необходимость идентификации и аутентификации пользователей ОО:

«Объект оценки должен уникально идентифицировать каждого пользователя и выполнять процедуру аутентификации идентифицированного пользователя до предоставления ему доступа к функциональным возможностям ОО».

Цели безопасности, связанные с управлением доступом и информационными потоками, также попадают в категорию целей предупредительного характера. Если ОО должен реализовывать более одной политики управления доступом и информационными потоками, то рекомендуется для каждой политики идентифицировать отдельные цели безопасности. Такой подход способствует упрощению процесса обоснования требований безопасности.

Примером цели обнаружения может служить цель, которая определяет необходимость обеспечения ОО невозможности отказа контрагентов от факта передачи или приема сообщения:

«Объект оценки должен включать средства, позволяющие получателю информации подготовить свидетельство, доказывающее происхождение этой информации».

Примером корректирующей цели (цели реагирования) может служить следующая цель, определяющая необходимость ответной реакции ОО на обнаруженные вторжения:

«При обнаружении событий, свидетельствующих о предстоящем нарушении безопасности, ОО должен принимать необходимые меры для противостояния данному нападению с минимальным снижением качества обслуживания пользователей ОО».

На данном этапе необходимо будет вернуться к формулировке целей безопасности для среды функционирования, чтобы проверить, не нужно ли добавить цели безопасности, связанные с действиями по управлению, чтобы обеспечить эффективность сервисов безопасности, предоставляемых ОО. В некоторых случаях требуемые действия по управлению очевидны и сразу могут быть выражены в виде (не-ИТ) цели безопасности. В других случаях требуемые действия по управлению могут зависеть от детализированных требований безопасности, используемых для реализации целей безопасности

для ОО. Например, связанная с «идентификацией и аутентификацией» пользователей цель безопасности могла бы быть реализована с помощью механизма паролей пользователей. Это будет предполагать наличие требования к пользователям не раскрывать своих паролей другим лицам. Такое требование может быть явно выражено как требование безопасности для не-ИТ-среды функционирования. На данной стадии, однако, допустимо, если неявное требование такого типа будет пропущено. Оно обнаружится при определении ФТБ, тогда можно будет уточнить изложение целей безопасности.

Там, где это возможно, при формулировании целей безопасности целесообразно неформально количественно определять ожидаемые минимальные значения эффективности, в основном снимая таким образом неопределенность относительно уровня эффективности, который должен быть обоснован в разделе ПЗ или ЗБ «Обоснование».

Количественная оценка может быть выражена:

а) в относительных величинах, например, по отношению к условиям среды функционирования или предыдущей ситуации;

б) в абсолютных числовых величинах.

Очевидно, что применение абсолютных числовых значений для количественной оценки является более предпочтительным, но в то же время и более трудным вариантом.

Не следует ожидать взаимно однозначного соответствия между целями и угрозами или политиками. Часто основная цель, требуемая для отработки политики, будет также противостоять и многим угрозам, связанным с этим сервисом. Кроме того, угрозы и политики, возможно, придется учитывать отдельно для разных типов активов и может возникнуть потребность в различных вспомогательных целях для каждого типа активов.

Существуют и другие методы, которые могут быть использованы для идентификации целей безопасности. Простой подход, который может быть эффективен при разработке коротких определений проблем безопасности, состоит в создании для каждой угрозы или политики одной цели, отражающей их изложение с указанием конкретных активов, источников угроз и т. д., если они неясны из изложения соответствующей угрозы или политики в определении проблемы безопасности.

Целям для ОО необходимо присваивать идентификационные наименования, отличающие их от целей для среды функционирования. Цели для ОО следует изложить ясно и четко и указать на то, что меры, реализующие цель, будут являться частью ОО и осуществляться ОО.

Изложение целей для ОО иногда начинается со слов «ФБО должны» или «система должна». ФБО являются той частью ОО, которая реализует ФТБ. Такое разграничение делается из практических соображений, чтобы уменьшить область ОО, подлежащую рассмотрению в ходе оценки. Поэтому использование термина «ФБО» является правильным; для любой цели та часть ОО, которая ее реализует, должна быть частью ФБО. Однако это в некоторой степени приводит к цикличности и сбивает с толку, так как такие цели обычно называются «целями безопасности для ОО», а не «целями безопасности для ФБО». Формулировка «система» также запутывает. Она может истолковываться так, что будет включать цели, реализуемые средой функционирования. Если так и предполагается, предпочтительнее использовать формулировку «ОО или его среда функционирования». Следует заметить, что в проектных решениях такие цели должны быть разделены на цели для ОО и на цели для среды функционирования ОО до окончательного утверждения целей.

10.6 Разработка обоснования целей безопасности

Заключительным шагом в определении целей безопасности является формирование обоснования, прослеживающего цели к угрозам, политикам и предположениям из определения проблемы безопасности, чтобы продемонстрировать, что все цели являются необходимыми, а также что цели охватывают все аспекты всех угроз, политик и предположений из определения проблемы безопасности. Это обоснование требуется согласно ГОСТ Р ИСО/МЭК 15408 во всех случаях (кроме ПЗ или ЗБ для низкого уровня доверия) и проверяется при оценке ПЗ или ЗБ.

Простой способ формирования обоснования состоит в подготовке таблиц взаимосвязи между элементами определения проблемы безопасности и целями безопасности и наоборот, а также в проверке на предмет наличия каких-либо противоречий, пропусков либо дублирования. В случае, когда угрозы, политики или предположения учитываются несколькими целями, обычно имеется простой способ разделения, который можно применить к элементу определения проблемы безопасности для демонстрации того, на какие части элемента направлены какие цели (см. пример из 10.2). Включение соответствующей информации в таблицу сделает прослеживание намного более четким и доступным для понимания.

Если предположить, что каждая цель безопасности может быть прослежена хотя бы к одной угрозе, политике или предположению, то в таблице следует продемонстрировать, что каждая цель безопасности является *необходимой*. Это не гарантирует отсутствия каких-либо избыточных целей безопасности, так как другие цели безопасности также могут быть прослежены к этим угрозам, политикам и предположениям, уже предоставляя должное покрытие. Однако это может быть обеспечено в рамках реализации второго требования проверки — достаточности.

Достаточность должна быть продемонстрирована путем предоставления неформализованных аргументов в дополнение к информации о перекрестных ссылках. Для каждой принимаемой во внимание угрозы необходимо пояснить, почему соответствующие цели безопасности совместно обеспечат эффективное противостояние данной угрозе. Следует отметить, что риск атак, проводимых как реализация угроз, не обязательно должен быть устранен полностью; может оказаться достаточным обеспечить обнаружение атаки, или восстановление системы после успешных атак, либо снижение вероятности атаки до приемлемого уровня. Таким образом, требуется эффективная контрмера (мера защиты информации) в контексте определения проблемы безопасности.

Аналогично для каждой идентифицированной ПБОр или предположения относительно среды функционирования необходимо посредством предоставления неформализованных аргументов обосновать, что соответствующие цели безопасности достаточны для обеспечения полного охвата ПБОр или для поддержки предположения.

Следует учитывать, что предположения, включенные в определение проблемы безопасности для идентификации угроз, которые можно считать несущественными или исключить из рассмотрения, не порождают целей безопасности и, следовательно, не должны появляться в обосновании целей.

Ниже в качестве примера приведен фрагмент обоснования целей на базе утвержденного ФСТЭК России профиля защиты.

«В таблице 1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 1 — Отображение целей безопасности для ОО на угрозы и политику безопасности организации

	Цель безопасности-1	Цель безопасности-2	Цель безопасности-3	Цель безопасности-4	Цель безопасности-5	Цель безопасности-6
Угроза-1					X	
Угроза-2	X	X				
Политика безопасности-1	X					
Политика безопасности-2		X				
Политика безопасности-3			X			
Политика безопасности-4				X		
Политика безопасности-5					X	
Политика безопасности-6						X

...

Цель безопасности-4

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности **Политика безопасности-4**, так как обеспечивает возможность контроля интерфейсов ввода (вывода) в СВТ.

Цель безопасности-5

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **Угроза-1** и реализацией политики безопасности **Политика безопасности-5**, так как обеспечивает возможность

контроля подключаемых типов внешних программно-аппаратных устройств, а также конкретных съемных машинных носителей информации.

...»

Если в ПЗ или ЗБ утверждается о соответствии другим ПЗ, то в обосновании необходимо продемонстрировать, что цели безопасности для ОО согласуются с изложениями целей безопасности в ПЗ, о соответствии которым утверждается. Если эти цели безопасности изложены схожим образом, то это можно продемонстрировать посредством прямого прослеживания, демонстрирующего, что цели в этих ПЗ не вступают в противоречие и охватывают все цели рассматриваемого ПЗ. В случае если ПЗ требует строгого соответствия, формулировки должны быть идентичными, и оценщики не будут принимать во внимание утверждения, представленные в обосновании.

Однако вполне возможно, что цели из ПЗ, о соответствии которому утверждается, могут быть структурированы или сформулированы совсем по-иному, так что простое соответствие отсутствует. В этом случае следует продемонстрировать, что цели безопасности для рассматриваемого ОО удовлетворяют требованиям разделов определения проблемы безопасности в профилях защиты, о соответствии которым утверждается. Исходя из этого, можно утверждать, что цели предоставляют такое же покрытие, что и цели из ПЗ, о соответствии которым утверждается, и таким образом обеспечивается согласованность.

Может оказаться невозможным привести убедительные доводы относительно достаточности, если в ПЗ или ЗБ утверждается о соответствии другим ПЗ, а в определении проблем безопасности из ПЗ, о соответствии которым утверждается, явно не охвачены все угрозы из определения проблемы безопасности рассматриваемого ПЗ. Решения для этой проблемы не существует — готовые к использованию продукты, соответствующие ПЗ, о соответствии которому утверждается, могут в точности соответствовать целям заказчика, однако в утверждении о соответствии ПЗ нет доказательств этому. Можно установить, что такие продукты действительно удовлетворяют требованиям заказчика, рассмотрев разделы ЗБ, связанные с угрозами, и приняв решение о том, что в них действительно рассмотрены и охвачены все применимые для заказчика угрозы.

11 Спецификация раздела «Определение расширенных компонентов»

В ряде случаев разработчик ПЗ или ЗБ не сможет специфицировать (изложить) функциональные требования безопасности и (или) требования доверия путем конкретизации существующих компонентов из ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3. В этих случаях ГОСТ Р ИСО/МЭК 15408 допускает определение расширенных (сформулированных в явном виде) компонентов. В данном разделе настоящего стандарта приведены некоторые рекомендации по спецификации расширенных компонентов.

При разработке ПЗ или ЗБ вместо использования расширенных компонентов следует сначала попытаться использовать существующие компоненты из ГОСТ Р ИСО/МЭК 15408 с соответствующим выполнением операций конкретизации (в частности, операции «уточнение»), а расширенные компоненты следует использовать только в тех случаях, когда это невозможно.

Конкретизация довольно часто позволяет решить проблему в том случае, когда с использованием компонента из ГОСТ Р ИСО/МЭК 15408 нельзя выразить конкретное требование, которое разработчик планирует изложить в ПЗ или ЗБ. Например, когда для разных типов пользователей различаются требования к аутентификации, это легко можно выразить с помощью уточнения компонентов класса FIA, которые отражают конкретные требования, посредством уточнений для характеристик типов пользователей, по отношению к которым применяются конкретные требования, и последующего использования совокупности компонентов для полного охвата всех типов пользователей. Аналогичным образом с помощью уточнений возможно изложить требования к управлению различными типами пользователей, субъектов, объектов или атрибутов безопасности.

В ГОСТ Р ИСО/МЭК 15408-1 приведены некоторые примеры уточнения требований, указывается, каким образом можно их использовать для более точной формулировки требований, а также даны рекомендации относительно определения расширенных компонентов. В настоящем стандарте приведены более подробные рекомендации.

До определения расширенного компонента необходимо исследовать опубликованные и прошедшие оценку ПЗ или ЗБ на предмет наличия определения расширенного компонента, который можно было бы использовать при определении функционального требования безопасности или требования доверия к безопасности, которое планирует включить разработчик. Использование уже определенного расширенного компонента из прошедшего оценку ПЗ или ЗБ имеет преимущество, состоящее в том,

что компонент уже проверен на непротиворечивость и соответствие требованиям ГОСТ Р ИСО/МЭК 15408 в рамках проведения оценки ПЗ или ЗБ, содержащих этот компонент.

В ГОСТ Р ИСО/МЭК 15408-1 требуется, чтобы при спецификации расширенных компонентов они были определены по аналогии с существующими компонентами ГОСТ Р ИСО/МЭК 15408 (с использованием предложенной в ГОСТ Р ИСО/МЭК 15408 структуры в качестве модели представления). Это относится к наименованию и обозначению расширенного компонента, способу изложения и уровню детализации. Что касается наименования расширенного компонента, необходимо определить, подходит ли компонент под один из классов или одно из семейств, уже определенных в ГОСТ Р ИСО/МЭК 15408, и выбрать обозначение, используя имя класса и (по возможности) имя семейства, добавив в идентификатор указание на то, что данный компонент является расширенным. По возможности компонент должен быть изложен в общем виде, допускающем применение операций назначения и (или) выбора. Это обеспечит разработчикам других ПЗ или ЗБ возможность использования расширенного компонента таким образом, чтобы он подходил для описания и их требований.

Описание расширенного компонента ФТБ с использованием функциональных компонентов ГОСТ Р ИСО/МЭК 15408 в качестве модели представления должно включать:

а) определение расширенного ФТБ на том же уровне абстракции, что и функциональные компоненты ГОСТ Р ИСО/МЭК 15408-2;

б) использование стиля и фразеологии (языка) функциональных компонентов ГОСТ Р ИСО/МЭК 15408-2;

в) использование подхода к топологии и номенклатуре компонентов в соответствии с ГОСТ Р ИСО/МЭК 15408-2.

Понимание того, что новый компонент ФТБ подобен другим компонентам, которые уже включены в состав существующего в ГОСТ Р ИСО/МЭК 15408 класса или семейства, способствует ограничению его новизны и использованию специфических для данного класса или семейства формулировок и понятий.

Стиль представления функциональных компонентов ГОСТ Р ИСО/МЭК 15408-2 предусматривает следующее:

а) большинство функциональных компонентов начинается фразой «ФБО должны», далее идет одно из следующих слов: предоставлять возможность, обнаруживать, осуществлять, обеспечивать, ограничивать, контролировать, разрешать, предотвращать, защищать, предоставлять;

б) используются устоявшиеся термины, такие как «атрибуты безопасности» и «уполномоченный пользователь»;

в) каждый элемент требований должен быть самостоятельным и понятным без каких-либо ссылок на другие элементы требований;

г) для каждого требования безопасности должна существовать возможность оценки, то есть должна существовать возможность сделать заключение о том, удовлетворяет ли ОО рассматриваемому требованию.

При формировании расширенного компонента ФТБ в явном виде необходимо также решить:

а) будут ли над ФТБ совершаться операции «выбор» и «назначение», подлежащие выполнению разработчиком ПЗ или ЗБ;

б) предполагает ли ФТБ какие-либо зависимости от других ФТБ, которые должны быть удовлетворены в ПЗ или ЗБ;

в) будет ли ФТБ требовать аудита каких-либо событий и, если будет, то какая информация о событиях подлежит регистрации;

г) будет ли ФТБ включать параметры безопасности, подлежащие управлению, например, зависеть от атрибутов безопасности, которые подлежат управлению.

Следует отметить, что для формулируемых в явном виде ФТБ нет необходимости определять операции, описанные в ГОСТ Р ИСО/МЭК 15408 («назначение», «выбор»), если не предполагается их повторное использование в ПЗ, ЗБ или функциональных пакетах.

Примечание — При разработке профилей защиты ФСТЭК России широко используются расширенные компоненты ФТБ с определенными для них операциями «назначение» и «выбор». Определение таких операций позволяет путем различного их выполнения определять различные ФТБ на основе одних и тех же компонентов требований:

- для усиления требований при переходе к ПЗ для старших классов защиты средств защиты информации одного вида или типа;
- для задания альтернативных ФТБ в ПЗ для разных типов средств защиты информации одного вида.

В качестве примера выполнения операций «назначение» и «выбор» для усиления требований при переходе к ПЗ для старших классов защиты рассмотрим расширенный (специальный) компонент ФТБ, используемый в ПЗ для средств контроля подключения съемных машинных носителей информации, утвержденных ФСТЭК России [3], [4].

Исходный расширенный компонент:

«FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

Иерархический для: нет подчиненных компонентов.

FDP_IFF_EXT.7.1 Функции безопасности средства контроля съемных машинных носителей информации должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*], основанную на следующих типах данных функций безопасности средства контроля съемных машинных носителей информации: [выбор: *интерфейсы ввода (вывода) средств вычислительной техники, типы подключаемых внешних программно-аппаратных устройств, конкретные съемные машинные носители информации, список пользователей* [*назначение: другие типы данных функций безопасности средства контроля съемных машинных носителей информации, используемых для реализации политики управления использованием подключаемых съемных машинных носителей информации*]].

Зависимости: FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации».

ФТБ на основе компонента FDP_IFF_EXT.7, используемые в профиле защиты для пятого класса защиты средств контроля подключения съемных машинный носителей информации:

«FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

FDP_IFF_EXT.7.1 ФБО должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*], основанную на следующих типах данных ФБО: *интерфейсы ввода (вывода) средств вычислительной техники, типы подключаемых внешних программно-аппаратных устройств* [назначение: *другие типы данных ФБО, используемых для реализации Политики управления использованием подключаемых съемных машинных носителей информации*].

Зависимости: FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации».

ФТБ на основе компонента FDP_IFF_EXT.7, используемые в профиле защиты для четвертого класса защиты средств контроля подключения съемных машинный носителей информации:

«FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации

FDP_IFF_EXT.7.1 ФБО должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*], основанную на следующих типах данных ФБО: *интерфейсы ввода (вывода) средств вычислительной техники, типы подключаемых внешних программно-аппаратных устройств, конкретные съемные носители информации* [назначение: *другие типы данных ФБО, используемых для реализации Политики управления использованием подключаемых съемных машинных носителей информации*].

Зависимости: FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации».

В качестве примера выполнения операций «назначение» и «выбор» для задания альтернативных ФТБ в ПЗ для разных типов средств защиты информации одного вида рассмотрим расширенный (специальный) компонент ФТБ, используемый в утвержденных ФСТЭК России профиле защиты для средств контроля подключения съемных машинный носителей информации и профиле защиты для средств контроля отчуждения (переноса) информации со съемных машинных носителей информации.

Исходный расширенный компонент:

«FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

Иерархический для: нет подчиненных компонентов.

FDP_IFC_EXT.3.1 Функции безопасности средства контроля съемных машинных носителей информации должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*] для [выбор: *съемных машинных носителей информации, специализированных съемных машинных носителей информации, используемых для хранения*

информации ограниченного доступа [назначение: *другие типы подключаемых программно-аппаратных устройств*]].

Зависимости: [FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации или FDP_IFF_EXT.8 Функции управления использованием специализированных съемных машинных носителей информации]».

ФТБ на основе компонента FDP_IFC_EXT.3, используемые в профиле защиты для средств контроля подключения съемных машинных носителей информации:

«FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

FDP_IFC_EXT.3.1 ФБО должны осуществлять [назначение: *Политика управления использованием подключаемых съемных машинных носителей информации*] для ***подключаемых произвольных*** *съемных машинных носителей информации* [назначение: *другие типы подключаемых программно-аппаратных устройств*].

Зависимости: [FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации или FDP_IFF_EXT.8 Функции управления использованием специализированных съемных машинных носителей информации]».

ФТБ на основе компонента FDP_IFC_EXT.3, используемые в профиле защиты для средств контроля отчуждения (переноса) информации со съемных машинных носителей информации:

«FDP_IFC_EXT.3 Политика управления использованием подключаемых съемных машинных носителей информации

FDP_IFC_EXT.3.1 ФБО должны осуществлять [назначение: *Политика управления использованием специализированных съемных машинных носителей информации*] для *специализированных съемных машинных носителей информации, используемых для хранения информации ограниченного доступа* [назначение: *другие типы подключаемых программно-аппаратных устройств*].

Зависимости: [FDP_IFF_EXT.7 Функции управления использованием подключаемых съемных машинных носителей информации или FDP_IFF_EXT.8 Функции управления использованием специализированных съемных машинных носителей информации]».

Наименование расширенного ФТБ, не включенного в ГОСТ Р ИСО/МЭК 15408-2, должно осуществляться в стиле, принятом для компонентов из ГОСТ Р ИСО/МЭК 15408-2, с использованием аналогичного подхода и принятых соглашений о наименовании. Для расширенных функциональных компонентов безопасности следует использовать букву «F» в наименовании для указания на то, что компонент функциональный, затем обозначение соответствующего класса и семейства, а затем номер компонента. Расширенный компонент, основанный на существующем классе, может быть размещен в соответствующем месте в рамках этого класса. Если расширенный компонент не связан с существующими классами, то для указания уже в наименовании на то, что он является новым, допустимо, например, создать класс компонентов («EXT») или добавить буквы («EXT») в конец имени компонента. Способ обозначения расширенного компонента можно указать в замечании по применению ПЗ или ЗБ. Следует следить за тем, чтобы соглашения по обозначению не противоречили при этом ГОСТ Р ИСО/МЭК 15408-2.

В приложении А приведены пример расширенного компонента и пояснение, по аналогии с тем, как это делается для компонентов ГОСТ Р ИСО/МЭК 15408-2. Это позволяет оценщику трактовать расширенный компонент по аналогии с компонентами, определенными в ГОСТ Р ИСО/МЭК 15408-2 при проведении оценки ПЗ или ЗБ, в которых определяется расширенный компонент.

Способом, аналогичным приведенному в примере из приложения А для расширенного функционального компонента безопасности, можно также определить расширенный компонент доверия к безопасности. Это имеет смысл, когда для типа продукта, описываемого в ЗБ или ПЗ, характерна определенная деятельность по обеспечению доверия, которая не охватывается существующими компонентами доверия к безопасности из ГОСТ Р ИСО/МЭК 15408-3. Помимо определения компонента доверия к безопасности в стиле, аналогичном используемому в ГОСТ Р ИСО/МЭК 15408-3, для расширенного компонента доверия к безопасности требуется также определить методику оценки, которая описывает деятельность оценщика по проверке соответствия продукта расширенному компоненту доверия к безопасности. Действия оценщика должны быть определены с использованием структуры и уровня детализации, определенных в ГОСТ Р ИСО/МЭК 18045 для проведения оценки компонентов из ГОСТ Р ИСО/МЭК 15408-3.

В расширенных компонентах доверия к безопасности следует предоставить определение следующих элементов (подробнее см. ГОСТ Р ИСО/МЭК 15408-1, подраздел С.3):

а) действий разработчика (заявителя, производителя);

В ПЗ, утвержденных ФСТЭК России, элементы действий разработчика названы как «элементы действий заявителя». Этим подчеркивается, что именно заявитель ответственен за предоставление свидетельств (документированных материалов) вместе с ОО для проведения сертификации по требованиям безопасности информации.

б) требований к содержанию и представлению свидетельств (документированных материалов), которые должен представить разработчик (заявитель, производитель);

В ПЗ, утвержденных ФСТЭК России, элементы содержания и представления свидетельств названы как «элементы содержания и представления документированных материалов». Данное уточнение сделано с целью исключения неоднозначности толкования термина «свидетельство» в русском языке.

в) действий оценщика (испытательной лаборатории).

В ПЗ, утвержденных ФСТЭК России, элементы действий оценщика названы как «элементы действий испытательной лаборатории». Данное уточнение сделано по причине того, что в системе сертификации ФСТЭК России в качестве оценщика выступает испытательная лаборатория.

В ГОСТ Р ИСО/МЭК 15408-3 продемонстрировано, что элементы, связанные с компонентами доверия, характеризуются следующим образом:

а) элементы действий разработчика предназначены для изложения действий, которые должен выполнить разработчик (обычно это представление свидетельств оценки);

б) элементы содержания и представления свидетельств предназначены для предъявления требований к содержанию и «качеству» свидетельств оценки, которые должен представить разработчик;

в) элементы действий оценщика включают в себя два типа элементов:

1) первым действием оценщика, связанным с компонентом доверия к безопасности, как правило, должно быть следующее:

«Оценщик должен подтвердить, что представленная информация отвечает всем требованиям к содержанию и представлению свидетельств»;

2) любой другой элемент действий оценщика обычно принимает вид изложения независимого шага оценивания и принятия решения оценщиком.

Следовательно, все требования к содержанию и представлению свидетельств должны быть не только ясно и понятно сформулированы, в них следует избегать (насколько возможно) требований субъективной оценки со стороны оценщика. Расширенное требование доверия к безопасности (ТДБ) должно определять ясные объективные критерии, на основе которых оценщик может сделать свое заключение. Для пояснения ТДБ целесообразно использовать операцию «уточнение» либо сформулировать «замечания по применению». Представление пояснения ТДБ способствует проведению оценки.

Целесообразно излагать расширенные ТДБ в стиле изложения компонентов доверия к безопасности, определенных в ГОСТ Р ИСО/МЭК 15408-3. Поэтому каждое отдельное требование необходимо оформлять в виде отдельного элемента требований. При этом необходимо при описании расширенного ТДБ обращаться к ГОСТ Р ИСО/МЭК 15408-1 (раздел 3) и использовать приведенную там терминологию, которая также используется и в ГОСТ Р ИСО/МЭК 15408-3.

Информацию об обозначении расширенных компонентов, использованных в ПЗ или ЗБ, рекомендуется включать в подраздел (или пункт), устанавливающий соглашения, например, в тот же, где изложены соглашения о стилях отображения результатов операций над компонентами.

Ниже представлен фрагмент такого подраздела на примере подраздела «Соглашения» ПЗ, утвержденных ФСТЭК России.

«…В настоящий ПЗ включен ряд требований безопасности, сформулированных в явном виде. Краткая форма имен компонентов требований, сформулированных в явном виде, содержит текст (EXT)».

После определения расширенного компонента ТДБ необходимо также определить шаги оценивания, которые необходимо выполнить оценщику для того, чтобы удостовериться в соответствии расширенному компоненту ТДБ. При этом в качестве примера следует использовать шаги оценивания из ГОСТ Р ИСО/МЭК 18045. Шаги оценивания должны охватывать все аспекты расширенного компонента ТДБ и давать оценщику четкие рекомендации по проведению оценки.

12 Спецификация раздела «Требования безопасности»

12.1 Введение

Данный раздел содержит рекомендации по формированию в ПЗ и ЗБ требований безопасности ИТ для ОО.

В ПЗ и ЗБ формулируются следующие типы требований безопасности ИТ:

а) функциональные требования безопасности ОО (ФТБ). Функциональные требования безопасности определяют требования к функциональным возможностям безопасности, которыми должен обладать ОО для того, чтобы обеспечить достижение целей безопасности для ОО;

б) требования доверия к безопасности ОО (ТДБ). Требования доверия к безопасности определяют требуемый уровень доверия к реализации ФТБ.

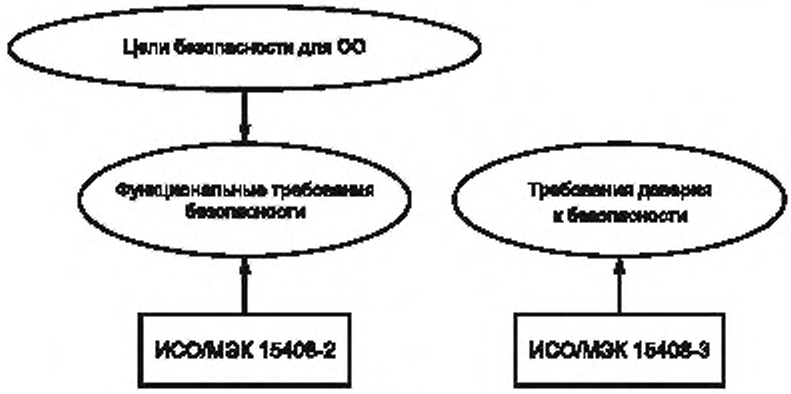

Рисунок 3 — Формирование требований безопасности ИТ

Как следует из рисунка 3, требования безопасности ИТ могут быть сформированы, где это возможно, с использованием каталога функциональных компонентов, определенных в ГОСТ Р ИСО/МЭК 15408-2, и каталога компонентов доверия к безопасности, определенных в ГОСТ Р ИСО/МЭК 15408-3.

Использование каталогов требований, определенных в ГОСТ Р ИСО/МЭК 15408, позволяет достичь определенного уровня стандартизации в области представления требований безопасности, что значительно облегчает сравнение ПЗ и ЗБ между собой. Руководство по поводу того, каким образом получить функциональные требования безопасности на основе парадигмы функциональных требований, изложенных в ГОСТ Р ИСО/МЭК 15408, приведено в 12.2.

Если в ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 отсутствуют соответствующие функциональные компоненты или компоненты доверия к безопасности, требования безопасности ИТ могут быть сформулированы в явном виде. При этом сформулированные в явном виде требования безопасности ИТ должны быть однозначными, подлежащими оценке и изложенными в стиле, подобном стилю изложения существующих компонентов ГОСТ Р ИСО/МЭК 15408.

В 12.3.7 и 12.4.3 даны рекомендации по спецификации соответственно ФТБ и ТДБ в тех случаях, когда в ГОСТ Р ИСО/МЭК 15408-2 и ГОСТ Р ИСО/МЭК 15408-3 нет подходящих компонентов требований для формулирования рассматриваемых ФТБ и ТДБ.

ГОСТ Р ИСО/МЭК 15408 обеспечивает определенную степень гибкости формирования ФТБ и ТДБ на основе компонентов требований, определяя набор разрешенных операций над компонентами. Разрешенными операциями являются следующие: назначение, итерация, выбор и уточнение.

Рекомендации по выполнению операций над функциональными компонентами, определенными в ГОСТ Р ИСО/МЭК 15408, приведены в 12.3.2; над компонентами доверия к безопасности — в 12.4.2.

При этом следует отметить, что в ГОСТ Р ИСО/МЭК 15408 каждому компоненту требований безопасности назначается основанное на определенной таксономии уникальное краткое имя.

Например, для FAU_GEN.1.2 из ГОСТ Р ИСО/МЭК 15408-2 краткое имя имеет следующий вид:

а) 'F' указывает на то, что это функциональное требование;

б) 'AU' указывает на то, что ФТБ принадлежит классу ФТБ «Аудит безопасности»;

в) 'GEN' указывает на то, что ФТБ принадлежит семейству «Генерация данных аудита безопасности» класса FAU;

г) '1' указывает на то, что это ФТБ «генерации данных аудита» в рамках семейства FAU_GEN;

д) '2' указывает на то, что ФТБ является вторым элементом компонента FAU_GEN.1.

В ГОСТ Р ИСО/МЭК 15408-3 используется схожее обозначение, кроме того, каждый элемент относится к одному из трех наборов элементов доверия:

а) 'D' указывает на то, что элемент относится к элементам действий разработчика (заявителя);

б) 'C' указывает на то, что элемент относится к элементам содержания и представления свидетельств (документированных материалов);

в) 'E' указывает на то, что элемент относится к элементам действий оценщика испытательной лаборатории.

Например, для ADV_TDS.1.2C из ГОСТ Р ИСО/МЭК 15408-3 краткое имя имеет следующий вид:

а) 'A' указывает на то, что это требование доверия;

б) 'DV' указывает на то, что ТДБ принадлежит классу «Разработка»;

в) 'TDS' указывает на то, что ТДБ принадлежит семейству «Проект ОО» класса ADV «Разработка»;

г) '1' указывает на то, что это ТДБ «Базовый проект» в рамках семейства ADV_TDS;

д) '2' указывает на то, что ФТБ является вторым элементом в наборе элементов доверия;

е) 'C' указывает на то, что элемент относится к элементам содержания и представления свидетельств (документированных материалов) рассматриваемого компонента.

Требования ФТБ и ТДБ выбираются на уровне компонентов: все элементы, входящие в компонент, должны быть включены в ПЗ или ЗБ, если в ПЗ или ЗБ включается рассматриваемый компонент.

В процессе выбора требований безопасности ИТ необходимо учитывать следующие два типа взаимосвязей между компонентами требований безопасности ИТ:

1) компоненты одного семейства могут находиться в иерархической связи. Отношение иерархии предполагает, что один компонент содержит все требования, определенные в другом компоненте этого семейства. Например, FAU_STG.4 иерархичен по отношению к FAU_STG.3, потому что все функциональные элементы, определенные в FAU_STG.3, также включены в FAU_STG.4. Однако, FAU_STG.4 не иерархичен по отношению к FAU_STG.1, и поэтому может потребоваться включение в разрабатываемый ПЗ или ЗБ обоих этих компонентов;

2) компоненты могут иметь зависимости от компонентов других семейств, что указывает на то, что компонент не является самостоятельным и полагается на функциональные возможности, предусмотренные другим компонентом или на взаимодействие с другим компонентом для выполнения своих функций. Например, компонент FIA_UAU.1 (связанный с требованием аутентификации пользователей) зависит от компонента FIA_UID.1 (связанного с требованием идентификации пользователей).

12.2 Парадигмы безопасности ГОСТ Р ИСО/МЭК 15408

12.2.1 Пояснение парадигм безопасности и их использование для моделирования функциональных возможностей безопасности

Для обеспечения лучшего понимания структуры классов, семейств и компонентов, определенных для функциональных требований безопасности в ГОСТ Р ИСО/МЭК 15408-2, в настоящем стандарте рассматривается парадигма функциональных требований безопасности, изложенная в ГОСТ Р ИСО/МЭК 15408-2 (раздел 5).

Назначение парадигмы безопасности в ГОСТ Р ИСО/МЭК 15408 состоит в том, чтобы предоставить основу для уточнения функциональных возможностей безопасности ОО до той степени детализации, которая требуется для демонстрации возможности достижения в рамках этой модели целей безопасности. Изложенные в предыдущих разделах парадигмы могут использоваться для разработки абстрактной модели функциональных возможностей безопасности, которая затем выражается с помощью функциональных требований безопасности, определенных в ГОСТ Р ИСО/МЭК 15408-2. В последующих пунктах приведены рекомендации по разработке такой модели и ее описанию с использованием функциональных требований безопасности.

12.2.2 Управление доступом к ресурсам и объектам и управление их использованием

12.2.2.1 Пояснение

В соответствии с парадигмой ГОСТ Р ИСО/МЭК 15408-2 функциональные возможности безопасности контролируют использование ресурсов, защищаемых ОО. Ресурсы могут быть либо внутренними по отношению к ОО (например, оперативная память, процессорное время, дисковое пространство, сервисы и т. д.), либо могут быть расположены вне ОО, но доступ к ним (по крайней мере для некоторых сущностей) при этом осуществляется под управлением функций ОО (например, сетевые сервисы, предоставляемые другой системой). Типичным примером ОО, контролирующим использование ресурсов, не являющихся частью ОО, является межсетевой экран.

Примерами ресурсов, которыми может потребоваться управлять для достижения целей безопасности, являются:

- память (как оперативная память, так и дисковое пространство);
- процессорное время;
- периферийные устройства или сетевые соединения;
- функции.

Пользователи определены в ГОСТ Р ИСО/МЭК 15408-1 как «сущность, взаимодействующая с ОО из-за пределов границ ОО». Субъекты определены в ГОСТ Р ИСО/МЭК 15408-1 как «активная сущность в ОО, выполняющая операции над объектами». Пользователи и субъекты являются активными сущностями, которые запрашивают сервисы ОО и тем самым взаимодействуют с объектами и ресурсами.

Для достижения целей безопасности использование ресурсов контролируется в ОО на основе правил, которые необходимо выполнять ОО. Эти правила могут управлять использованием ресурсов, а также регистрировать процессы, связанные с использованием ресурсов.

Перечень параметров (далеко неполный), которые могут подвергаться оценке в рамках этих правил, включает:

- тип и идентификатор сущности, которая инициировала запрос;
- другие атрибуты сущности, которая инициировала запрос;
- тип и идентификатор ресурса, на который направлен запрос;
- другие атрибуты ресурса, на который направлен запрос;
- тип запроса;
- время и дата;
- внутреннее состояние ОО.

Для реализации правил на основе вышеуказанных параметров от ОО требуются поддержка и управление этими параметрами:

- для внешних сущностей (также называемых «пользователями») следует идентифицировать и, возможно, аутентифицировать эту внешнюю сущность, хотя бы в той мере, которая необходима для выполнения правил. Если правила основаны только на параметрах внешней сущности, относящейся к конкретной группе внешних сущностей, то для ОО достаточно идентифицировать и, возможно, аутентифицировать эту совокупность или группу;

- достаточно часто ОО поддерживает перечень внешних сущностей и, возможно, их атрибуты безопасности, которым разрешено использование сервисов, находящихся под управлением ФБО. В этом случае требуются функциональные возможности по управлению перечнем внешних сущностей и их атрибутами безопасности (при условии, что перечень не является статичным).

Часть ОО, которая реализует функциональные возможности безопасности, используемые для достижения целей безопасности, а также все другие части ОО, способные изменять либо обходить функциональные возможности безопасности, называются «Функциональными возможностями безопасности ОО» (ФБО). В зависимости от архитектуры ОО функциональные возможности ОО могут совпадать с ОО либо составлять определенную часть ОО. Если ФБО представляют собой только часть ОО, то важно, чтобы никакая другая часть ОО, не входящая в состав ФБО, не могла влиять на ФБО или обходить их способом, нарушающим достижение целей безопасности.

И внешние сущности, и субъекты, которые запрашивают сервисы, при использовании управляемых ресурсов будут использовать интерфейсы ФБО (ИФБО).

В некоторых случаях субъекты действуют от лица внешних сущностей. В таких случаях внешняя сущность (или пользователь) «связывается» с субъектом. В рамках этого процесса связывания для отражения связывания зачастую должны вноситься изменения в атрибуты безопасности. Примером могут служить ОО, в которых субъект наследует атрибуты безопасности внешней сущности, но могут применяться и более сложные правила, определяющие, например, каким образом наследуются атрибуты безопасности субъекта в рамках процесса связывания.

Ресурсы могут быть сгруппированы по «объектам», и в ОО могут быть реализованы определенные правила использования этих объектов, отличные от правил использования ресурсов, входящих в состав объекта. Примером может служить ОО, реализующий правило в отношении максимальных квот для дискового пространства (ресурса) и правило управления доступом к файлам (объектам), созданным на основе ресурсов дискового пространства. Этот пример демонстрирует, что один и тот же ресурс может быть предметом рассмотрения в рамках разных правил, реализуемых ОО, когда один набор правил регулирует использование ресурса, а другой набор правил предназначен для объектов, созданных на основе ресурсов.

Правила, регулирующие доступ к объектам и их использование, обычно различаются для различных типов объектов. Чтобы избежать путаницы, ГОСТ Р ИСО/МЭК 15408 позволяет формировать набор правил для различных объектов, субъектов и операций в виде различных «политик функций безопасности» (ПФБ) и ссылаться в отдельных ФТБ на ПФБ для указания ПФБ, к которой относятся данные ФТБ. Политика функции безопасности всегда должна иметь определенную «область действия», представляющую собой определение набора субъектов, пользователей, объектов, ресурсов и операций, по отношению к которым она применяется. При определении области действия ПФБ определение набора субъектов, пользователей, объектов, ресурсов и операций должно быть четким и однозначным. Правила, реализуемые посредством действий субъектов или пользователей при использовании объектов или ресурсов, определяются как часть ПФБ. Эти правила обычно основываются на конкретных атрибутах субъектов, пользователей, объектов или ресурсов. Атрибуты, влияющие на правила ПФБ, называются «атрибутами безопасности». Требования к управлению атрибутами безопасности, существенными для ПФБ, также являются частью ПФБ, в том числе и определение того, как осуществляется инициализация атрибутов безопасности при создании, импорте или регистрации (для пользователей) сущности, охватываемой ПФБ. Таким образом, ПФБ описывает правила доступа и использования определенного множества объектов или ресурсов с помощью определенного набора активных сущностей (пользователей или субъектов), используя определенный набор операций и функций управления атрибутами безопасности, применяемых в этих правилах.

Типичным примером является политика управления доступом для объектов файловой системы в операционной системе. Активные сущности представляют собой процессы, некоторые из которых выполняются от лица пользователя и, следовательно, им присущи атрибуты безопасности, порождаемые при связывании на основе атрибутов безопасности пользователя. Операциями являются такие системные вызовы, которые выполняются на объектах файловой системы. Например, открытие файла для чтения, записи или изменения, просмотр либо изменение атрибутов файлов, создание либо удаление файла. Кроме того, существуют операции, которые управляют атрибутами безопасности процессов или объектов файловой системы. Типичными примерами атрибутов безопасности, которые являются существенными для такой ПФБ, являются:

- атрибуты безопасности объектов: списки управления доступом, тип файла;
- атрибуты безопасности пользователей: идентификаторы пользователей, роли пользователей;
- атрибуты безопасности процессов: идентификатор процесса, уровень доверия к процессу.

Другие ПФБ могут регулировать операции, которые внешние сущности выполняют напрямую, без промежуточного субъекта. В качестве примера можно привести средство межсетевого экранирования, которое регулирует, каким образом сетевые сервисы и функции могут использоваться внешней по отношению к ОО системой. При этом также существуют активные сущности (внешние системы, которые инициализируют запрос), объекты (внешние системы, которые являются целью запроса) и операции (сетевые сервисы). Правила такой ПФБ могут базироваться на определении внешних по отношению к ОО систем, вовлеченных в операцию, типе выполняемой операции (например, используемый порт), контексте операции (например, установлено ли было ранее соединение через конкретный порт) и (или) содержимом сетевых пакетов.

Обычной практикой является определение более одной ПФБ даже для одного и того же множества пользователей, субъектов, объектов и операций. Примером являются политика дискреционного управления доступом (первая ПФБ) и политика мандатного управления доступом (вторая ПФБ). Хотя множество пользователей, субъектов, объектов и операций, рассматриваемых в ПФБ, являются одним и тем же, правила ПФБ и набор атрибутов безопасности, используемых в этих правилах, различаются, что оправдывает определение двух ПФБ.

12.2.2.2 Использование

Политики управления доступом предоставляют основу для моделирования ОО в терминах ресурсов и объектов, а также операций, разрешенных над этими ресурсами и объектами, посредством ОО (либо через ОО) для активных сущностей (расположенных как в границах ОО, так и вне ОО). Таким образом, первым шагом при построении модели ОО, пригодной для определения функциональных требований безопасности, связанных с управлением доступом, является определение ресурсов, объектов, операций, предоставляемых ОО, а также субъектов и пользователей, инициирующих операции. Первоначально модель должна включать только те типы ресурсов, объектов, операций, субъектов и пользователей, которые напрямую следуют из целей безопасности и общих функциональных возможностей ОО, описываемых в начале ПЗ или ЗБ. При разработке ЗБ для существующего продукта ИТ или системы ИТ, сущности, определенные в модели, должны иметься для ОО. При определении

функциональных требований безопасности этот первоначальный набор, возможно, потребуется уточнить для обеспечения непротиворечивости и полноты.

Определение в модели сущностей, отсутствующих в ОО, приведет к проблемам во время оценки, так как согласно ГОСТ Р ИСО/МЭК 15408 предполагается, что ФТБ и сущности, упомянутые в ФТБ, являются абстрактными моделями сущностей, которые существуют в ОО и, следовательно, могут быть отображены посредством уточнения на сущности в проекте или реализации ОО.

Затем должны быть определены правила, регулирующие доступ к ресурсам и объектам и их использование посредством операций для субъектов и (или) пользователей, определенных в модели таким образом, чтобы были достигнуты цели безопасности. При разработке ЗБ для существующего ОО, правила для сущностей, определенных в модели, должны по возможности быть абстрактной моделью реального поведения ОО, чтобы правила, реализуемые ОО, являлись уточнениями правил в модели.

Частью определения правил является идентификация параметров, которые используются в этих правилах. По всей вероятности, потребуется определить атрибуты безопасности ресурсов, пользователей, субъектов и объектов. Эти атрибуты безопасности следует представить в виде совокупного списка, так как могут потребоваться правила для инициализации и управления.

При определении этих правил достаточно часто оказывается, что для разных видов ресурсов, объектов, пользователей, субъектов или операций правила различаются. Чтобы упростить описание модели, следует сформировать наборы ресурсов, объектов, пользователей, субъектов и операций с идентичными (или почти идентичными) правилами в ПФБ. Каждой ПФБ следует присвоить имя, позволяющее идентифицировать ее уникальным образом.

Следует определить правила для создания и удаления субъектов и объектов. Для различных типов субъектов и объектов эти правила могут различаться. В этих правилах необходимо также определить, каким образом инициализировать атрибуты субъектов и объектов.

Следует определить правила для управления атрибутами безопасности субъектов и объектов в случаях, когда эти атрибуты не являются статическими. Эти правила могут включать операции, инициализируемые внешними сущностями посредством ИФБО, а также правила, описывающие, каким образом изменяются атрибуты безопасности в рамках операций, выполняемых ФТБ.

Следует определить правила регистрации («создания») и удаления пользователей, если в ОО необходимо регистрировать пользователей. Правила регистрации пользователей включают в себя также правила инициализации атрибутов безопасности пользователей. В некоторых случаях регистрация пользователей не требуется. Они могут запрашивать сервисы, проходить идентификацию и, возможно, аутентификацию, предоставляя данные для установления своей подлинности (аутентификационные данные). Эти данные могут также включать атрибуты безопасности пользователя. В этих случаях должны быть определены правила, которые определяют принимаемые данные для установления своей подлинности и способ их проверки.

Следует определить правила идентификации и (при необходимости) аутентификации пользователей. Эти правила определяют учетные данные, которые должен предоставить пользователь (тип учетных данных, возможные ограничения на учетные данные, например, минимальная и максимальная длина, минимальный и максимальный срок действия и т. д.), а также ответную реакцию ФБО при предоставлении неверных учетных данных.

Следует определить правила управления атрибутами безопасности пользователей. Это делается по аналогии с определением атрибутов безопасности субъектов и объектов.

Если ОО поддерживает функцию связывания пользователь — субъект, следует определить правила, используемые при таком связывании. Эти правила могут включать в себя:

- условия, которые должны быть выполнены для разрешения связывания;
- установку атрибутов безопасности субъекта после связывания.

После этого необходимо проанализировать, требуются ли дополнительные правила управления. Примером такого дополнительного правила является правило, позволяющее создать новый атрибут безопасности (например, новую роль пользователя), возможно, вместе с правилами, которые определяют, каким образом управлять этим атрибутом безопасности (например, определение набора атрибутов безопасности пользователя, получаемых им в рамках роли).

12.2.3 Управление пользователями

12.2.3.1 Пояснение

В парадигме ГОСТ Р ИСО/МЭК 15408 пользователь является внешней по отношению к ОО сущностью, которая запрашивает сервисы ОО, используя его интерфейсы. Пользователям, возможно, потребуется зарегистрироваться, прежде чем они смогут использовать сервисы ОО, либо ОО может разрешать

пользователям запрашивать некоторые сервисы без предварительной регистрации. Во многих случаях решение ОО о предоставлении запрашиваемого сервиса зависит от некоторых атрибутов безопасности пользователя. Атрибуты безопасности пользователя могут либо быть представлены пользователем вместе с запросом, либо могут быть получены из хранящихся в ОО данных о пользователе либо группе, к которой принадлежит пользователь.

В первом случае ОО необходимо удостовериться, что атрибуты безопасности, представленные пользователем, доверенные. Это подразумевает, что ОО реализует правила, устанавливающие, каким образом оцениваются атрибуты безопасности, и удостоверяется в том, что пользователь (который может быть неизвестен) использует атрибуты безопасности правомерно.

Во втором случае ОО необходимо знать идентификатор пользователя или группы, к которой он принадлежит. Кроме того, в этом случае в ОО необходимо реализовать правила, определяющие, каким образом можно проверить, что заявленные идентификатор пользователя или участие пользователя к группе являются корректными. Этот процесс называется аутентификацией и требует, чтобы пользователь предоставил аутентификационные данные, используемые ОО для формирования доверия к правильности заявленного идентификатора или членства в группе. Должны быть определены правила, которые специфицируют, каким образом выполняется процесс аутентификации и каким образом можно управлять параметрами процесса аутентификации.

Если требуется регистрация пользователей, то необходимо определить правила в отношении того, каким образом пользователи могут регистрироваться и каким образом можно управлять их атрибутами безопасности.

В некоторых случаях ОО будет использовать один из своих субъектов для действий от лица пользователя. В этом случае субъект «привязан к пользователю» с помощью ФБО, то есть в ФБО должны быть правила в отношении того, каким образом определяются атрибуты безопасности субъекта, когда он связан с пользователем. Очень часто субъект наследует часть атрибутов безопасности пользователя, что позволяет применять атрибут безопасности пользователя в соответствии с политиками управления доступом даже в том случае, когда фактический доступ выполняется субъектом.

12.2.3.2 Использование

Для определения функций управления пользователями требуется выполнить следующие шаги:

- идентифицировать и определить типы пользователей, которые могут получить доступ к ОО (вместе с набором атрибутов безопасности, которые могут быть присвоены каждому типу пользователей);
- идентифицировать для каждого типа пользователей, должны ли пользователи проходить регистрацию перед использованием функций ОО;
- для каждого типа пользователей, которым необходимо проходить регистрацию, определить правила регистрации пользователя (как выполняется регистрация) и атрибуты безопасности пользователя, которые должны быть установлены при регистрации;
- определить для каждого типа пользователей, требуется ли идентификация. Если идентификация требуется, то необходимо определить правила, указывающие на то, каким образом осуществляется идентификация пользователя;
- определить для каждого типа пользователей, требуется ли аутентификация. Если аутентификация требуется, то необходимо определить правила, указывающие на то, каким образом осуществляется аутентификация пользователя, и определить условия, при которых пользователю необходимо проходить аутентификацию;
- определить правила управления процессом аутентификации (включая управление учетными данными, используемыми для аутентификации);
- для каждого типа пользователей определить правила управления атрибутами безопасности пользователя;
- если возможно либо требуется связывание пользователь — субъект, необходимо определить правила для осуществления такого связывания. Особо следует определить правила безопасности, указывающие на то, каким образом устанавливаются в ходе связывания атрибуты безопасности субъекта.

12.2.4 Собственная защита ОО

12.2.4.1 Пояснение

Собственная защита функций безопасности требуется в случае наличия одного из следующих условий:

- в предполагаемой среде функционирования ОО источник угроз имеет возможность провести атаку на функций безопасности таким образом, что цель безопасности может быть не достигнута;
- цель безопасности может быть не достигнута из-за сбоя элемента среды функционирования ОО;

- цель безопасности может быть не выполнена из-за сбоя элемента ФБО.

В этих случаях необходимо определить функции собственной защиты в рамках ФБО, которые обнаруживают эти условия и реагируют на них способом, позволяющим выполнить цели безопасности и в таких условиях.

Определение собственной защиты ОО в функциональной модели требует:

- идентификации возможных сценариев атак и сбоев, способных нарушить достижение какой-либо цели безопасности;
- идентификации функции, способной предотвратить атаку или сбой. Примером такой функции является усиленная физическая защита ОО, предотвращающая определенные физические атаки;
- идентификации функций обнаружения атак и соответствующего реагирования на атаки или сбои в случаях, когда невозможно предотвратить атаки и сбои (распространенный случай).

Обнаружение атаки извне или сбоя системы в среде функционирования ОО может требовать мониторинга использования ИФБО и проверки на наличие условий, возникающих в результате атаки, мониторинга состояний линий связи на предмет возникновения состояний, свидетельствующих об атаке, или мониторинга посредством датчиков (сенсоров, агентов), имеющихся в составе ОО для обнаружения атак.

12.2.4.2 Использование

Для определения функций собственной защиты ОО необходимо из определения проблемы безопасности идентифицировать, требуются ли такие функции для достижения целей безопасности. Если требуются, то необходимо выбрать, требуется ли предотвращать атаку извне (например, с помощью усиления некоторых мер физической защиты) либо требуется обнаруживать атаку или сбой и обеспечивать своевременное ответное реагирование.

Следует начинать с перечня атак или сбоев, которые могут произойти в предполагаемой среде функционирования ОО и которые, если их игнорировать, потенциально нарушают достижение целей безопасности. Для каждого элемента перечня следует определить, каким образом предусмотрена обработка случаев атак либо сбоев, например предотвращаются ли они реализованными функциональными возможностями безопасности ОО, либо существует необходимость определить функциональные возможности безопасности ОО, которые обнаруживают атаку либо сбой и обеспечивают соответствующее реагирование.

В случае наличия функции, предотвращающей атаку, должно быть предоставлено ее описание с соответствующим обоснованием того, для отражения каких типов атак она предназначена.

Для случая обнаружения и реагирования должны быть определены (на абстрактном уровне) критерии и правила обнаружения (следует сформулировать в виде абстрактного правила, что, как предполагается, ОО должен делать в подобном случае).

Обнаружение сбоев ФБО может быть осуществлено посредством мониторинга переменных внутреннего состояния, внутренних функций, выполняя тесты, или с помощью избыточных функций или данных и проверки их на непротиворечивость.

Ответное реагирование может состоять:

- в корректирующем действии, которое устраняет последствие атаки или сбоя. Примерами являются функции, которые могут обнаружить и автоматически исправить сбой на основе избыточности данных или функциональных возможностей;
- в корректирующем действии, которое частично устраняет последствия атаки или сбоя, но приводит к некоторому сокращению функциональных возможностей ОО (которые должны согласовываться с целями безопасности). Примерами являются функции восстановления после сбоя или атаки, однако восстановление может занять время и может быть не полным. В таких случаях нужно обеспечить, чтобы не происходило задержки либо потери функциональных возможностей или данных вследствие того, что неполное восстановление нарушает достижение каких-либо целей безопасности;
- подготовке ОО для корректирующего действия, выполняющегося вручную (например, остановка частей ОО, которые подверглись воздействию при атаке или при сбое, либо всего ОО, с требованием, чтобы остановленные части либо ОО в целом были перезапущены в безопасном режиме);
- остановке поврежденных частей ОО или всего ОО без предоставления в рамках ФБО метода надежной перезагрузки. Примером является ОО, который уничтожает важные функции или данные при обнаружении атаки или сбоя для поддержки уверенности в том, что ОО не нарушает целей безопасности.

Перечень приведенных корректирующих действий упорядочен по увеличению степени воздействия на функциональные возможности ОО.

12.2.5 Защита каналов связи

12.2.5.1 Пояснение

Функции защиты данных при обмене информацией с внешней сущностью либо при передаче между различными частями распределенного ОО с использованием ненадежного или недоверенного канала связи являются еще одним примером функций, которые требуют дополнительного моделирования. Для моделирования обмена данными должны быть определены свойства безопасности канала связи. Такие свойства могут включать:

- аутентификацию участников обмена данными;
- защиту целостности данных, передаваемых по каналу связи (может включать защиту от повторной передачи перехваченных сообщений и (или) изменения последовательности сообщений);
- защиту конфиденциальности данных, передаваемых по каналу связи;
- защиту от потери данных;
- обеспечение неотказуемости при отправке и (или) получении сообщений.

Для моделирования канала передачи данных должны быть определены узлы коммуникации, а также характеристики безопасности канала связи. Это относится и к каналам передачи данных, функционирующим в реальном масштабе времени, и к неактивным каналам передачи данных.

12.2.5.2 Использование

Идентификация функций, необходимых для обеспечения безопасности, требует выполнения следующих шагов:

- идентификация каналов (соединений);
- определение необходимых характеристик безопасности для каждого канала связи. Примерами таких характеристик безопасности являются:
- аутентификация узлов;
- обеспечение целостности (возможно, включая защиту от повторной передачи перехваченных сообщений, защиту последовательности сообщений и т. д.);
- обеспечение конфиденциальности (возможно, включая защиту от анализа трафика);
- обеспечение неотказуемости (факта отправки, получения или и того и другого);
- обеспечение защиты от потери передаваемых данных.

Для каждого из каналов должны быть определены необходимые характеристики безопасности. В ЗБ определяются также механизмы, используемые для реализации этих характеристик безопасности. В ПЗ механизмы должны быть определены только до требуемого уровня детализации. Этот уровень детализации может быть достаточно высоким, если для любого соответствующего профилю защиты ОО предполагается также, что он должен удовлетворять требованиям по возможности взаимодействия (функциональной совместимости). В этих случаях в ПЗ может быть определен механизм даже вплоть до уровня конкретного протокола, а также параметры протокола (например, криптографический алгоритм в соответствии с законодательством Российской Федерации), которые необходимы для обеспечения совместимости.

При идентификации перечня каналов следует рассматривать не только физические каналы связи, но и логические каналы (например, на уровне протоколов прикладного уровня), которые требуют специфической защиты. Такие каналы могут размещаться в стеке на разных уровнях протоколов, когда отдельные уровни обеспечивают разные типы защиты. Например, IPsec на уровне IP может обеспечивать аутентификацию узлов (в данном случае систем), а также защиту целостности и конфиденциальности. Протокол прикладного уровня (который может представлять разные логические каналы связи) на уровне выше, чем IPsec, может обеспечить дополнительную аутентификацию (например, пользователя или приложения), а также выполнение функции обеспечения неотказуемости. В этом случае IPsec и протокол прикладного уровня следует перечислить как отдельные каналы с собственными характеристиками безопасности.

Следует отметить, что большинство функций обеспечения безопасности каналов реализуют защиту целостности и защиту от потери данных путем обнаружения условий, связанных с соответствующими нарушениями. По аналогии с функциями обнаружения, описанными в 12.2.4 «Собственная защита ОО», может возникнуть необходимость в определении реакции ОО при обнаружении рассмотренных выше условий. Кроме того, может возникнуть необходимость в определении реакции на неуспешные попытки аутентификации и отрицания факта получения или отправки данных.

Следует также отметить, что экспорт данных ФБО или данных пользователя из области управления ОО и импорт данных ФБО или данных пользователя в ОО может рассматриваться как особый

случай передачи данных, когда взаимодействующий объект (узел) неизвестен. В случае экспорта и импорта данных могут рассматриваться следующие характеристики:

- обеспечение целостности (возможно, включая защиту от повторной передачи перехваченных сообщений, контроль «давности» сообщений и т. д.);
- обеспечение конфиденциальности;
- обеспечение неотказуемости (при экспорте, импорте или и том и другом).

12.2.6 Аудит безопасности

12.2.6.1 Пояснение

Мониторинг определенных критичных событий, связанных с безопасностью, и поддержка регистрации этих событий для последующего анализа или оценка при автоматическом реагировании на эти события является еще одной функцией безопасности, которая может быть необходима ОО для достижения целей безопасности. Критичными событиями, связанными с безопасностью, могут быть события, непосредственно связанные с запросами на использование сервисов ОО активными сущностями, а также связанные с обнаружением критического состояния безопасности или события, которое может быть не связано напрямую с таким запросом.

Примерами таких критических событий безопасности являются:

- успешные и (или) неуспешные попытки использования сервисов, предоставляемых ФБО;
- неожиданное возникновение сбоя;
- неожиданное или некорректное поведение (режим функционирования) удаленного доверенного продукта ИТ;
- сбой, обнаруженный функцией собственного тестирования;
- изменение заданных критических порогов безопасности для критичных данных ФБО;
- возникновение большого числа событий, каждое из которых в отдельности не является достаточно критичным для регистрации в журнале аудита.

12.2.6.2 Использование

Для построения модели аудита безопасности требуется:

- сформировать список событий, подлежащих аудиту;
- определить правила, устанавливающие, в каком случае событие подлежит аудиту (например, только при отклонении запроса);
- определить данные, которые должны быть указаны при регистрации каждого события;
- определить правила обработки и анализа собранных данных аудита.

Целесообразно проводить анализ каждой отдельной функциональной возможности безопасности, если имеются подлежащие аудиту события, связанные с этой функциональной возможностью безопасности. Кроме того, должен быть осуществлен анализ модели функциональных возможностей безопасности в отношении необходимости генерации записей аудита при возникновении критических внутренних состояний.

12.2.7 Требования к архитектуре объекта оценки

12.2.7.1 Пояснение

В дополнение к перечисленным выше требованиям может оказаться необходимым определить требования к архитектуре ОО. Такие требования могут быть нужны для того, чтобы обеспечить возможность проведения анализа архитектуры, а также для поддержки понимания архитектуры ОО. Эти требования обычно связаны с конкретными характеристиками, которые должен реализовывать ОО. Типичными примерами таких характеристик являются:

- отказоустойчивость;
- управление потоками информации;
- характеристики обеспечения конфиденциальности;
- характеристики функционирования в режиме реального времени.

Требования к архитектуре зачастую поддерживаются требованиями, рассмотренными в предыдущих пунктах. Например, управление потоками информации и обеспечение конфиденциальности обычно сопровождаются определенными правилами, регулирующими доступ к объектам, а отказоустойчивость обычно сопровождается требованиями аудита безопасности, используемыми для выявления сбоев. Правила управления доступом и особенно правила аудита безопасности являются необходимыми, но обычно не достаточными для реализации требований к характеристикам безопасности.

Требования к архитектуре труднее идентифицировать и определить, чем другие ФТБ. Однако они могут требоваться для полного достижения некоторых целей безопасности, и следовательно, их нужно определить как часть ФТБ в ПЗ или ЗБ.

12.2.7.2 Использование

Идентификация и моделирование требований к архитектуре осуществляются посредством выполнения следующих шагов:

- определение целей безопасности, которые не были охвачены либо не были полностью охвачены требованиями, определенными на предыдущих этапах;
- определение поддержки, с точки зрения архитектуры ОО необходимой для достижения этих целей;
- определение правил, которые относятся к поддержке архитектуры.

Настоящий стандарт не предназначен для использования в качестве руководства по выбору требований к архитектуре ОО. Для ЗБ эти требования, вероятнее всего, предопределяются архитектурой ОО, рассматриваемого в ЗБ. Например, если известно, что ОО является распределенным, то для достижения сформулированных целей безопасности может возникнуть необходимость в требованиях к поддержке согласованности данных в распределенных частях ОО или требованиях к защите данных от несанкционированного доступа при их передаче между распределенными частями ОО. Хотя можно утверждать, что поддержка внутренних функций ФБО в рамках ОО будет избыточной до тех пор, пока ОО выполняет цели безопасности на уровне ИФБО, определение обязательных внутренних функций, которые поддерживают достижение целей безопасности, помогает понимать и анализировать ОО в ходе оценки.

12.3 Спецификация функциональных требований безопасности в профиле защиты или задании по безопасности

12.3.1 Выбор функциональных требований безопасности

Определив цели безопасности для ОО в рамках определения проблемы безопасности, необходимо уточнить, как эти цели безопасности будут достигаться. Для этого осуществляется спецификация ФТБ, например, путем выбора подходящей совокупности ФТБ, выполняемого на уровне компонентов. При этом процесс выбора ФТБ значительно упрощается, если используются предопределенные функциональные пакеты, соответствующие конкретным целям безопасности для ОО.

Функциональные требования безопасности выбираются на основе модели общих функциональных возможностей ОО. В этой функциональной модели определяются ресурсы, пользователи, субъекты, объекты и операции. Затем ФТБ определяют функциональные возможности безопасности таким образом, чтобы в рамках функциональной модели ОО достигались цели безопасности. Как и любая модель, эта модель является абстрактным представлением реальных функциональных возможностей ОО, но уровень абстракции должен быть достаточным для понимания основных функций ОО. Ресурсы, пользователи, субъекты, объекты и операции, которые нет необходимости контролировать для достижения целей безопасности при определении функциональных требований безопасности, могут не включаться в рассмотрение. Например, если единственная цель безопасности для ОО состоит в управлении доступом к данным, то при определении ФТБ может не возникнуть необходимости в рассмотрении ресурса «процессорное время».

В процессе формирования ФТБ для включения в ПЗ или ЗБ выделяются несколько стадий.

В целях рассмотрения в процессе выбора целесообразно различать следующие два типа ФТБ:

а) основные ФТБ, непосредственно удовлетворяющие конкретным целям безопасности для ОО;

б) поддерживающие ФТБ, не предназначенные для непосредственного удовлетворения целей безопасности для ОО, но способствующие выполнению основных ФТБ и тем самым косвенным образом способствующие удовлетворению целей безопасности для ОО.

Хотя в ГОСТ Р ИСО/МЭК 15408 не разделяются явным образом ФТБ на основные и поддерживающие, такое деление подразумевается при рассмотрении таких вопросов, как зависимость между функциональными компонентами и демонстрация взаимной поддержки функциональных требований безопасности. Таким образом, хотя нет необходимости в явном разделении функциональных требований безопасности в ПЗ или ЗБ на основные или поддерживающие, признание наличия этих двух типов ФТБ может оказаться полезным при формировании раздела «Обоснование» в ПЗ или ЗБ. Первой стадией в процессе выбора ФТБ, соответствующих конкретным целям безопасности для ОО, является идентификация для функциональной модели ОО основных ФТБ, непосредственно удовлетворяющих данным целям безопасности. После формирования полной совокупности основных ФТБ начинается итерационный процесс формирования полной совокупности поддерживающих ФТБ. Как упоминалось выше, все ФТБ (и основные, и поддерживающие) целесообразно, когда это возможно, формировать на основе функциональных компонентов, определенных в ГОСТ Р ИСО/МЭК 15408-2. В 12.3.2 представлены

рекомендации по идентификации функциональных компонентов, которые должны использоваться для отражения общих функциональных требований безопасности. При выборе функциональных компонентов, определенных в ГОСТ Р ИСО/МЭК 15408, целесообразно учитывать рекомендации, содержащиеся в приложениях к ГОСТ Р ИСО/МЭК 15408-2 и связанные с интерпретацией данных компонентов.

Взаимосвязь между основными и поддерживающими ФТБ показана на рисунке 4. Данная взаимосвязь учитывается при формировании обоснования в ПЗ или ЗБ, в котором требуется показать взаимную поддержку ФТБ. При этом требуется раскрыть характер поддержки, выполняемой поддерживающими ФТБ для достижения целей безопасности ОО.

Рисунок 4 — Взаимосвязь основных и дополнительных ФТБ

Формирование полной совокупности поддерживающих ФТБ включает следующие стадии:

а) идентификация дополнительных ФТБ, необходимых (с точки зрения разработчика ПЗ) для удовлетворения зависимостей (определенных в ГОСТ Р ИСО/МЭК 15408-2 для соответствующих функциональных компонентов) всех основных ФТБ, в том числе всех зависимостей от поддерживающих ФТБ, идентифицированных на этой стадии;

б) идентификация любых дополнительных ФТБ, необходимых для достижения целей безопасности для ОО, включая ФТБ, необходимые для защиты основных ФТБ от многоходовых атак (многоходовые атаки направлены на преодоление защитных механизмов, реализующих определенную функцию безопасности, затем — на реализацию угрозы, для противостояния которой данная функция безопасности предназначена);

в) идентификация дополнительных ФТБ, необходимых (с точки зрения разработчика ПЗ) для удовлетворения зависимостей тех поддерживающих ФТБ, которые были выбраны на предыдущих стадиях.

Идентификация поддерживающих ФТБ согласно ГОСТ Р ИСО/МЭК 15408-2 представляет собой итерационный процесс, например:

а) предположим, что в ПЗ или ЗБ включена цель безопасности, требующая, чтобы ОО определенным образом реагировал на события, являющиеся показателем нарушения безопасности. Наличие в ПЗ подобной цели предполагает идентификацию основных ФТБ на базе компонента FAU_ARP.1 «Сигналы нарушения безопасности»;

б) согласно ГОСТ Р ИСО/МЭК 15408-2 компонент FAU_ARP.1 имеет зависимость от компонента FAU_SAA.1 «Анализ потенциальных нарушений», который также должен быть включен в ПЗ или ЗБ в качестве поддерживающего ФТБ;

в) компонент FAU_SAA.1 имеет зависимость от FAU_GEN.1 «Генерация данных аудита»;

г) компонент FAU_GEN.1 имеет зависимость от FPT_STM.1 «Надежные метки времени»;

д) компонент FPT_STM.1 не требует ввода дополнительных функциональных компонентов.

Некоторые зависимости могут быть оставлены неудовлетворенными. При этом необходимо пояснить, почему соответствующие ФТБ не требуются для достижения целей безопасности.

При удовлетворении зависимостей необходимо обеспечить согласованность соответствующих компонентов. Например, в случае FAU_ARP.1 согласованность достигается характером требований (FAU_ARP.1 зависит от ожидания в отношении потенциального нарушения безопасности, которое определено применением FAU_SAA.1.2).

Для других компонентов добиться согласованности может быть проблематично. Например, при включении в ПЗ компонента FDP_ACC.1 одновременно идентифицируется конкретная ПФБ управления доступом. При удовлетворении зависимости FDP_ACC.1 от компонента FDP_ACF.1 необходимо обеспечить применение FDP_ACF.1 к той же политике управления доступом, которая идентифицировалась при включении в ПЗ компонента FDP_ACC.1. Если к компоненту FDP_ACC.1 применяется операция «итерация» для различных политик управления доступом, то зависимость от компонента FDP_ACF.1 должна быть удовлетворена несколько раз, принимая во внимание каждую политику управления доступом.

Идентификация дополнительных поддерживающих ФТБ (то есть тех, которые не требуются для удовлетворения зависимостей) включает в себя идентификацию любых других ФТБ, которые считаются необходимыми для содействия достижению целей безопасности для ОО. Такие ФТБ должны способствовать достижению целей безопасности для ОО путем сокращения доступных нарушителю возможностей для атак. Кроме того, реализация дополнительных поддерживающих ФТБ может потребовать от нарушителя более высокого уровня подготовки и значительных ресурсов для проведения результативной атаки. В качестве дополнительных ФТБ могут выступать следующие:

а) ФТБ, основанные на соответствующих компонентах из того же класса, что и основные ФТБ. Например, если компонент FAU_GEN.1 «Генерация данных аудита» включен в ПЗ, то может возникнуть потребность в создании и ведении журнала аудита безопасности для хранения сгенерированных данных (для формулирования подобных требований необходим один или более функциональных компонентов из семейства FAU_STG), а также в наличии средств просмотра сгенерированных данных аудита (для формулирования подобных требований необходим один или более функциональных компонентов из семейства FAU_SAR). В качестве альтернативы включению поддерживающих ФТБ сгенерированные данные аудита безопасности могут быть экспортированы для просмотра в другую систему.

б) ФТБ, основанные на соответствующих компонентах класса FPT «Защита функциональных возможностей безопасности ОО». Такие ФТБ обычно направлены на защиту целостности и (или) доступности ФБО или данных ФБО, на которые полагаются другие ФТБ. Например, для защиты ФБО от нарушений и модификации в ПЗ могут быть включены ФТБ на основе компонента FPT_TEE.1 «Тестирование внешних сущностей» и компонентов семейства FPT_PHP «Физическая защита ФБО».

в) ФТБ, основанные на соответствующих компонентах класса FMT «Управление безопасностью». Эти компоненты могут использоваться для спецификации поддерживающих ФТБ управления безопасностью. Так, например, в ПЗ может быть включено поддерживающее ФТБ на базе компонента FMT_REV.1, связанное с отменой атрибутов безопасности, если в ПЗ включено ФТБ, связанное с атрибутами безопасности (например, атрибутами управления доступом).

Выбор поддерживающих ФТБ должен всегда осуществляться в соответствии с целями безопасности и функциональной моделью, чтобы сформировать целостный набор взаимно поддерживающих ФТБ. Таким образом, на выбор поддерживающих ФТБ существенное влияние может оказывать процесс построения подраздела ПЗ «Обоснование». Необходимо избегать включения в ПЗ поддерживающих ФТБ, которые не направлены на достижение целей безопасности, так как включение подобных ФТБ приведет к ограничению сферы применения ПЗ вследствие следующих обстоятельств:

а) некоторые ОО могут быть не способны удовлетворить избыточные поддерживающие ФТБ;

б) увеличение числа ФТБ увеличивает стоимость оценки.

Если ПЗ создается на основе другого (базового) ПЗ, то процесс выбора ФТБ значительно упрощается. Однако в новый ПЗ должны быть включены (при необходимости) ФТБ, отличные от ФТБ базового ПЗ, для учета любых различий в определении проблемы безопасности для ОО и (или) в целях безопасности в разрабатываемом и базовом профилях защиты.

12.3.2 Выбор функциональных требований безопасности из ГОСТ Р ИСО/МЭК 15408-2

В приведенных ниже таблицах 2—7 представлено прослеживание между рассмотренными парадигмами и компонентами ФТБ, определенными в ГОСТ Р ИСО/МЭК 15408-2. Некоторые компоненты охватывают более одного аспекта парадигмы и поэтому приводятся в таблицах несколько раз.

Таблица 2 — Управление доступом

Требование	Применимые компоненты
Определение субъектов, объектов, операций	FDP_ACC.1, FDP_ACC.2, FDP_IFC.1, FDP_IFC.2, FMT_SMF.1
Определение атрибутов безопасности	FDP_DAU.1, FDP_DAU.2, FDP_IFF.1, FDP_IFF.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2

Окончание таблицы 2

Требование	Применимые компоненты
Создание субъектов, объектов	FDP_ITC.1, FDP_ITC.2, FMT_SMF.1
Экспортирование объектов	FDP_ETC.1, FDP_ETC.2
Управление атрибутами безопасности	FDP_ITC.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FTA_LSA.1
Определение правил доступа	FDP_ACF.1, FDP_IFF.1, FDP_IFF.2, FDP_ROL.1, FDP_ROL.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2
Управление правилами управления доступом	FMT_MOF.1, FMT_SMF.1

Таблица 3 — Управление пользователями

Требование	Применимые компоненты
Определение типов пользователей	FMT_SMF.1
Определение атрибутов безопасности	FIA_ATD.1
Правила идентификации пользователей	FIA_UID.1, FIA_UID.2
Правила аутентификации пользователей	FIA_AFL.1, FIA_SOS.1, FIA_SOS.2, FIA_UAU.1, FIA_UAU.2, FIA_UAU.3, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7
Управление учетными данными и атрибутами безопасности пользователей	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3, FTA_LSA.1, FTA_MCS.1, FTA_MCS.2
Управление правилами идентификации и аутентификации	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1
Управление связями пользователь — субъект	FIA_USB.1

Таблица 4 — Собственная защита ОО

Требование	Применимые компоненты
Обнаружение неисправности	FPT_TEE.1, FPT_ITI.2, FPT_ITT.3, FPT_PHP.1, FPT_PHP.2, FPT_PHP.3, FPT_RPL.1, FPT_TST.1, FRU_FLT.1, FRU_FLT.2
Реагирование на неисправность	FPT_ITT 3, FPT_PHP 2, FPT_PHP.3, FPT_RCV.1, FPT_RCV.2, FPT_RCV.3, FPT_RCV.4, FPT_RPL.1, FRU _FLT.1, FRU_FLT.2
Управление правилами обнаружения и реагирования	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1

Таблица 5 — Защита каналов связи

Требование	Применимые компоненты
Установление канала связи	FMT_SMF.1, FTP_ITC.1, FTP_TRP.1
Определение свойств канала связи (атрибутов безопасности)	FCO_NRO.1, FCO_NRO.2, FCO_NRR.1, FCO_NRR.2, FDP_UTC.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FPT_ITC.1, FPT_ITI.1, FPT_ITI.2, FPT_RPL.1, FTP_ITC 1, FTP_TRP.1
Управление свойствами канала связи	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1
Управление правилами установления связи	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1, FTA_TAH.1, FTA_TSE.1

Таблица 6 — Аудит

Требование	Применимые компоненты
Определение событий, подлежащих аудиту	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1
Определение реагирования на события	FAU_ARP.1, FAU_SAA.1, FAU_SAA.2, FAU_SAA.3, FAU_SAA.4
Определение управления событиями	FAU_SAR.1, FAU_SAR.2, FAU_SAR.3
Определение управления журналом аудита	FAU_STG.1
Управление правилами аудита	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3

Таблица 7 — Требования к архитектуре

Требование	Применимые компоненты
Защита журнала аудита	FAU_STG.2, FAU_STG.3, FAU_STG.4
Управление информационными потоками	FDP_IFF.3, FDP_IFF.4, FDP_IFF.5, FDP_IFF.6
Передача данных внутри ОО	FDP_ITT.1, FDP_ITT.2, FDP_ITT.3, FDP_ITT.4
Защита остаточной информации	FDP_RIP.1, FDP_RIP.2
Целостность хранимых данных	FDP_SDI.1, FDP_SDI.2
Управление	FMT_MTD.1
Защита конфиденциальности	FPR_ANO.1, FPR_ANO.2, FPR_PSE.1, FPR_PSE.2, FPR_PSE.3, FPR_UNL.1, FPR_UNO.1, FPR_UNO.2, FPR_UNO.3, FPR_UNO.4
Сбой безопасности	FPT_FLS.1
Доступность	FPT_ITA.1, FPT_ITT.1, FPT_ITT.2
Синхронизация состояния	FPT_SSP.1, FPT_SSP.2
Надежные метки времени	FPT_STM.1
Непротиворечивость данных	FPT_TDC.1, FPT_TRC.1

Приведенные таблицы призваны помочь в идентификации подходящих ФТБ, если функциональная модель безопасности определена в соответствии с рекомендациями 12.2 и 12.3.1. На усмотрение разработчика ПЗ или ЗБ остаются выбор компонента и изложение аспектов функциональной модели безопасности с использованием компонента и разрешенных операций.

Для архитектурных требований предоставляется перечень возможных архитектурных вопросов, прослеженный к компонентам ФТБ из ГОСТ Р ИСО/МЭК 15408-2, связанным с этими вопросами.

12.3.3 Выполнение операций над функциональными требованиями безопасности

12.3.3.1 Разрешенные операции

Как было изложено выше, над функциональными компонентами могут быть выполнены разрешенные операции. Выполняя операции над функциональными компонентами, разработчик ПЗ может сформировать соответствующее данному ПЗ требование безопасности. Допустимыми операциями являются:

а) назначение — позволяет специфицировать идентифицированный параметр (результат спецификации может быть в том числе и «пустым» значением);

б) итерация — позволяет несколько раз использовать функциональный компонент с различным выполнением операций для определения различных требований;

в) выбор — позволяет специфицировать один или несколько элементов из списка;

г) уточнение — позволяет добавить детали к требованиям безопасности, ограничивая таким образом возможную совокупность приемлемых решений без необходимости введения новых зависимостей от других ФТБ.

12.3.3.2 Операция «итерация»

Операция «итерация» часто используется для определения ФТБ на основе компонентов класса FMT («Управление безопасности»), которые включаются в ПЗ для удовлетворения зависимостей многих других функциональных компонентов. Для того чтобы удовлетворить такие зависимости, обычно необходимо использовать компоненты класса FMT, над которыми операции «назначение» и «выбор» выполняют по-разному. Например, компонент FMT_MSA.1 может быть использован многократно для определения отдельных ФТБ, соответствующих управлению различными типами атрибутов безопасности. Аналогично может потребоваться неоднократное использование компонентов семейств FDP_ACC и FDP_ACF в тех случаях, когда требуется, чтобы ОО реализовывал различные политики управления доступом, например, дискреционную и ролевую.

Целесообразно использовать операцию «итерация» для улучшения читабельности ПЗ, например, для того чтобы разбить сложное и громоздкое ФТБ на отдельные понятные ФТБ. Использование операции «итерация» тем не менее может породить другие потенциальные проблемы при представлении ФТБ в ПЗ или ЗБ.

12.3.3.3 Операции «назначение» и «выбор»

Существует возможность, когда результат выполнения операции «назначение» может быть пустым, в то время как для операции «выбор» идентифицируется по крайней мере одно значение параметра. Выполнение (завершение) операций «назначение» и «выбор» не оставляется возможности разработчику ЗБ конкретизации (кроме «уточнения») функционального компонента для удовлетворения целей безопасности. Другими словами, исключаются аспекты (так как операция выполнена), которые подлежат определению разработчиком ЗБ.

Отдельные операции «назначение» и «выбор» потребуют завершения автором ЗБ. Чрезмерное ограничение в ПЗ путем завершения операций или слишком подробная детализация могут необоснованно ограничить количество ОО, для которых могло бы быть заявлено соответствие ПЗ.

Баланс выполнения (завершения) операций основывается на том, что ПЗ должен:

а) представлять собой полный набор требований;

б) быть независимым от реализации;

в) быть достаточно детализированным, чтобы демонстрировать удовлетворение целей безопасности.

Следовательно, операции «назначение» и «выбор» целесообразно выполнять, исходя из необходимости демонстрации достижения целей безопасности. Важным тестом правильности выполнения операции над компонентом является процесс формирования «Обоснования требований безопасности ИТ»: аргументы, используемые для демонстрации пригодности требований безопасности ИТ для удовлетворения целей безопасности, не должны опираться на детали, которые не были специфицированы в ФТБ. Например, для ФТБ управления доступом, основанного на компоненте FDP_ACF.1, спецификацию правил управления доступом можно возложить на разработчика ЗБ в том случае, если такие правила уже определены в ПБОр, для удовлетворения которой предназначена соответствующая (управлению доступом) цель безопасности. В этом случае разработчик ПЗ должен завершить операции «назначение» и «выбор» лишь в той степени, в какой это требуется для удовлетворения общей цели безопасности, оставляя достаточную степень свободы разработчику ЗБ, для которого утверждается о соответствии некоторому ПЗ, в вопросе определения специфических правил доступа, реализованных в ОО.

Один из рекомендуемых подходов к решению упомянутой выше проблемы — частичное выполнение операций. Следуя данному подходу, можно оставить разработчику ЗБ максимальную свободу действий и вместе с тем предотвратить такое выполнение операций «назначение» и «выбор», которое несовместимо с целями безопасности для ОО.

Например, в нижеследующем ФТБ (основанном на FAU_STG.4.1) операция «выбор» выполнена частично путем предотвращения выбора варианта «игнорирование подвергаемых аудиту событий», который разработчик считает несовместимым с целями безопасности для ОО. Таким образом, ФТБ предоставляет разработчику ЗБ два (а не три) варианта выбора:

«ФБО должны выполнить *предотвращение событий, подвергающихся аудиту, исключая предпринимаемые уполномоченным пользователем со специальными правами, запись поверх самых старых хранимых записей аудита* и [назначение: другие действия, которые нужно предпринять в случае возможного сбоя хранения журнала аудита] при переполнении журнала аудита».

Используя операцию «назначение», разработчик ПЗ может пожелать ограничить выбор для автора ЗБ набором вариантов, приемлемых для среды функционирования. В этом случае разработчик ПЗ может пожелать выполнить операцию «назначение» путем превращения ее в операцию «выбор» из приемлемых вариантов, которая, в свою очередь, может быть выполнена автором ЗБ.

Общий принцип — частичное выполнение операции «выбор» является допустимым, если результирующее ФТБ представляет подмножество вариантов выбора, которые являются разрешенными для исходного функционального компонента. Аналогично частичное выполнение операции «назначение» является допустимым, если допустимые значения выполнения операции «назначение» над ФТБ являются допустимыми и для исходного функционального компонента. Если по какой-либо причине эти условия не выполняются, то необходимо использовать расширенный функциональный компонент с другими операциями «назначение» и «выбор».

Выполнение операций «назначение» и «выбор» должно быть прямым. То есть при выполнении операции «назначение» необходимо обеспечить, чтобы специфицируемый параметр был бы однозначным (точно выраженным). При выполнении операции «выбор» необходимо выбрать вариант (варианты) из списка с учетом целей безопасности для ОО.

Например, требование на основе элемента FMT_SAE.1.1 могло быть представлено следующим образом:

«ФБО должны ограничить возможность назначать срок действия для [паролей пользователя] только [уполномоченным администратором].

Ниже приведен пример выполнения операции «выбор» в утвержденном ФСТЭК России профиле защиты.

Фрагмент исходного компонента:

«FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на [выбор (выбрать одно из): минимальный, базовый, детализированный, неопределенный] уровне аудита».

Фрагмент компонента с выполненной операцией «выбор»:

«FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на *базовом* уровне аудита;

...».

Если операция остается невыполненной, то целесообразно пояснить, что выполнение операции возлагается на разработчика ЗБ. Например, требование на основе элемента FDP_RIP.1.1 могло бы быть специфицировано в ПЗ следующим образом:

«ФБО должны обеспечить недоступность любого предыдущего информационного содержания ресурсов при *распределении ресурса* для следующих объектов: [назначение: список специфицируемых разработчиком ЗБ объектов]».

Невыполненные (либо выполненные частично) операции целесообразно, где необходимо, сопровождать рекомендациями разработчику ЗБ о том, каким образом следует выполнять операции (например, в виде замечаний по применению).

Ниже приведен пример замечаний по применению из утвержденного ФСТЭК России профиля защиты:

«FAU_ARP.1 Сигналы нарушения безопасности

FAU_ARP.1.1 ФБО должны предпринять [информирование администратора СКН], [назначение: *список других действий*] при обнаружении возможного нарушения безопасности.

Зависимости: FAU_SAA.1 Анализ потенциального нарушения.

Замечания по применению: разработчик ЗБ, кроме информирования администратора СКН, может перечислить и другие действия при обнаружении возможного нарушения безопасности. В этом случае разработчику ЗБ необходимо будет четко определить содержание, последовательность и результаты таких действий».

Для каждого ФТБ, включенного разработчиком в ПЗ, необходимо привести логическое обоснование относительно завершения любой операции «назначение» или «выбор» в функциональном компоненте, используемом для выражения ФТБ. В ЗБ все операции «назначение» и «выбор» должны быть завершены.

12.3.3.4 Операция «уточнение»

Для каждого ФТБ, включаемого в ПЗ или ЗБ, необходимо принять решение о том, нуждается ли оно в каком-либо уточнении.

Операция «уточнение» может быть выполнена над любым элементом любого функционального компонента и заключается в добавлении некоторых технических деталей, которые не налагают новых требований к определенным в тексте, но ограничивают набор допустимых реализаций.

Считается, что операция «уточнение» выполнена допустимым образом, если выполнение уточненного требования приводит к выполнению неуточненного требования.

Использование операции «уточнение» может быть подходящим в следующих случаях:

а) когда ПЗ разрабатывается организацией, которая имеет дополнительные технические детали, такие как информация, относящаяся к политике организации, отсутствующая в компоненте ГОСТ Р ИСО/МЭК 15408-2;

б) когда выбранный функциональный компонент допускал бы реализацию, которая бы не имела смысла или даже была бы неприемлемой для рассматриваемого типа ОО, пока эта возможность не была исключена выполнением операции «уточнение»;

в) когда может быть улучшен стиль изложения ФТБ.

Как и случае с операциями «назначение» и «выбор», рекомендуется выделить текст, который был уточнен, чтобы помочь пользователю документа (и в особенности оценщику ПЗ).

Далее приводится пример выполнения операции «уточнение» применительно к требованию на основе элемента FMT_MTD.3.1:

«ФБО должны обеспечить присвоение данным ФБО только безопасных значений.

Уточнение: ФБО должны обеспечить, **чтобы минимальная длина пароля, требуемого ОО, была по крайней мере шесть символов**».

12.3.3.5 Выделение результатов выполнения операций

В целях унификации выделения результатов выполнения операций над компонентами требований безопасности рекомендуется в ПЗ или ЗБ включать подраздел (или пункт), устанавливающий соглашения о стилях выделения результатов операций.

Ниже представлен фрагмент такого подраздела на примере подраздела «Соглашения» профилей защиты, утвержденных ФСТЭК России.

«ГОСТ Р ИСО/МЭК 15408 допускает выполнение определенных операций над компонентами требований безопасности. Соответственно в настоящем ПЗ используются операции «уточнение», «выбор», «назначение» и «итерация».

Операция «уточнение» используется для добавления в компонент требований безопасности некоторых подробностей (деталей) и таким образом ограничивает диапазон возможностей его удовлетворения. Результат операции «уточнение» в настоящем ПЗ обозначается **полужирным текстом**.

Операция «выбор» используется для выбора одного или нескольких элементов из перечня в формулировке компонента требования. Результат операции «выбор» в настоящем ПЗ обозначается *подчеркнутым курсивным текстом*.

Операция «назначение» используется для присвоения конкретного значения ранее неконкретизированному параметру. Операция «назначение» обозначается заключением значения параметра в квадратные скобки — [назначаемое значение].

Операция «итерация» используется для более чем однократного использования компонента требований безопасности при различном выполнении разрешенных операций (уточнение, выбор, назначение). Выполнение «итерации» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента — (номер итерации).

Настоящий профиль защиты содержит ряд незавершенных операций над компонентами функциональных требований безопасности. Эти операции должны быть завершены в задании по безопасности для конкретной реализации СКН».

12.3.4 Спецификация требований аудита

Если в ПЗ включены требования аудита (основанные на компоненте FAU_GEN.1), то при формировании всех остальных включаемых в ПЗ функциональных требований необходимо специфицировать минимальный набор подлежащих аудиту событий и минимальный объем подлежащей аудиту информации.

Выбор подлежащих аудиту событий и подлежащей аудиту информации зависит от следующих основных факторов:

а) определенные в ПБОр требования к аудиту безопасности;

б) значимость аудита безопасности для достижения целей безопасности;

в) значимость некоторых событий и их характеристик для целей безопасности;

г) анализ «стоимость — эффективность».

Например, если ОО предназначен для защиты от негативных действий нарушителей, то аудиту должны подлежать события, связанные с нарушением политики управления доступом. При этом в состав событий, подлежащих аудиту, можно не включать события, связанные с администрированием ОО со стороны администратора. Множество таких событий зависит от доверия к администратору, которое при этом должно быть изложено в виде предположения.

При проведении анализа «стоимость — эффективность» должны быть рассмотрены следующие вопросы:

а) является ли регистрируемая информация полезной для ее последующего анализа;

б) имеются ли у администратора необходимые ресурсы (например, инструментальные средства поддержки) для эффективного анализа собранной информации;

в) каковы предполагаемые затраты на хранение и обработку собираемых данных.

В ГОСТ Р ИСО/МЭК 15408 введены три предопределенных уровня аудита: минимальный, базовый и детализированный. Для каждого предопределенного уровня в ГОСТ Р ИСО/МЭК 15408-2 определен минимальный набор подлежащих аудиту событий, а также минимальный объем подлежащей регистрации информации с привязкой к функциональным компонентам.

Предопределенные уровни аудита могут быть охарактеризованы следующим образом:

а) минимальный уровень аудита требует, чтобы аудиту подвергалось только определенное подмножество действий или событий, связанных с данным функциональным компонентом (подвергаемые аудиту события — это обычно наиболее значимые события);

б) базовый уровень аудита требует, чтобы аудиту подвергались все действия или события, связанные с данным функциональным компонентом (например, как успешные, так и неуспешные попытки доступа к ОО);

в) детализированный уровень аудита отличается от базового наличием требований к регистрации дополнительной информации. Детализированный уровень аудита необходим в тех случаях, когда объема генерируемых данных аудита недостаточно или когда анализ данных аудита предполагается проводить с использованием специальных средств анализа или средств обнаружения вторжений.

В ПЗ, утвержденных ФСТЭК России, уровень аудита, определяемый в FAU_GEN.1, устанавливается в зависимости от класса защиты средства защиты информации. Например, для четвертого класса защиты применяется базовый уровень аудита.

Если ни один из перечисленных уровней аудита не является подходящим для конкретного случая, то целесообразно выбрать неопределенный уровень аудита и в явном виде перечислить все подлежащие аудиту события в элементе FAU_GEN.1.1. Например, можно принять за основу минимальный уровень аудита, но в ряде случаев отклоняться от минимальных требований вследствие того, что какое-либо подмножество действий или событий является более значимым для достижения целей безопасности. Например, если в ПЗ включен компонент FDP_ACF.1, то может потребоваться более детальный аудит неуспешных попыток доступа по сравнению с успешными.

Чтобы сформировать список событий, подлежащих аудиту, необходимо проанализировать каждый используемый в ПЗ функциональный компонент. Если же назначен один из предопределенных уровней аудита (минимальный, базовый или детализированный), то подлежащие аудиту события в явном виде идентифицируются в подразделе «Аудит», приводящемся для каждого семейства компонентов. Рекомендуется составить таблицу, в которой представлены события и (при необходимости) дополнительная подлежащая регистрации информация.

12.3.5 Спецификация требований управления

В подразделе «Управление» для каждого семейства (см. ГОСТ Р ИСО/МЭК 15408-2) определен список действий управления применительно к компонентам данного семейства. Наличие списка действий управления может предполагать включение в ПЗ отдельных компонентов из класса FMT «Управление безопасностью». Подраздел «Управление» определен в ГОСТ Р ИСО/МЭК 15408 в качестве информативного, и поэтому обосновывать отсутствие в ПЗ тех или иных компонентов управления нет необходимости (если, конечно, данные компоненты управления не идентифицированы в подразделе «Зависимости»).

Таким образом, возможные действия управления специфицируются тогда, когда функциональные компоненты ссылаются на настраиваемые данные ФБО, которые подлежат управлению и контролю. Например, цели безопасности для ОО могут быть не достигнуты в том случае, если не реализованы ограничения на внесение изменений в ФБО администраторами ОО. Поэтому компоненты класса FMT часто включаются в ПЗ для разработки на их основе поддерживающих ФТБ, способствующих достижению целей безопасности для ОО, и для того, чтобы ФТБ в целом являлись взаимно поддерживающими.

Действия по управлению могут быть получены на основе функциональной модели ОО. Типичными действиями по управлению, подлежащими рассмотрению, являются:

- регистрация или отмена регистрации пользователей;
- создание объектов;
- изменение атрибутов безопасности пользователей, объектов, сеансов и т. д.
- изменение в поведении ФБО (включая запуск или остановку всех или некоторых функций ОО);
- изменение параметров аудита;
- изменение переменных внутреннего состояния ФБО, имеющих отношение к безопасности (например, изменения режима функционирования на техническое обслуживание).

При выборе компонентов из класса FMT следует применять рекомендации, приведенные в ГОСТ Р ИСО/МЭК 15408-2 (приложение Н).

12.3.6 Спецификация функциональных требований, приведенных в профиле защиты

Если в ЗБ заявлено соответствие одному или нескольким ПЗ, то, вероятно, ФТБ уже специфицированы в ПЗ. В таких случаях необходимо принять решение — специфицировать ФТБ в ЗБ полностью (для того чтобы весь текст был в одном месте) либо включить в ЗБ ссылку на ФТБ, специфицированные в ПЗ, и специфицировать либо те ФТБ, которых нет в ПЗ, либо те, которые отличаются от специфицированных в ПЗ.

Последний подход упрощает ЗБ, но от пользователя ЗБ при этом потребуется изучить и ПЗ, и ЗБ для получения полного представления. Пользователей ЗБ больше интересуют функциональные возможности безопасности ИТ, чем ФТБ. Это же относится и к оценщику ОО (так как содержание свидетельств оценки — проектной, тестовой документации, руководств — в краткой спецификации ОО проще привязать к функциям безопасности ИТ, чем к ФТБ). Основная цель спецификации ФТБ в ЗБ — продемонстрировать соответствие ФТБ ЗБ функциональным требованиям соответствующих ПЗ и функциональным требованиям, определенным в ГОСТ Р ИСО/МЭК 15408-2. В некоторых случаях описание ФТБ помещают в приложении с тем, чтобы не вводить пользователя ЗБ в заблуждение наличием в ЗБ двух функциональных спецификаций безопасности.

Тем не менее необходимо отметить, что некоторые ФТБ в ПЗ могут иметь незавершенные операции («назначение», «выбор»), которые должен выполнить разработчик ЗБ. В этом случае необходимо, чтобы ФТБ были полностью специфицированы, операции полностью завершены, а их результат — выделен. Все необходимые пояснения должны быть также выделены. Такой подход облегчает пользователю ЗБ (и оценщику ЗБ в частности) понимание, какие операции и каким образом были выполнены, а также облегчает формирование раздела «Обоснование ЗБ».

12.3.7 Спецификация функциональных требований, отсутствующих в профиле защиты

В некоторых случаях необходимо специфицировать ФТБ, которые отсутствуют в соответствующем ПЗ. Это может быть, когда:

а) для ОО отсутствует подходящий ПЗ, соответствие которому может быть заявлено в ЗБ;

б) спонсор (заказчик) считает, что преимущества от включения требования дополнительной по отношению к ПЗ функциональности оправдывают дополнительные расходы на оценку.

В этих случаях целесообразно использовать подход к спецификации ФТБ, аналогичный подходу, описанному в предыдущем разделе. Если в ЗБ включаются дополнительные по отношению к ПЗ требования, то необходимо обеспечить отсутствие противоречия между ними и ФТБ, включенными в ПЗ (в разделе ЗБ «Обоснование» необходимо продемонстрировать отсутствие противоречия).

12.3.8 Спецификация в профиле защиты функциональных требований, не изложенных в ГОСТ Р ИСО/МЭК 15408-2

Если при разработке ПЗ требуется включить в документ функциональное требование, для которого в ГОСТ Р ИСО/МЭК 15408 отсутствует соответствующий функциональный компонент, то в качестве формы представления рассматриваемого ФТБ необходимо использовать форму представления функциональных компонентов в ГОСТ Р ИСО/МЭК 15408.

Принятие решения о наличии либо отсутствии соответствующего функционального компонента в ГОСТ Р ИСО/МЭК 15408-2 может оказаться сложным, так как предполагает хорошее знание ГОСТ Р ИСО/МЭК 15408. С учетом этого рекомендуется использовать положения 12.3.2, где идентифицируются функциональные компоненты ГОСТ Р ИСО/МЭК 15408-2 для выражения основным функциональным требованиям безопасности. В большинстве случаев ФТБ может быть получено путем соответствующего использования операций «уточнение», «назначение» и «выбор», однако не рекомендуется формулировать ФТБ на основе конкретного функционального компонента, если это сразу не приводит к формированию необходимого ФТБ (например, вводит зависимости, не соответствующие целям безопасности).

В этом случае необходимо применять другой подходящий функциональный компонент или при отсутствии такового формулировать ФТБ в явном виде, используя модель представления функциональных компонентов ГОСТ Р ИСО/МЭК 15408.

Рекомендации по определению расширенных (специальных) компонентов представлены в разделе 11.

12.3.9 Представление функциональных требований безопасности

При формировании перечня ФТБ разработчик ПЗ должен представить их таким образом, чтобы обеспечить наилучшее понимание требований безопасности пользователями и согласование ФТБ с требованиями ГОСТ Р ИСО/МЭК 15408.

В процессе представления ФТБ необходимо учитывать следующие рекомендации.

Во-первых, целесообразно объединить ФТБ в группы и озаглавить данные группы ФТБ, исходя из контекста ПЗ. Заголовки групп ФТБ могут отличаться от заголовков классов, семейств и компонентов, определенных в ГОСТ Р ИСО/МЭК 15408-2.

Во-вторых, значительно повысить читабельность ФТБ можно за счет соответствующего использования операции «уточнение». С помощью операции «уточнение» можно заменить термины более общего характера (например, «атрибуты безопасности») на специфические термины, в большей степени соответствующие конкретному типу ОО или описываемой функциональной возможности безопасности.

Далее приведен пример выполнения операции «уточнение» над элементом FMT_MSA.3.1 функционального компонента FMT_MSA.3 «Инициализация статических атрибутов».

Элемент FMT_MSA.3.1 в ГОСТ Р ИСО/МЭК 15408-2 имеет следующий вид:

«FMT_MSA.3.1. ФБО должны осуществлять [назначение: *ПФБ управления доступом, ПФБ управления информационными потоками*], чтобы обеспечить [выбор: *ограничительные, разрешающие, с другими свойствами*] значения по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ».

После выполнения операций «назначение», «выбор» и «уточнение», соответствующих элементу FMT_MSA.3.1, ФТБ принимает следующий вид:

«ФБО должны осуществлять [дискреционную политику управления доступом], чтобы обеспечить ограничительные значения по умолчанию для **разрешений на доступ к объекту».**

В данном примере операция «уточнение» была использована для того, чтобы в формулировке ФТБ заменить выражение более общего характера «атрибуты безопасности, которое используется для осуществления ПФБ» на выражение «разрешение на доступ к объекту», которое в большей степени соответствует специфицированной при выполнении операции «назначение» дискреционной политике управления доступом.

Каждое использование операции «уточнение» должно сопровождаться соответствующим пояснением в разделе ПЗ «Обоснование» в целях облегчения последующей оценки ПЗ.

Реализация описанного подхода к представлению ФТБ проиллюстрирована на примере формирования ПЗ, приведенном в приложении Б настоящего стандарта.

12.3.10 Разработка подраздела «Обоснование требований безопасности»

Если задание по безопасности или профиль защиты не является ЗБ или ПЗ низкого уровня доверия (более подробные сведения об этом приведены в 15.1), то требуется наличие обоснования, в котором разъясняется, каким образом цели безопасности удовлетворяются функциональными требованиями безопасности. В этом обосновании необходимо проследить связь всех целей безопасности с функциональными требованиями безопасности, которые совместно должны способствовать достижению цели, а также необходимо продемонстрировать, что каждое функциональное требование безопасности прослеживается к по крайней мере одной цели безопасности и к каждой цели безопасности прослеживается по крайней мере одно требование безопасности.

В большинстве случаев отдельная цель безопасности будет прослеживаться к более чем одному функциональному требованию безопасности и зачастую одно функциональное требование безопасности будет поддерживать более чем одну цель безопасности. В большинстве ПЗ и ЗБ число функциональных требований безопасности будет превосходить число целей безопасности, так как цели безопасности формулируются в более общем виде, чем функциональные требования безопасности. Например, цель безопасности:

«ОО должен уникально идентифицировать каждого пользователя и выполнять процедуру аутентификации идентифицированного пользователя до предоставления ему доступа к функциональным возможностям ОО» будет, скорее всего, прослеживаться к ряду функциональных требований безопасности, специфицируя:

- каким образом осуществляется идентификация пользователей;

- каким образом осуществляется аутентификация пользователей;
- реакцию в случае неудачной аутентификации;
- каким образом создаются и управляются пользователи и данные аутентификации пользователей;
- каким образом осуществляется связь «пользователь — субъект».

Важнее, чем прослеживание целей безопасности к функциональным требованиям безопасности, является обоснование того, что совокупность функциональных требований безопасности, прослеженных к цели безопасности, в полном объеме удовлетворяют этой цели. В приведенном выше примере это обоснование может быть получено достаточно легко, но это справедливо не для всех целей. Особенно для случая целей безопасности, специфицирующих свойства ОО, обоснование того, что функциональные требования безопасности полностью удовлетворяют цели безопасности, может быть нетривиальным. Например, в случае цели безопасности:

«ОО должен обеспечить, что никакая информация не может поступать от субъекта с определенной меткой безопасности субъекту с более низкой по иерархии меткой безопасности или несовместимой меткой безопасности».

Трудно обосновать, что функциональные требования безопасности, устанавливающие мандатное управление доступом на основе решетки доступа, способствуют достижению цели безопасности в полной мере. Могут быть добавлены дополнительные функциональные требования безопасности, например к архитектуре, которые обеспечат лучшую поддержку для управления информационными потоками, но и при этом может не быть возможности продемонстрировать, что в совокупности функциональные требования безопасности способствуют достижению цели безопасности в полной мере. В приведенном примере даже при правильной реализации всех функциональных требований безопасности могут все же существовать скрытые каналы, позволяющие осуществлять передачу информации способом, противоречащим цели безопасности. Это следует учитывать при обосновании полноты, предоставляемой в части обоснования требований безопасности, и указать, что в рамках модели ОО, обеспечиваемой совокупностью функциональных требований, цель безопасности полностью достигнута, то есть предоставить обоснование отсутствия функциональных требований безопасности, противоречащих цели безопасности.

В общем случае можно сказать, что прослеживание между целями безопасности и функциональными требованиями безопасности, а также обоснование полноты упрощается в том случае, когда цели безопасности излагаются в виде функций, а не свойств, и на уровне детализации, близком к уровню детализации функциональных требований безопасности. Цели безопасности следует, таким образом, формулировать как можно более точно. При разработке ЗБ или ПЗ имеет смысл пересмотреть цели безопасности и попытаться сформулировать их точнее в случае возникновения проблем с прослеживанием целей безопасности к функциональным требованиям безопасности или с обоснованием того, что функциональные требования безопасности способствуют достижению цели безопасности в полной мере.

12.4 Спецификация в ПЗ или ЗБ требований доверия к безопасности

12.4.1 Выбор требований доверия к безопасности

Выбор требований доверия к безопасности зависит от следующих факторов:

а) ценности активов, подлежащих защите, и риска их компрометации;

б) технической реализуемости;

в) стоимости разработки и оценки;

г) требуемого времени для разработки и оценки ОО;

д) требований рынка (для продуктов ИТ);

е) зависимостей функциональных компонентов и компонентов доверия к безопасности.

Чем выше ценность активов, подлежащих защите, и чем больше риск компрометации этих активов, тем выше требуется уровень доверия к безопасности для функциональных возможностей безопасности, используемых для защиты рассматриваемых активов. Эти моменты следует отразить при формировании целей безопасности. Организации могут устанавливать свои собственные правила определения уровня доверия к безопасности, который требуется для снижения риска для этих активов до приемлемого уровня. Это, в свою очередь, определяет требуемый уровень доверия к безопасности продуктов ИТ, которые предполагается использовать в этой организации.

Остальные факторы, такие как стоимость и затраты времени, целесообразно рассматривать как ограничения на уровень доверия к безопасности, который является практически достижимым. Техническая реализуемость рассматривается в том случае, когда считается практически нецелесообразной

подготовка свидетельства (документированного материала), требуемого конкретными компонентами доверия к безопасности. Данная ситуация актуальна для наследуемых систем (в случаях, когда конструкторская документация с достаточным уровнем детализации недоступна), а также в тех случаях, когда в идеале требуется высокий уровень доверия к безопасности, но технически невозможно за приемлемое время подготовить требуемое формальное либо полуформальное свидетельство. В тех случаях, когда имеются ограничения на практически достижимый уровень доверия к безопасности, целесообразно согласиться с тем, что максимально достижимый уровень доверия к безопасности меньше, чем теоретически возможный. Такое восприятие риска должно быть отражено и при изложении целей безопасности.

Изложение целей безопасности может также указывать на то, какие конкретные требования доверия к безопасности должны быть включены в набор ТДБ. Например:

а) цели безопасности для ОО могут устанавливать, что ОО должен быть стойким к нарушителям с высоким потенциалом нападения. Это предполагает четкое указание на включение компонента AVA_VAN.5, который требует демонстрации подобной стойкости;

б) цели безопасности могут требовать рассмотрения вопросов собственной защиты, разделения доменов или невозможности обхода, и в этом случае необходимо включить в ПЗ или ЗБ компонент ADV_ARC.1. В классе ADV имеется только один компонент, но требуемый уровень архитектурного описания зависит от компонента, выбираемого из класса ADV_TDS;

в) при формулировке целей безопасности может быть отмечено, что безопасность ОО серьезно зависит от безопасности среды разработки. В этом случае настоятельно рекомендуется включить в набор ТДБ компонент из семейства ALC_DVS «Безопасность разработки», содержащий требование анализа безопасности среды разработки.

Выбор ТДБ относительно несложен, если требуется просто выбрать подходящий пакет доверия к безопасности, например, ОУД, определенный в ГОСТ Р ИСО/МЭК 15408. Для того чтобы выбрать подходящий с точки зрения сформулированных целей безопасности пакет доверия к безопасности, необходимо изучить его описание (например, при выборе ОУД см. ГОСТ Р ИСО/МЭК 15408-3, раздел 6).

Возможны случаи, когда пакет доверия к безопасности соответствует требуемому уровню доверия, но в нем отсутствуют требования, связанные с некоторыми целями безопасности. В этих случаях целесообразно включать в ТДБ дополнительные (по отношению к пакету) требования доверия к безопасности для того, чтобы учесть все цели безопасности.

Если в ПЗ включены расширенные требования доверия к безопасности, то необходимо удовлетворить все зависимости компонентов доверия к безопасности, содержащих эти дополнительные требования. Например, если в ПЗ пакет ОУД3 усилен путем использования компонента AVA_VAN.3 «Сосредоточенный анализ уязвимостей», то в ПЗ также необходимо включить компоненты ADV_TDS.3 «Базовый модульный проект» и ADV_IMP.1 «Представление реализации ФБО». Кроме того, должен быть включен компонент ADV_FSP.4 «Полная функциональная спецификация», так как ADV_TDS.3 имеет зависимость от ADV_FSP 4.

Если ПЗ или ЗБ разрабатываются для конкретного класса защиты средств защиты информации, установленных соответствующим нормативным правовым актом ФСТЭК России для данного вида средств защиты информации, состав требований доверия определяется на основе этого документа. Типовой состав компонентов доверия в зависимости от класса защиты средств защиты информации приведен в таблице 8.

Таблица 8 — Типовой состав компонентов доверия в зависимости от класса защиты средств защиты информации

Класс защиты средства защиты информации	Требования доверия к безопасности средств защиты информации		Уровень контроля отсутствия недекларированных возможностей
	Оценочный уровень доверия по ГОСТ Р ИСО/МЭК 15408-3	Дополнительные требования доверия к безопасности, определенные на основе ГОСТ Р ИСО/МЭК 15408-3	
4	ОУД3	ADV_FSP.4 «Полная функциональная спецификация» ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности» ADV_TDS.3 «Базовый модульный проект» ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация»	4

Окончание таблицы 8

Класс защиты средства защиты информации	Требования доверия к безопасности средств защиты информации		Уровень контроля отсутствия недекларированных возможностей
	Оценочный уровень доверия по ГОСТ Р ИСО/МЭК 15408-3	Дополнительные требования доверия к безопасности, определенные на основе ГОСТ Р ИСО/МЭК 15408-3	
4	ОУД3	ALC_FLR.1 «Базовое устранение недостатков» ALC_TAT.1 «Полностью определенные инструментальные средства разработки» AVA_VAN.5 «Усиленный методический анализ» ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения средства защиты информации» AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства защиты информации»	4
5	ОУД2	ADV_IMP.2 «Полное отображение представления реализации функциональных возможностей безопасности» ADV_TDS.3 «Базовый модульный проект» ALC_FLR.1 «Базовое устранение недостатков» AVA_VAN.4 «Методический анализ уязвимостей» ALC_TAT_EXT.0 «Определение инструментальных средств разработки» ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения средства защиты информации» AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства защиты информации»	4
6	ОУД1	ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения средства защиты информации» AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность средства защиты информации»	—

Как видно по таблице 8, ТДБ для средств защиты информации определяются на базе предопределенных в ГОСТ Р ИСО/МЭК 15408 наборов требований доверия — оценочных уровней доверия (ОУД). При этом применяется усиление ОУД (включение в набор требований доверия компонентов, не входящих в данный ОУД) и расширение ОУД (включение в набор требований доверия компонентов, не входящих в ГОСТ Р ИСО/МЭК 15408-3, то есть расширенных компонентов). В терминах документов ФСТЭК России расширенные компоненты именуются «специальными».

12.4.2 Выполнение операций над требованиями доверия к безопасности

Возможны следующие операции:

а) «итерация», допускающая многократное использование одного и того же компонента доверия к безопасности;

б) «уточнение», позволяющее детализировать ТДБ;

в) «назначение», позволяющее устанавливать в элементе ТДБ значения указанного параметра.

На практике выполнение операции «итерация» может потребоваться в тех случаях, когда требуются различные «уточнения» для одного и того же компонента доверия к безопасности, используемого для разных частей ОО, либо при определении в ПЗ или ЗБ различных наборов ТДБ для разных компонентов составного ОО (см. 14.1). В последнем случае выполнение операции «итерация» требуется для компонентов доверия к безопасности (уточненных или нет), которые используются для более чем одного компонента составного ОО. Применение операции «уточнение» к ТДБ может быть выполнено в следующих целях:

а) в целях предписания разработчику продукта ИТ использовать конкретные инструментальные средства разработки, методики, модели жизненного цикла, методы анализа, системы обозначений, определенные стандарты и так далее;

б) в целях предписания действий оценщика, например:

1) компонент ADV_IMP.1 определяет, какие части представления реализации ОО должны быть оценены;

2) компонент AVA_VAN.1 определяет минимальную совокупность общедоступных источников уязвимостей, подлежащих анализу, так как в них обычно описаны уязвимости, актуальные в контексте ОО.

Таким образом (с помощью применения операции «уточнение»), в ПЗ, утвержденные ФСТЭК России, интегрированы требования руководящего документа ФСТЭК России по контролю отсутствия недекларированных возможностей (РД НДВ [9]).

Фрагмент требований РД НДВ:

«Контроль исходного состояния ПО

Контроль заключается в фиксации исходного состояния ПО и сравнении полученных результатов с приведенными в документации.

Результатами контроля исходного состояния ПО должны быть рассчитанные уникальные значения контрольных сумм загрузочных модулей и исходных текстов программ, входящих в состав ПО.

Контрольные суммы должны рассчитываться для каждого файла, входящего в состав ПО.

Статический анализ исходных текстов программ

Статический анализ исходных текстов программ должен включать следующие технологические операции:

- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;
- контроля соответствия исходных текстов ПО его объектному (загрузочному) коду».

Исходный компонент доверия:

«ADV_IMP.2 Полное отображение представления реализации ФБО

Зависимости: ADV_TDS.3 Базовый модульный проект;

ALC_TAT.1 Полностью определенные инструментальные средства разработки;

ALC_CMC.5 Расширенная поддержка.

Элементы действий заявителя (разработчика, производителя)

ADV_IMP.2.1D Заявитель (разработчик, производитель) должен обеспечить доступ к представлению реализации для всех ФБО:

для аппаратных средств — на уровне схем аппаратных средств и (или) представления (кода) на языке описания аппаратных средств (в соответствии с национальным стандартом ГОСТ Р 50754 «Язык описания аппаратуры цифровых систем — VHDL» или ином языке описания аппаратных средств);

для программного обеспечения — на уровне исходных текстов всего программного обеспечения, входящего в состав ОО (с указанием в документации значений контрольных сумм файлов с исходными текстами ПО).

ADV_IMP.2.2D Заявитель (разработчик, производитель) должен обеспечить прослеживание всего представления реализации к описанию проекта ОО.

Элементы содержания и представления документированных материалов

ADV_IMP.2.1C Представление реализации должно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дополнительных проектных решений.

ADV_IMP.2.2C Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.

ADV_IMP.2.3C В прослеживании между всем представлением реализации и описанием проекта ОО **(для всех модулей, отнесенных к осуществляющим или поддерживающим выполнение ФТБ)** должно быть продемонстрировано их соответствие, **а для модулей изделия, определенных как «не влияющие на выполнение ФТБ», должно быть предоставлено соответствующее обоснование**.

Элементы действий испытательной лаборатории

ADV_IMP.2.1E Испытательная лаборатория должна подтвердить, что информация, представленная заявителем в документированных материалах, удовлетворяет всем требованиям к содержанию и представлению документированной информации, изложенным в ADV_IMP.2.1C — ADV_IMP.2.3C, **в том числе на основе результатов:**

а) контроля исходного состояния ПО;

б) контроля полноты и отсутствия избыточности исходных текстов на уровне файлов и на уровне функциональных объектов (процедур)».

Кроме того, с помощью применения операции «уточнение» в профилях защиты, утвержденных ФСТЭК России, детализированы требования к реализации функций безопасности среды функционирования ОО:

Фрагменты исходных компонентов:

«AGD_OPE.1 Руководство пользователя по эксплуатации

...

AGD_OPE.1.6C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ.

...

AGD_PRE.1 Подготовительные процедуры

...

AGD_PRE1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

...»

Фрагменты уточненных компонентов доверия:

«AGD_OPE.1 Руководство пользователя по эксплуатации

...

Элементы содержания и представления свидетельств (документированных материалов)

...

AGD_OPE.1.6C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть **приведено** описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ**, имеющих отношение к пользователю**.

...

AGD_PRE.1 Подготовительные процедуры

...

AGD_PRE1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО**, реализации и оценки реализации всех функций безопасности среды функционирования ОО** в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

...»

Действующая редакция ГОСТ Р ИСО/МЭК 15408 не предъявляет требований к разработчику (заявителю) по проведению анализа уязвимостей.

«AVA_VAN.4 Методический анализ уязвимостей

...

Элементы действий разработчика

AVA_VAN.4.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA_VAN.4.1C ОО должен быть пригоден для тестирования.

...»

Предыдущая редакция ГОСТ Р ИСО/МЭК 15408 предъявляла следующие требования:

«AVA_VLA.3 Умеренно стойкий

...

Элементы действий разработчика

AVA_VLA.3.1D Разработчик должен выполнить анализ уязвимостей.

AVA_VLA.3.2D Разработчик должен предоставить документацию анализа уязвимостей.

Элементы содержания и представления свидетельств

AVA_VLA.3.1C Документация анализа уязвимостей должна содержать описание анализа поставляемых материалов ОО, выполненного для поиска способов, которыми пользователь может нарушить ПБО.

AVA_VLA.3.2C Документация анализа уязвимостей должна содержать описание решения в отношении идентифицированных уязвимостей.

AVA_VLA.3.3C Документация анализа уязвимостей должна показать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде ОО.

AVA_VLA.3.4C Документация анализа уязвимостей должна содержать логическое обоснование, что ОО с идентифицированными уязвимостями устойчив по отношению к очевидным атакам проникновения.

AVA_VLA.3.5C Документация анализа уязвимостей должна показывать, что поиск уязвимостей является систематическим.

...»

Для обеспечения преемственности требований и сохранения принятой технологии сертификации в ПЗ, утвержденных ФСТЭК России, требования по проведению анализа уязвимостей сохранены путем выполнения уточнения над соответствующими компонентами ТДБ из семейства AVA_VAN:

«AVA_VAN.4 Методический анализ уязвимостей

...

Элементы действий заявителя

AVA_VAN.4.1D Заявитель должен **выполнить анализ уязвимостей ОО**.

Элементы содержания и представления свидетельств (документированных материалов)

AVA_VAN.4.1C **Документация анализа уязвимостей должна:**

содержать результаты анализа, выполненного для поиска способов, которыми потенциально может быть нарушена реализация ФТБ;

идентифицировать проанализированные предполагаемые уязвимости;

демонстрировать для всех идентифицированных уязвимостей, что ни одна из них не может быть использована в предполагаемой среде функционирования ОО.

...»

Что касается выполнения операции «назначение» над компонентами ТДБ, то в ГОСТ Р ИСО/МЭК 15408-3 имеются два примера, где допускается выполнение операции «назначение»: элементы ADV_INT.1.1D и ADV_SPM.1.1D.

В первом случае разработчику ПЗ или ЗБ нужно определить при помощи операции «назначение» подмножество ФБО, к которому применяется элемент.

Исходный элемент:

«ADV_INT.1.1D Разработчик должен выполнить проектирование и реализацию [назначение: *подмножество ФБО*] таким образом, чтобы внутренняя структура была полностью определенной».

Элемент с примером выполнения операции «назначение»:

«ADV_INT.1.1D Разработчик должен выполнить проектирование и реализацию [ФБО подсистемы аудита безопасности] таким образом, чтобы внутренняя структура ФБО была полностью определенной».

Во втором случае разработчику ПЗ или ЗБ нужно определить при помощи операции «назначение» подмножество формально моделируемых политик безопасности.

Исходный элемент:

«ADV_SPM.1.1D Разработчик должен представить формальную модель ПБО для [назначение: *список формально моделируемых политик*]».

Элемент с примером выполнения операции «назначение»:

«ADV_SPM.1.1D Разработчик должен представить формальную модель ПБО для [политики управления доступом]».

Кроме того, операции «назначение» и «выбор» активно применяются при определении (конкретизации) расширенных (специальных) компонентов ТДБ в ПЗ, утвержденных ФСТЭК России.

12.4.3 Спецификация в профиле защиты или задании по безопасности требований доверия к безопасности, не включенных в ГОСТ Р ИСО/МЭК 15408-3

Если в ПЗ включается расширенное ТДБ, то есть ТДБ, для которого в ГОСТ Р ИСО/МЭК 15408 нет соответствующего компонента доверия к безопасности, то рассматриваемое ТДБ должно быть определено в стиле компонентов из ГОСТ Р ИСО/МЭК 15408.

Рекомендации по определению расширенных (специальных) компонентов ТДБ представлены в разделе 11.

12.4.4 Определение документированных материалов (свидетельств), необходимых для проведения оценки

Для проведения работ по оценке соответствия продукта ИТ требованиям безопасности заявитель должен предоставить испытательной лаборатории документированные материалы (свидетельства), предусмотренные компонентами доверия к безопасности (в частности, элементами AXX_XXX.#.#C). Согласно требованиям ФСТЭК России для сертификации средств защиты информации 4—6 классов защиты должны быть представлены документированные материалы (свидетельства) согласно таблице 9.

Таблица 9 — Документированные материалы (свидетельства), предоставляемые заявителем для проведения сертификационных испытаний средств защиты информации

Документированные материалы (свидетельства), предоставляемые заявителем для проведения сертификационных испытаний средств защиты информации (в соответствии с ГОСТ Р ИСО/МЭК 15408-3—2013 и ГОСТ Р ИСО/МЭК 18045—2013)	Класс защиты средства защиты информации		
	6	5	4
1. Задание по безопасности	+	+	+
2. Функциональная спецификация	+	+	+
3. Проект на уровне подсистем (эскизный проект)		+	+
4. Проект на уровне модулей (технический проект)		+	+
5. Описание архитектуры безопасности		+	+
6. Представление реализации		+	+
7. Руководство пользователя по эксплуатации	+	+	+
8. Руководство по подготовительным процедурам	+	+	+
9. Описание процедур поставки		+	+
10. Документация по управлению конфигурацией:			
список управления конфигурацией (список конфигурации)	+	+	+
план управления конфигурацией			+
документация по применению управления конфигурацией			+
протоколы (записи) системы управления конфигурацией			+
описание технологии обновления средства защиты информации	+	+	+
регламент обновления программного обеспечения средства защиты информации	+	+	+
11. Документация по безопасности разработки			+
12. Документация процедур устранения недостатков		+	+
13. Документация определения жизненного цикла (модель жизненного цикла, используемая при разработке и сопровождении объекта оценки)			+
14. Документация инструментальных средств разработки		+	+
15. Тестовая документация (заявителя, разработчика)		+	+
16. Свидетельство о покрытии тестами		+	+
17. Материалы анализа глубины тестирования			+
18. Документация анализа уязвимостей		+	+
19. Описание технологии выпуска обновлений межсетевого экрана	+	+	+
20. Регламент обновления средства защиты информации	+	+	+
21. Документация процедуры представления обновлений для проведения внешнего контроля	+	+	+

Знак «+» в таблице 9 означает, что свидетельство требуется для проведения сертификационных испытаний средства защиты информации соответствующего класса защиты.

Содержание свидетельства определяется компонентами доверия к безопасности для соответствующего класса защиты.

Важно отметить, что свидетельства — это сведения (исходные данные), необходимые испытательной лаборатории для проведения сертификационных испытаний. При этом требований к количеству

или номенклатуре предоставляемых документов не предъявляется. Сведения могут быть сгруппированы заявителем (разработчиком) в документы по его усмотрению (в одном документе или электронном источнике может содержаться сразу несколько свидетельств; свидетельства могут содержаться в документах, в которых также присутствует иная информация, не относящаяся напрямую к сертификационным испытаниям). Заявитель также может включить содержание свидетельств в состав документов, которые он разработал в соответствии с национальными стандартами или техническим заданием на разработку средства защиты информации, выданным заказчиком (если применимо). При этом важно, чтобы испытательной лаборатории была предоставлена подробная информация относительно того, в каких документах (или электронных источниках) содержатся сведения, предусмотренные требованиями к содержанию конкретных свидетельств.

Также в целях поддержки сертификационных испытаний заявитель должен представлять в испытательную лабораторию образцы вредоносного программного обеспечения, описания компьютерных атак и т. п., противостояние которым заявляется как функциональная возможность ОО.

В зависимости от вида и (или) типа ОО это, например, могут быть:

- базы данных признаков компьютерных вирусов (для САВЗ);
- базы компьютерных атак (для СОВ);
- базы уязвимостей (для СА3).

12.4.5 Обоснование требований доверия к безопасности

Структура профиля защиты и задания по безопасности (если они не разрабатываются для низкого уровня доверия в соответствии с 15.1) требует также наличия обоснования выбора требований доверия к безопасности. Как было показано на рисунке 3, не требуется получение требований доверия к безопасности на основе определения проблемы безопасности или целей безопасности и, следовательно, требования доверия к безопасности могут быть получены из других источников. Поэтому ГОСТ Р ИСО/МЭК 15408-1 позволяет не предоставлять пояснений относительно того, каким образом были получены требования доверия к безопасности или каких-либо указаний конкретных правил, требующих наличия конкретного набора требований доверия к безопасности.

Во многих случаях требования доверия к безопасности получаются на основе угроз и источников угроз, идентифицированных в «Определении проблемы безопасности» с намерением выбрать требования доверия к безопасности таким образом, чтобы от ОО можно было ожидать противостояния атакам со стороны источников угроз, включенных в «Определение проблемы безопасности». В этом случае следует указать это в обосновании выбора требований доверия к безопасности.

Если ПЗ или ЗБ разрабатываются для конкретного класса защиты средств защиты информации, то включение конкретных требований доверия к безопасности ОО в ПЗ или ЗБ обосновывается требованиями соответствующего нормативного правового акта ФСТЭК России для данного вида средств защиты информации. Например, для средств контроля съемных носителей информации — требованиями документа ФСТЭК России «Требования к средствам контроля съемных машинных носителей информации».

13 Краткая спецификация объекта оценки

Краткая спецификация ОО требуется для ЗБ, но не требуется для ПЗ. Таким образом, данный раздел применим только в отношении ЗБ.

Основное назначение краткой спецификации ОО состоит в том, чтобы предоставить потребителям описание функциональных возможностей безопасности ОО, поясняющее, каким образом выполняются ФТБ. В краткой спецификации ОО следует описывать ФБО в контексте общих функциональных возможностей и архитектуры ОО и предоставлять достаточный уровень детализации для формирования абстрактного представления ОО в целом и того, каким образом ОО обеспечивает выполнение ФТБ.

Следовательно, краткая спецификация ОО представляет собой сконцентрированную на вопросах безопасности абстрактную модель всего ОО, в которой субъекты, объекты, атрибуты и правила безопасности, определенные в ФТБ, рассматриваются в контексте архитектуры ОО и его общих функциональных возможностей. Эта модель является довольно абстрактной моделью по отношению к целому ряду не связанных с безопасностью функций, обеспечиваемых ОО, поскольку эти функции не имеют отношения к функциональным возможностям безопасности, реализуемым ОО. Уровень детализации, предоставленный в краткой спецификации ОО, должен быть выше уровня детализации описания ОО,

с основным акцентом на пояснении того, каким образом обеспечивается выполнение ФТБ. Необходимо предоставить прослеживание, демонстрирующее, каким образом функциональные требования безопасности выполняются функциональными возможностями, описанными в краткой спецификации ОО.

Начинать краткую спецификацию рекомендуется с общего обзора, в котором представлено абстрактное описание архитектуры ОО, в том числе границ ФБО. Целесообразно описать, каким образом ФБО осуществляют собственную защиту от вмешательства и обхода, даже если не требуется соответствие компоненту ASE_TSS.2. Затем следует описать функциональные возможности безопасности на основе функциональной модели, которая используется для получения ФТБ. Также целесообразно осуществлять разработку краткой спецификации ОО параллельно с разработкой раздела ЗБ, описывающего ФТБ, что позволяет удостовериться в том, что каждое ФТБ сформулировано в соответствии с функциональной моделью. Таким образом, выполняется прослеживание функциональных возможностей безопасности, описанных в краткой спецификации ОО, к ФТБ. В краткую спецификацию ОО следует включать функциональную модель (полученную на основе использования рекомендаций из 12.2), сопровождаемую текстом, в котором эта модель рассматривается в контексте всего ОО со всеми его функциями и архитектурой. Это предоставляет пользователю ПЗ или ЗБ понимание того, почему были выбраны определенные функциональные возможности безопасности или элементы функциональных возможностей безопасности и каким образом они поддерживают общие функциональные возможности ОО. Кроме того, автоматически предоставляется дополнительное прослеживание краткой спецификации ОО к ФТБ, так как они разрабатываются на основе одной и той же модели.

Для случая составного ОО в краткой спецификации ОО необходимо описывать отдельные компоненты и то, каким образом они взаимодействуют для обеспечения выполнения ФТБ. В описании должна быть представлена информация относительно того, каким образом ФТБ для составного ОО может прослеживаться к функциональным требованиям безопасности ОО-компонентов, а также то, каким образом эти ФТБ взаимодействуют. Дополнительные рекомендации относительно заданий по безопасности для составных ОО приведены в 14.1.

14 Спецификация ПЗ и ЗБ для составных ОО и ОО-компонентов

14.1 Составные объекты оценки

В рамках среды функционирования большая часть ОО взаимодействует с другими продуктами или системами ИТ. Во многих случаях будет необходима поддержка таких продуктов или систем ИТ для выполнения функциональных требований безопасности. Простым примером служит ОО, являющийся системой управления базой данных (СУБД), которая полагается на защиту файлов, разделение адресного пространства и функции аутентификации пользователей базовой операционной системы. Еще одним примером может служить операционная система, которая полагается на внешний LDAP-сервер (сервер облегченного протокола доступа к каталогам) для хранения цифровых сертификатов и списков отозванных сертификатов, используемых для аутентификации, а также на внешнюю инфраструктуру открытых ключей для генерации сертификатов и списков отозванных сертификатов и своевременного выпуска их через LDAP-сервер. Объединяя эти два примера, система управления базами данных (вследствие зависимости от аутентификации пользователей в операционной системе) также полагается на LDAP-сервер и систему инфраструктуры открытых ключей для аутентификации пользователей. Этот пример можно расширить на случай использования смарт-карт в процессе аутентификации пользователя. В этом случае существуют зависимости от самой смарт-карты, а также от системы, используемой для персонализации смарт-карт.

Приведенные выше примеры демонстрируют, что простое на первый взгляд ФТБ (аутентификация пользователей) может потребовать правильного и защищенного взаимодействия целого ряда продуктов ИТ, которые могут быть соответствующим образом оценены по отдельности. В данном подразделе рассматривается проблема спецификации ФТБ для ОО в сочетании с целями безопасности для среды функционирования с целью рассмотрения проблемы удовлетворения ФТБ с помощью комбинации продуктов ИТ.

В приведенных выше примерах имеются следующие зависимости:

- система управления базами данных полагается на операционную систему для аутентификации пользователей, защиты файлов и разделения адресного пространства;
- операционная система полагается на базовые аппаратные средства для разделения адресного пространства и защиты от непосредственного доступа неуполномоченных программ к подключенным устройствам ввода/вывода и выделенным реестрам параметров конфигурации процессора;

- операционная система полагается на LDAP-сервер для защиты от информации, используемой для аутентификации пользователя, от несанкционированного доступа. Она также полагается на LDAP-сервер для своевременного предоставления информации по запросу способом, который также защищает информацию от необнаруживаемой модификации при передаче между LDAP-сервером и операционной системой;

- операционная система полагается на инфраструктуру открытых ключей для генерации цифровых сертификатов с правильной информацией о пользователе — владельце сертификата и для правильного управления этими сертификатами (в том числе своевременного выпуска сертификатов, а также списков отозванных сертификатов на LDAP-сервере);

- операционная система полагается на смарт-карту для защиты секретного ключа пользователя и для использования этого ключа только после получения правильной аутентификационной информации (в рассматриваемом примере PIN-кода);

- смарт-карта полагается на операционную систему основного компьютера для защиты PIN-кода пользователя с момента ввода его пользователем, при передаче на смарт-карту и до момента надежного удаления PIN-кода из памяти операционной системы основного компьютера. Смарт-карта полагается на операционную систему основного компьютера для защиты от несанкционированного использования PIN-кода пользователя, например, предоставления его на смарт-карту без разрешения пользователя.

Данный список зависимостей приведен для демонстрации того, каким образом списки зависимостей могут рассматриваться в ПЗ или ЗБ.

При анализе зависимостей можно легко идентифицировать:

- зависимость базы данных от операционной системы при обеспечении функциональных возможностей безопасности;
- зависимость операционной системы от аппаратных средств;
- зависимость операционной системы от LDAP-сервера;
- зависимость операционной системы от инфраструктуры открытых ключей;
- зависимость операционной системы от смарт-карты;
- зависимость смарт-карты от операционной системы основного компьютера.

В случае зависимости одного компонента от другого в ГОСТ Р ИСО/МЭК 15408 такие компоненты называются соответственно «зависимым» и «базовым». В приведенном примере при комбинировании базы данных и операционной системы база данных является зависимым компонентом, а операционная система — базовым компонентом. Аналогично при комбинировании операционной системы и аппаратных средств операционная система является зависимым компонентом, а аппаратные средства — базовым компонентом. В случае смарт-карты и операционной системы оба компонента зависят друг от друга и, следовательно, являются одновременно и зависимым, и базовым компонентами.

При разработке ПЗ или ЗБ для зависимого компонента зависимости от базового компонента должны рассматриваться как предположения, а цели безопасности для среды функционирования получаются на основе этих предположений. Для случая системы управлениями базой данных (СУБД) возможны следующие предположения:

Предположение-1:

«Среда функционирования будет защищать программное обеспечение СУБД от вмешательства и обхода со стороны любого другого прикладного программного обеспечения, выполняющегося на той же системе, что и СУБД»;

Предположение-2:

«Среда функционирования будет защищать файлы, используемые СУБД для хранения данных пользователей и данных ФБО от несанкционированного доступа»;

Предположение-3:

«Среда функционирования будет осуществлять идентификацию и аутентификацию отдельных пользователей и предоставлять метод получения для СУБД идентификатора пользователя, от имени которого осуществляется запрос к СУБД».

Эти предположения могут быть использованы для определения вполне конкретных целей для операционной системы как части среды функционирования. Уровень детализации этих целей во многом зависит от конкретных требований, предъявляемых к СУБД. Например, если к СУБД предъявляются требования по аудиту, то может быть полезным потребовать также определенного уровня аудита от операционной системы с тем, чтобы обнаруживать попытки обхода или вмешательства в функциональные возможности безопасности операционной системы, от которой зависит СУБД. Примеры целей безопасности, полученных на основе приведенных ранее предположений:

«Операционная система должна предоставить механизм, который позволяет СУБД выполняться в собственном домене, защищенном от вмешательств и обхода со стороны других прикладных программ, выполняющихся под управлением операционной системы.

Операционная система должна защищать от несанкционированного доступа исполняемые программы, которые относятся к СУБД.

Операционная система должна предоставить механизм, который позволяет обнаруживать нарушения целостности программного обеспечения СУБД и запрещать запуск СУБД в случае, если обнаружено нарушение целостности, которое не может быть исправлено.

Операционная система должна предоставить механизм управления доступом к файлам, который разграничивает по меньшей мере доступ по чтению и доступ к записи/изменению и позволяет индивидуально определять уровень доступа (в том числе запрещать доступ) вплоть до уровня отдельных пользователей.

Операционная система должна позволять ограничивать управление правами доступа к файлам для отдельных пользователей или определенных групп пользователей.

Операционная система должна осуществлять идентификацию и аутентификацию отдельных пользователей до разрешения им вызова функций СУБД.

Операционная система должна использовать защищенный механизм аутентификации, который ограничивает вероятность ошибочной аутентификации пользователя вероятностью меньшей, чем 1/1000000.

Операционная система должна поддерживать возможность аудита успешных и неудачных попыток аутентификации; запись аудита должна содержать указание идентификатора пользователя, время и дату попытки аутентификации.

Операционная система должна предоставлять интерфейс, который СУБД может использовать для правильного получения заявленного идентификатора пользователя, от имени которого вызывается функция базы данных».

Большинство целей безопасности можно легко проследить к ФТБ, определенным в соответствии с ГОСТ Р ИСО/МЭК 15408-2. Исключение составляет только первая цель безопасности, так как в ней рассматривается архитектурное свойство (разделение на домены). В документации по архитектуре безопасности следует описать, каким образом это свойство реализуется операционной системой. Документация по архитектуре безопасности является обязательной для уровней доверия ОУД2 и выше.

В случае, аналогичном рассмотренному выше, где СУБД является зависимым компонентом, а ОС — базовым, можно определить цели безопасности для ОС с достаточно высоким уровнем детализации, близким к уровню детализации в ФТБ. По возможности следует предоставлять такой уровень детализации.

Возможны и другие случаи, когда предположения и цели безопасности для среды функционирования, получаемые на основе этих предположений, должны иметь более общий характер. В примере с использованием операционной среды в качестве зависимого компонента и LDAP-сервера в качестве базового нужно сделать следующие предположения:

«В среде функционирования должна обеспечиваться защита цифровых сертификатов и списков отозванных сертификатов, требуемых операционной системой для аутентификации пользователя, от несанкционированной модификации от несанкционированного добавления сертификатов и списков отозванных сертификатов».

В этом случае в ПЗ или ЗБ могут не включаться некоторые детали описания такой защиты, что предоставит возможность различных способов удовлетворения этого предположения. Цели безопасности для среды функционирования, получаемые на основе этого предположения, могут иметь следующий вид:

«LDAP-сервер должен осуществлять идентификацию и аутентификацию пользователей до разрешения изменения и (или) добавления сертификатов и списков отозванных сертификатов, используемых операционной системой для аутентификации пользователей.

Среда функционирования должна защищать данные, передаваемые между LDAP-сервером и операционной системой от необнаруживаемой модификации (включая добавление и повтор)».

В приведенном примере разработчик ПЗ или ЗБ, вероятнее всего, не захочет подробнее специфицировать способ, которым достигаются эти цели безопасности для среды функционирования, предоставляя возможность использования целого ряда различных способов удовлетворения этих требований.

При разработке ПЗ или ЗБ для зависимого компонента необходимо различать случай, когда базовый компонент уже оценен, и результаты его оценки доступны при оценке зависимого компонента, и случай, когда базовый компонент либо не подвергался оценке, либо результаты его оценки недоступны.

Для первого случая ГОСТ Р ИСО/МЭК 15408-3 содержит класс доверия АСО «Композиция», который определяет критерии оценки композиции оцененных компонентов. Разработчик ПЗ или ЗБ для составного ОО должен включить компоненты из класса АСО, которые он считает подходящими для выбранного уровня доверия. Для содействия этому в ГОСТ Р ИСО/МЭК 15408-3 определены три составных пакета доверия, которые могут быть включены в ПЗ или ЗБ для составного ОО. При принятии решения о выборе компонентов из класса АСО «Композиция», отличных от включенных в эти предопределенные пакеты, нужно удостовериться в выполнении зависимостей.

14.2 ОО-компоненты

Наряду с ОО, которые являются самодостаточными и не имеют каких-либо явных зависимостей от других компонентов ИТ в среде функционирования, существует ряд типов ОО, для которых это условие не выполняется. В ПЗ или ЗБ такие ОО называются «составными ОО». Типичными примерами составных ОО являются:

- пакет программного обеспечения, который предоставляет определенные функциональные возможности безопасности, но предназначен для интеграции в ряд различных продуктов. Пакет программного обеспечения полагается на продукт, в который он интегрируется, для защиты своих ФБО и данных ФБО, а также при управлении некоторыми данными ФБО;
- приложение, реализующее управление доступом к своим собственным объектам, но полагающееся на средства идентификации и аутентификации пользователей, предоставляемые средой функционирования.

Во всех этих случаях одна или более целей безопасности прослеживаются к (сопоставляются с) ФТБ ОО только частично и частично же прослеживаются к среде функционирования. Поэтому ОО может быть оценен только с использованием предположения о том, что среда функционирования правильно реализует ФТБ, которые в полной мере достигают части целей безопасности, которых не в состоянии достичь ОО самостоятельно.

Таким образом, ПЗ или ЗБ для компонента незначительно отличается от ПЗ или ЗБ для самодостаточного продукта ИТ. Единственное отличие состоит в том, что в целях безопасности для ИТ-среды функционирования, необходимых для полного достижения целей безопасности для ОО, обычно указывают (по возможности) тип продукта ИТ в среде функционирования, предназначенного для достижения цели. В примере, приведенном в 14.1, в ЗБ для операционной системы могут быть четко и раздельно определены цели безопасности, которые должны достигаться базовыми аппаратными средствами, LDAP-сервером и смарт-картой. Эти цели безопасности следует определять как можно точнее, чтобы их можно было легко проследить к (сопоставить с) ФТБ, определенным в ЗБ этих компонентов. Это позволяет упростить прослеживание соответствия при оценке композиции этих ОО-компонентов как составного ОО.

15 Отдельные вопросы

15.1 Профили защиты и задания по безопасности низкого уровня доверия

Согласно ГОСТ Р ИСО/МЭК 15408 для профиля защиты или задания по безопасности, в котором требования доверия не выше определенных в ОУД1, допустимо упростить этот профиль защиты или задание по безопасности. В таком случае можно опустить:

- определение проблемы безопасности;
- цели безопасности;
- обоснование целей безопасности;
- обоснование требований безопасности, за исключением обоснования неудовлетворенных зависимостей между требованиями безопасности, определенными в ГОСТ Р ИСО/МЭК 15408.

Это допустимо для простых ПЗ или ЗБ, ориентированных на продукты с низким уровнем доверия. Все прочие разделы ПЗ или ЗБ при этом необходимо разрабатывать согласно описанным ранее рекомендациям.

В ПЗ или ЗБ низкого уровня доверия может утверждаться о соответствии только ПЗ низкого уровня доверия, в то время как в ПЗ или ЗБ более высокого уровня доверия может утверждаться о соответствии

ПЗ низкого уровня доверия. Такие ПЗ или ЗБ должны включать все требуемые настоящим стандартом разделы, не включенные в ПЗ низкого уровня доверия, о соответствии которому утверждается.

15.2 Соответствие национальным интерпретациям ГОСТ Р ИСО/МЭК 15408

В дополнение к требованиям, определенным для ПЗ или ЗБ в ГОСТ Р ИСО/МЭК 15408, в системах сертификации (в частности, в системе сертификации ФСТЭК России) могут быть определены конкретные национальные интерпретации ГОСТ Р ИСО/МЭК 15408, связанные со структурой и содержанием ПЗ или ЗБ.

В случае утверждения эти национальные интерпретации должны учитываться разработчиками ПЗ или ЗБ.

15.3 Функциональные пакеты и пакеты доверия

Помимо ПЗ или ЗБ в ГОСТ Р ИСО/МЭК 15408 допускается также определение функциональных пакетов и пакетов доверия. Функциональный пакет содержит набор ФТБ; пакет доверия содержит набор ТДБ. Использование смешанных пакетов, содержащих и ФТБ, и ТДБ, не допускается.

Используемый функциональный пакет или пакет доверия должен иметь имя, позволяющее его идентифицировать, и содержать набор применимых и эффективных требований. Например, функциональный пакет может содержать ФТБ, относящиеся к одному конкретному аспекту безопасности. Типичным примером является функциональный пакет, определяющий функциональные возможности безопасности, связанные с аудитом (минимальный набор подлежащих аудиту событий, защита журнала аудита, требования просмотра данных аудита, управление аудитом), и не рассматривающий какие-либо другие вопросы. Такой функциональный пакет может быть в дальнейшем повторно использован для обеспечения безопасности разных типов продуктов ИТ (например, операционных систем, систем управления базами данных, межсетевых экранов). При определении функционального пакета либо пакета доверия имеет смысл удовлетворять зависимости либо непосредственно в рамках пакета, либо посредством предоставления рекомендации по поводу того, каким образом следует учитывать неудовлетворенные зависимости при использовании пакета.

В существующих профилях защиты ФСТЭК России встречается также следующая ситуация. В ПЗ для СКН для 4 класса защиты (ИТ.СКН.П4.ПЗ) в качестве пакета доверия определен ОУД3 усиленный и расширенный. В частности, ОУД3 усилен компонентом ADV_IMP.2 «Полное отображение представления реализации ФБО». Компонент ADV_IMP.2 «Полное отображение представления реализации ФБО» имеет зависимость от компонента ALC_CMC.5 «Расширенная поддержка». По общему правилу компонент ALC_CMC.5 «Расширенная поддержка» либо следовало включить в ПЗ для СКН, либо обосновать неудовлетворение зависимости, либо предоставить рекомендации по удовлетворению этой зависимости в задании по безопасности. В ПЗ для СКН для 4 класса защиты (ИТ.СКН.П4.ПЗ) зависимость не была удовлетворена, так как уровень требований ALC_CMC.5 «Расширенная поддержка» (этот компонент является штатным для ОУД6) является необоснованно высоким для ОУД3 и 4 класса защиты СКН; вместе с тем в пакет доверия и в ПЗ ИТ.СКН.П4.ПЗ был включен компонент ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация» как достаточное усиление, соответствующее общему уровню требований пакета доверия и классу защиты СКН.

16 Использование автоматизированных инструментальных средств

Структурированный характер ГОСТ Р ИСО/МЭК 15408 делает актуальным вопрос об автоматизации разработки и оценки таких ключевых документов, определенных в комплексе стандартов ГОСТ Р ИСО/МЭК 15408, как профили защиты и задания по безопасности.

Использование соответствующих инструментальных средств позволит разработчику ПЗ или ЗБ сконцентрироваться на содержании документов за счет того, что инструментальные средства будут автоматически решать ресурсоемкие задачи (правильного представления ПЗ, проверку удовлетворения зависимостей и др.), а также позволит освободить экспертов от наиболее трудоемких действий при оценке ПЗ или ЗБ.

Приложение А
(справочное)

Пример определения расширенного компонента

В данном приложении приведен пример определения расширенного функционального компонента безопасности, относящегося к требованиям по реагированию на нарушения безопасности.

А.1. Пример определения расширенного функционального компонента безопасности, относящегося к требованиям по реагированию на нарушения безопасности

«1 Класс FFW: Реакция на нарушения безопасности

Средства защиты информации уровня узла информационной системы могут быть в определенное время недоступны для управления со стороны администратора средства защиты информации. Поэтому для оперативного решения проблем безопасности может потребоваться взаимодействие средства защиты информации с пользователем технического средства, в интересах которого функционирует средство защиты информации. Это взаимодействие может быть в форме выдачи предупреждающих сообщений пользователю, а также в форме предоставления пользователю возможности осуществить определенные действия (например, средствами защиты информации блокировать доступ к средству вычислительной техники).

Рисунок А.1 — Декомпозиция класса FFW «Реакция на нарушения безопасности»

1.1 Действия по реагированию (семейство FFW_ARP_EXT)

1.1.1 Характеристика семейства

Семейство FFW_ARP_EXT определяет реакцию на обнаружение возможного нарушения безопасности.

1.1.2 Ранжирование компонентов

В FFW_ARP_EXT.1 «Сигналы нарушения безопасности» функциональных возможностей безопасности должны осуществлять определенные действия в случае обнаружения возможного нарушения безопасности.

1.1.3 Управление: FFW_ARP_EXT.1

Для функций управления из класса FMT могут рассматриваться следующие действия.

а) Управление действиями (добавление, удаление или модификация).

1.1.4 Аудит: FFW_ARP_EXT.1

Если в ПЗ или ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий.

а) Минимальный: действия, предпринимаемые в ответ на возможные нарушения безопасности.

1.1.5 FFW_ARP_EXT.1 Сигналы нарушения безопасности

Иерархический для: нет подчиненных компонентов.

Зависимости: отсутствуют.

1.1.5.1 FFW_ARP_EXT.1.1

Функциональные возможности безопасности должны осуществить [назначение: список действий] при обнаружении возможного нарушения безопасности.

1.1.6 Замечания по применению для пользователя

При возможном нарушении безопасности, выявленном средством защиты информации, следует осуществить определенные действия. Это может быть выдача предупреждающих сообщений пользователю, а также предоставление пользователю возможности осуществить определенные действия (например, блокировать доступ к средству вычислительной техники).

Предупреждающие сообщения должны быть направлены на оказание помощи в устранении возникшей проблемы.

Разработчику ПЗ или ЗБ следует быть особенно внимательным при определении последовательности осуществления таких действий.

1.1.7 Операции

1.1.7.1 Назначение

В элементе FFW_ARP_EXT.1.1 разработчику ПЗ или ЗБ следует определить действия, предпринимаемые в случае возможного нарушения безопасности. Примером списка таких действий является: «выдача предупреждающих сообщений пользователю, предоставление пользователю возможности осуществить блокирование доступа к средству вычислительной техники». Можно также указать, что предпринимаемые действия могут определяться уполномоченным пользователем».

Приложение Б
(рекомендуемое)

Основные примеры

Б.1 Введение

В данном приложении приведены примеры угроз, ПБОр, предположений безопасности, целей безопасности. Кроме того, данное приложение содержит рекомендации по выбору функциональных компонентов, описанных в ГОСТ Р ИСО/МЭК 15408-2, для спецификации конкретных требований безопасности.

Формулировки угроз, ПБОр, предположений безопасности, целей и требований безопасности из данного приложения могут быть адаптированы для использования в конкретных ПЗ и ЗБ.

Б.2 Примеры угроз

При разработке ПЗ или ЗБ важным моментом является определение угроз. Ниже приведены примеры угроз:

- необнаруженная компрометация активов ИТ (преднамеренная или нет) в результате санкционированных действий уполномоченного пользователя ОО;
- уполномоченный пользователь ОО может получить доступ к информации или ресурсам без разрешения их владельца или лица, ответственного за данную информацию или данные ресурсы;
- необнаруженная компрометация активов ИТ в результате попытки нарушителя (сотрудника организации или постороннего лица) выполнить действия, которые ему не разрешены;
- нарушитель может перехватить данные, передаваемые по сети;
- уполномоченный пользователь ОО расходует общие ресурсы, ставя под угрозу возможность для других уполномоченных пользователей получить доступ к этим ресурсам или использовать эти ресурсы;
- уполномоченный пользователь ОО может (преднамеренно или случайно) передавать (по скрытому каналу) чувствительную информацию пользователям, которые не имеют допуска к работе с данной информацией;
- пользователь может участвовать в передаче информации (как отправитель или получатель), а затем впоследствии отрицать данный факт;
- компрометация активов ИТ в результате использования ОО уполномоченным пользователем в несоответствующее время дня или в несоответствующем месте;
- уполномоченный пользователь ОО может экспортировать информацию от ОО (в виде электронной или твердой копии) и впоследствии обрабатывать ее способами, противоречащими ее маркировке по степени секретности (конфиденциальности);
- нарушитель (постороннее лицо или сотрудник организации) может получить несанкционированный доступ к информации или ресурсам, выдавая себя за уполномоченного пользователя ОО;
- целостность информации может быть поставлена под угрозу из-за ошибки пользователя, аппаратных ошибок или ошибок при передаче;
- нарушитель может иметь возможность наблюдать за многократным использованием ресурсов или услуг какой-либо сущностью (субъектом или объектом) и, анализируя факты такого использования, получать информацию, которую требуется сохранить в секрете;
- целостность информации может быть нарушена вследствие несанкционированной модификации или уничтожения информации нарушителем;
- нарушитель может иметь возможность наблюдать законное использование ресурса или услуги пользователем, в то время как пользователь желает сохранить в секрете факт использования этого ресурса или услуги;
- пользователь ОО может (преднамеренно или случайно) наблюдать (изучать) информацию, сохраненную в ОО, к которой он не имеет допуска.

Следующие угрозы могут учитываться при формулировании целей безопасности для среды:

- ошибка человека, отказ программного обеспечения, аппаратных средств или источников питания могут вызвать внезапное прерывание в работе ОО, приводящее к потере или искажению критичных по безопасности данных;
- старение и износ носителей данных или несоответствующее хранение и обращение со сменным носителем могут привести к его порче, ведущей к потере или искажению критичных по безопасности данных;
- критичные по безопасности части ОО могут быть подвергнуты физической атаке, ставящей под угрозу их безопасность;
- компрометация активов ИТ может происходить в результате непреднамеренных или преднамеренных действий, предпринятых администраторами или другими привилегированными пользователями;
- целостность и (или) доступность активов ИТ может быть нарушена в результате непреднамеренного занесения в систему компьютерного вируса уполномоченным пользователем ОО.

Б.3 Примеры политики безопасности организации

Данный пункт содержит два типичных примера ПБОр.

ПБОр на основе дискреционного принципа управления доступом — право доступа к конкретным объектам данных определяется на основе:

а) идентификационной информации владельца объекта;

б) идентификационной информации субъекта, осуществляющего доступ;

в) явных и неявных прав доступа к объекту, предоставленных субъекту владельцем данного объекта.

ПБОр на основе мандатного принципа управления доступом — право доступа к информации, маркированной по степени секретности (уровню конфиденциальности), определяется следующим образом:

а) данному лицу разрешен доступ к информации, только если оно имеет соответствующий допуск;

б) данное лицо не может изменять обозначение степени секретности (уровня конфиденциальности) информации в сторону снижения, если у него нет явных полномочий на выполнение таких действий.

Для каждой конкретной организации может потребоваться большая степень детализации ПБОр, чем в приведенных примерах.

Б.4 Примеры предположений безопасности

Данный подраздел содержит примеры предположений безопасности, относящихся к физической защите, персоналу и связности ОО и его среды.

Б.4.1 Примеры предположений, связанных с физической защитой

Предположение о расположении ресурсов ОО — предполагается, что ресурсы ОО расположены в пределах контролируемой зоны, позволяющей предотвратить несанкционированный физический доступ.

Предположение о физической защите ОО — предполагается, что аппаратные средства и программное обеспечение ОО, критичные по отношению к реализации политики безопасности, физически защищены от несанкционированной модификации со стороны потенциальных нарушителей.

Б.4.2 Примеры предположений, связанных с персоналом

В данном пункте приведены примеры предположений, связанных с персоналом, которые могут быть использованы при формировании ПЗ или ЗБ:

- предполагается, что назначены один или несколько уполномоченных администраторов, которые компетентны (обладают необходимой квалификацией), чтобы управлять ОО и безопасностью информации, которую содержит ОО. При этом данным администраторам можно доверять в том, что они не злоупотребят преднамеренно своими привилегиями с тем, чтобы нарушить безопасность;
- предполагается, что нарушители имеют высокий уровень специальных знаний, мотивации и необходимые ресурсы;
- предполагается, что пользователи ОО обладают необходимыми привилегиями для доступа к информации, которой управляет ОО.

Б.4.3 Примеры предположений, имеющих отношение к связности

В данном пункте приведены примеры предположений, имеющих отношение к связности, которые могут быть использованы при формировании ПЗ или ЗБ:

- предполагается, что все соединения с периферийными устройствами находятся в пределах контролируемой зоны;
- предполагается, что межсетевой экран настроен таким образом, что он является единственной точкой сетевого соединения между частной (приватной) сетью и (потенциально) враждебной сетью;
- предполагается, что любые другие системы, с которыми связывается ОО, принадлежат тому же органу управления, что и ОО, и работают при тех же самых ограничениях политики безопасности.

Б.5 Примеры целей безопасности для ОО

В данном подразделе приведены примеры целей безопасности для ОО, которые могут быть использованы при формировании ПЗ или ЗБ:

- ОО должен предоставить уполномоченному администратору средства, позволяющие ему эффективно управлять ОО и его (ОО) функциями безопасности, а также гарантировать, что только уполномоченные администраторы могут получить доступ к таким функциональным возможностям;
- ОО должен предусматривать средства разрешения субъекту использовать ресурс или услугу без раскрытия идентификационной информации пользователя другим сущностям (объектам или субъектам);
- ОО должен предусматривать средства регистрации любых событий, относящихся к безопасности, чтобы помочь администратору в обнаружении потенциальных нарушений (атак) или неправильной настройки параметров, которые делают ОО уязвимым для потенциальных нарушений (атак), а также держать пользователей подотчетными за любые действия, которые они исполняют и которые связаны с безопасностью;
- ОО должен предоставлять пользователям средства управления и ограничения доступа других пользователей (или идентифицированных групп пользователей) к объектам и ресурсам, по отношению к которым первые являются владельцами или ответственными, в соответствии с набором правил, определенных политикой безопасности с дискреционным управлением доступа P.DAC;

- ОО должен предусматривать средства защиты конфиденциальности информации при передаче последней по сети между двумя конечными системами;

- ОО должен иметь возможность ограничения входа (доступа к ОО) пользователя на основе времени и расположения устройства входа (доступа);

- ОО должен выполнять уникальную идентификацию всех пользователей и аутентификацию (проверку подлинности) идентификационной информации до предоставления пользователю доступа к сервисам ОО;

- ОО должен иметь средства обнаружения нарушения целостности информации;

- ОО должен хранить и сохранять целостность меток для информации, хранимой и обрабатываемой ОО. Вывод данных (экспорт) ОО должен иметь метки секретности (конфиденциальности), которые в точности соответствуют внутренним меткам секретности (конфиденциальности);

- ОО должен защищать конфиденциальность информации, за управление которой ОО отвечает, в соответствии с политикой безопасности с мандатным управлением доступа P.MAC, основанной на непосредственном сравнении индивидуальных разрешений (полномочий) по отношению к информации и маркировки чувствительности (конфиденциальности и др.) информации (мандатный принцип контроля доступа);

- ОО должен иметь средства подготовки доказательства авторства для того, чтобы предотвратить возможность отрицания отправителем информации факта ее отправки получателю, и доказательства получения информации для того, чтобы предотвратить возможность отрицания получателем информации факта получения этой информации;

- ОО должен иметь средства собственной защиты от внешнего вмешательства или вмешательства со стороны недоверенных субъектов или от попыток недоверенных субъектов обойти функции безопасности ОО;

- ОО должен предусматривать средства для разрешения субъекту использовать ресурс или услугу без раскрытия идентификационной информации пользователя другим сущностям (объектам или субъектам) и в то же время держать эту сущность (субъект) подотчетной за это использование;

- ОО должен предотвращать доступ пользователей к выполнению операций над ресурсами ОО, на которые они явным образом не уполномочены;

- ОО должен иметь средства управления использованием ресурсов пользователями ОО и субъектами в целях предотвращения несанкционированного отказа в обслуживании;

- ОО должен иметь средства возврата к состоянию правильного функционирования, позволяя пользователю отменить транзакции в случае неправильной последовательности транзакций;

- ОО должен иметь средства, позволяющие сущности многократно использовать ресурсы или услуги, выполняя это обособленно от других сущностей (объектов или субъектов), имеющих возможность доступа к тем же ресурсам или услугам;

- ОО должен иметь средства, позволяющие пользователю использовать ресурс или услугу без раскрытия другим сущностям факта использования ресурса или услуги.

Б.6 Примеры целей безопасности для среды

В данном подразделе приведены примеры целей безопасности для среды, которые могут быть использованы при формировании ПЗ или ЗБ:

- администраторы ОО должны обеспечить эффективное использование функциональных возможностей аудита. В частности:

а) должны быть предприняты соответствующее действия (меры) для того, чтобы гарантировать непрерывное ведение журналов аудита, например, путем регулярного архивирования файлов регистрационных журналов перед очисткой журналов аудита с тем, чтобы обеспечить достаточное свободное пространство (на диске);

б) журналы аудита следует регулярно проверять и принимать соответствующие меры по обнаружению нарушений безопасности или событий, которые, по всей видимости, могут привести к таким нарушениям в будущем;

- ответственные за ОО должны обеспечить, чтобы данные аутентификации для каждой учетной записи пользователя ОО сохранялись в тайне и не раскрывались лицам, не уполномоченным использовать данную учетную запись;

- ответственные за ОО должны обеспечить отсутствие подключения к внешним системам или пользователям, которые могут нарушить безопасность ИТ;

- ответственные за ОО должны обеспечить безопасность ОО на этапах его поставки, установки и эксплуатации;

- ответственные за ОО должны обеспечить, чтобы те части ОО, которые являются критичными по отношению к реализации политики безопасности, были защищены от физического нападения, которое могло бы поставить под угрозу безопасность ИТ;

- ответственные за ОО должны обеспечить, чтобы процедуры и (или) механизмы были представлены таким образом, что после отказа системы или другой неисправности восстановление системы достигается без ущерба для безопасности ИТ.

Б.7 Пример соответствия целей безопасности и угроз

В таблице Б.1 приведен пример соответствия целей безопасности и угроз.

Таблица Б.1 — Пример соответствия целей безопасности и угроз

Активы	Угрозы	Цели безопасности	
Данные на носителях	Данные раскрыты путем незаконного перемещения носителя	Предупреждение	Контроль перемещения носителя Предотвращение раскрытия данных
		Обнаружение	Контроль хранения носителей
	Обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом	Предупреждение	Управление эксплуатацией (например, ограничение возможности использования прикладной программы или терминала приложений) Контроль прав доступа к данным
		Обнаружение	Аудит регистрационного журнала эксплуатации приложения, обнаружение незаконного умышленного изменения, искажения или хищения данных и контроль последовательной нумерации данных
		Реагирование	Резервное копирование/восстановление данных
	Данные раскрыты путем их выгрузки с носителя данных неуполномоченным лицом	Предупреждение	Управление эксплуатацией (например, ограничение использования функции выгрузки или терминала приложения) Предотвращение раскрытия данных
		Обнаружение	Аудит информации журнала эксплуатации
Данные на носителях	Использование остаточной информации на носителе	Предупреждение	Очистка памяти при удалении данных Предотвращение раскрытия данных
	Незаконное копирование данных	Предупреждение	Управление эксплуатацией (например, ограничение использования функции копирования или терминала приложения) Контроль прав доступа к данным Предотвращение раскрытия данных
		Обнаружение	Аудит эксплуатации Контроль оригинала (например, при помощи идентификационных меток, встроенных в исходные тексты)
	Данные незаконно используются или их использование затруднено из-за изменения атрибутов доступа к данным неуполномоченным лицом	Предупреждение	Управление эксплуатацией (например, ограничение использования функции изменения атрибутов данных или терминала приложения) Контроль прав доступа к файлу регистрации атрибутов
		Обнаружение	Аудит эксплуатации
		Реагирование	Резервное копирование/восстановление данных
	Данные получены незаконно путем фальсификации файла	Предупреждение	Управление эксплуатацией (например, ограничение использования функций создания и удаления файлов или рабочего терминала) Предотвращение раскрытия данных
Данные на носителях	Данные повреждены из-за разрушения носителя	Обнаружение	Аудит информации о владельцах файлов

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Данные на носителях	Данные повреждены из-за разрушения носителя	Предупреждение	Физическая защита носителей и управление доступом к месту их хранения Дублирование хранимых носителей
		Обнаружение	Контроль хранимых носителей
		Реагирование	Резервное копирование/восстановление данных
	Данные уничтожены или их использование затруднено из-за неисправности устройства ввода-вывода	Предупреждение	Контроль качества устройств ввода-вывода Дублирование хранимых носителей
		Обнаружение	Обнаружение отказов (средствами ОС) Аудит файла (журнала) регистрации выполнения программы
		Реагирование	Резервное копирование/восстановление данных
	Обращение к данным, изменение, удаление, добавление в приложение или извлечение из приложения данных неуполномоченным лицом путем использования соответствующей команды	Предупреждение	Управление эксплуатацией (например, ограничение использования команд или терминала) Контроль прав доступа к данным
		Обнаружение	Аудит информации из файла (журнала) регистрации операций, обнаружение незаконного умышленного изменения, искажения или хищения данных и контроль последовательной нумерации данных
		Реагирование	Резервное копирование/восстановление данных
Данные на носителях	Данные ошибочно удалены уполномоченным лицом	Предупреждение	Обеспечение соответствующих руководств по эксплуатации или автоматизация операций Предотвращение операционных ошибок (например, путем повторной проверки и последовательной регистрации прав удаления)
		Обнаружение	Аудит информации из журнала эксплуатации
		Реагирование	Резервное копирование/восстановление данных
Данные в телекоммуникационных линиях	Данные перехвачены или разрушены в телекоммуникационной линии	Предупреждение	Физическая защита телекоммуникационных линий или контроль подключения оборудования к линиям Предотвращение раскрытия данных, обнаружение незаконного умышленного изменения, искажения или хищения данных
		Обнаружение	Обнаружение незаконного умышленного изменения, искажения или хищения данных
		Реагирование	Повторная передача данных
	Данные прослушиваются, незаконно умышленно изменены, искажены, похищены, удалены или дополнены в системе коммутации	Предупреждение	Управление эксплуатацией коммутационной системы (например, ограничение использования анализаторов протоколов ЛВС)

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Данные в телекоммуникационных линиях	Данные незаконно используются в результате подмены их адресата, отправителя или изменения атрибутов доступа в системе коммутации	Предупреждение	Управление эксплуатацией системы коммутации (ограничение использования функции отладки)
		Обнаружение	Управление обнаружением незаконного умышленного изменения, искажения или похищения данных Аудит журнала, содержащего информацию о работе отладочных средств
		Реагирование	Повторная передача данных
	Связь заблокирована из-за повреждения линии	Предупреждение	Установка резервных телекоммуникационных линий Контроль качества телекоммуникационных линий
		Обнаружение	Обнаружение повреждений (средствами ОС)
		Реагирование	Повторная передача данных
	Связь заблокирована из-за аномалий в канале связи	Предупреждение	Установка резервных каналообразующих устройств Контроль качества каналов связи
		Обнаружение	Обнаружение отказов (средствами ОС)
		Реагирование	Повторная передача данных
	Несанкционированная повторная передача данных в неразрешенный адрес	Предупреждение	Управление эксплуатацией системы коммутации (например, наложение ограничений на регистрацию программ)
		Обнаружение	Предотвращение повторной передачи (путем использования порядковых номеров или временных меток)
Прикладные программы (приложения)	Выполнение приложения неуполномоченным лицом	Предупреждение	Управление правами на выполнение программы Управление эксплуатацией системы коммутации (ограничение числа дисплеев отображения работы программ) Управление расположением и маршрутом выполнения программ Обеспечение безопасности в момент отсутствия оператора Наложение ограничений на использование терминалов приложений
		Обнаружение	Аудит выполнения программ
		Реагирование	Резервирование/восстановление данных
	Обращение к данным в библиотеке программ, модификация или удаление данных в библиотеке программ неуполномоченным лицом	Предупреждение	Управление правами доступа к библиотекам программ Управление функционированием (ограничение использования команд модификации) Ограничение использования терминалов
		Обнаружение	Аудит функционирования
		Реагирование	Резервное копирование/восстановление программ

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Прикладные программы (приложения)	Незаконное использование программы или затруднение ее использования путем изменения ее атрибутов доступа неуполномоченным лицом	Предупреждение	Управление правами на выполнение программы Управление правами на доступ к каталогу библиотеки программ Управление функционированием (ограничение использования команд модификации)
		Обнаружение	Аудит функционирования
Прикладные программы (приложения)	Аномалии в ходе выполнения программы из-за аппаратного отказа компьютера	Предупреждение	Использование аппаратной конфигурации с дублированием Контроль качества аппаратных средств
		Обнаружение	Обнаружение недостатков (средствами ОС)
		Реагирование	Восстановление работоспособности аппаратного обеспечения
Прикладные процессы и данные	Несанкционированное использование прикладных процессов (например, запросов по Telnet и FTP)	Предупреждение	Управление правами на выполнение программ Использование межсетевых экранов (фильтров прикладного уровня) Использование инструкций по эксплуатации
		Обнаружение	Аудит выполнения программ
	Блокировка прикладных процессов (атаки, направленные на переполнение трафика, например, запросы на обработку потока ненужных данных)	Предупреждение	Назначить приоритеты обработки процессов Запретить передачу электронной почты
		Обнаружение	Аудит сетевого доступа
	Отрицание факта обмена данными или отрицание их содержания	Предупреждение	Принятие мер, препятствующих отказу (например, сохранение доказательств, используя третью доверенную сторону) Использование инструкций по эксплуатации
	Отказ от авторства данных	Предупреждение	Использование удостоверяющих сервисов (например, подтверждения авторства) Использование инструкций по эксплуатации
Прикладные процессы и данные	Несанкционированная передача данных	Предупреждение	Управление потоками данных (например, использование межсетевого экрана и применение правил базы данных) Контроль качества прикладных программ Управление функционированием (например, наложение ограничений на регистрацию программ)
		Обнаружение	Аудит доступа к данным
	Несанкционированное использование данных или программ путем использования оставшихся в программах отладочных функций	Предупреждение	Управление правами на доступ к данным и на выполнение программ Управление функционированием (например, ограничение возможности использовать функцию отладки)
		Обнаружение	Аудит выполнения прикладной программы

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Прикладные процессы и данные	Необоснованный отказ от предоставления услуги	Предупреждение	Назначение приоритетов обработки процессов Контроль качества прикладных программ Обучение и обеспечение инструкциями эксплуатационного персонала Контроль качества аппаратных средств обработки данных Оценка производительности ресурсов обработки данных
		Обнаружение	Аудит выполнения прикладной программы
	Незаконное умышленное изменение, искажение, похищение, удаление или разрушение данных	Предупреждение	Управление правами на использование данных Управление созданием и пересылкой данных
		Обнаружение	Обнаружение изменений данных
		Реагирование	Резервное копирование данных
Прикладные процессы и данные	Несанкционированное выполнение операций	Предупреждение	Управление правами на выполнение операций Контроль места выполнения операций (удаленный, через Интернет и т. д.)
		Обнаружение	Аудит выполнения операций
	Нарушение конфиденциальности	Предупреждение	Управление правами на использование конфиденциальной информации Анонимность и использование псевдонимов Обеспечение правильности завершения сеанса обработки данных
Отображаемые данные	Просмотр данных неуполномоченным лицом	Предупреждение	Физическая защита (изоляция) дисплея Обеспечение выполнения требований эксплуатационной документации
	Несанкционированное копирование или печать	Предупреждение	Обеспечение защиты во время отсутствия уполномоченного лица Ограничение использования функций копирования и печати Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Контроль подлинности (электронные метки)
Вводимые данные	Данные раскрыты во время ввода	Предупреждение	Контроль доступа в помещение, в котором расположен терминал ввода информации Обеспечение выполнения требований эксплуатационной документации
	Введенные данные несанкционированно изъяты (или удалены)	Предупреждение	Контроль носителя, на котором хранятся введенные данные Обеспечение выполнения требований эксплуатационной документации
		Реагирование	Резервное копирование вводимых данных
Данные, выводимые на печать	Ознакомление или изъятие данных неуполномоченным лицом	Предупреждение	Физическая защита печатаемых данных Обеспечение выполнения требований эксплуатационной документации

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Данные, выводимые на печать	Несанкционированное копирование	Предупреждение	Защита от копирования Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Контроль подлинности (электронная метка)
Данные пользователей	Пользователь (человек, система, терминал) не может быть идентифицирован	Предупреждение	Идентификация доступа Идентификация (назначение идентификатора каждому пользователю/системе; IP-адрес) Ограничение рабочих мест
		Обнаружение	Аудит выполнения идентификации
	Маскировка путем использования раскрытой идентификационной информации пользователя (человека, системы, терминала)	Предупреждение	Аутентификация пользователя Контроль идентификационной информации
		Обнаружение	Аудит выполнения идентификации
	Пользователь не идентифицирован	Предупреждение	Безотлагательная аутентификация (аутентификация до любых действий пользователя) Надежная идентификация Аутентификация на основе секретного ключа, пароля, биометрических характеристик Аутентификация с обратной связью
		Обнаружение	Аудит выполнения аутентификации
Данные пользователей	Маскировка путем использования незаконно раскрытой информации аутентификации	Предупреждение	Использование нескольких механизмов аутентификации Управление доступом к серверу (раннее обнаружение атак; регистрация информации о выполнении аутентификации) Защита аутентификационной информации Ограничение путей доступа (например, запрет доступа с использованием общих телекоммуникационных линий и Интернет) Использование одноразовых паролей
		Обнаружение	Аудит доступа к системе
		Реагирование	Блокировка работы пользователя
	Маскировка путем незаконного (логического) вывода аутентификационной информации	Предупреждение	Аутентификация (предотвращение логического вывода) Управление доступом к серверу (раннее обнаружение атак; обеспечение невозможности получения доступа к серверу на длительный период) Использование нескольких механизмов аутентификации Управление аутентификационной информацией (например, предотвращение логического вывода, использование синтаксических правил генерации аутентификационной информации и изменение ее начального значения)
		Обнаружение	Аудит доступа к системе

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Данные пользователей	Маскировка путем использования недействительной аутентификационной информации	Реагирование	Блокировка работы пользователя Минимизация нежелательного воздействия (минимизация времени действия)
		Предупреждение	Контроль срока действия аутентификационной информации Управление аутентификационной информацией (например, контроль за уничтожением информации)
		Обнаружение	Аудит доступа к системе
	Использование недействительного права из-за сбоя журнала регистрации прав пользователей	Предупреждение	Контроль за пользователями (безотлагательное отражение модификации прав пользователей)
		Обнаружение	Аудит доступа к системе
	Действия пользователя несанкционированно раскрыты (нарушение конфиденциальности)	Предупреждение	Управление правами доступа к регистрационной информации, имеющей отношение к пользователям Анонимность и использование псевдонимов Обеспечение правильности завершения сеанса обработки данных
		Обнаружение	Аудит доступа к системе
	Отрицание факта передачи данных	Предупреждение	Предотвращение отказа от факта передачи данных Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Аудит обмена данными
	Отрицание владения данными	Предупреждение	Автоматическая регистрация владельца в процессе формирования данных
		Обнаружение	Аудит доступа к системе
	Отрицание факта приема данных	Предупреждение	Предотвращение отказа от факта приема данных Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Аудит обмена данными
Данные пользователей	Данные посланы несоответствующему получателю вследствие его маскировки под авторизованного пользователя или ошибки спецификации	Предупреждение	Аутентификация адресата Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Аудит обмена данными
	Маскировка путем подделки информации аутентификации	Предупреждение	Управление правами доступа к аутентификационной информации Проверка достоверности аутентификационной информации Управление аутентификационной информацией (например, предотвращение фальсификации, надежная организация процесса аутентификации, физическая защита устройств аутентификации)
		Обнаружение	Управление доступом к серверу (раннее обнаружение атак)

Продолжение таблицы Б.1

Активы	Угрозы	Цели безопасности	
Системные службы и данные	Система незаконно используется пользователем, который выдает себя за оператора во время отсутствия оператора	Предупреждение	Обеспечение соответствующей защиты во время отсутствия оператора (например, временное прекращение работы, сеанса и проведение повторной аутентификации)
Системные службы и данные	Нарушение безопасности системы вследствие несанкционированного действия или ошибки уполномоченного пользователя	Предупреждение	Предотвратить ошибки уполномоченного пользователя (например, путем использования запросов подтверждения выполняемых действий) Управление правами пользователя (назначение минимально необходимых прав) Управление аудитом, разработка инструкций, повышение квалификации пользователей и применение штрафов
		Обнаружение	Аудит функционирования системы
	Внедрение вирусов	Предупреждение	Проверка на отсутствие вирусов в полученных программах, а также файлах, присоединенных к сообщениям, поступающим по электронной почте Управление доступом (назначение соответствующих прав доступа и защита файлов) Запрет использования данных или программ, полученных извне Контроль инсталляции программ
		Обнаружение	Аудит работы системы
		Реагирование	Выполнение необходимых ответных действий (например, остановка системы или отключение от внешней системы)
Системные службы и данные	Несанкционированное проникновение в систему	Предупреждение	Идентификация, аутентификация и подтверждение прав пользователей (авторизация) при доступе в систему Управление конфигурацией системы (например, подключением оборудования и внешними соединениями) Управление пользователями
		Обнаружение	Аудит функционирования системы
	Проникновение в систему, используя известные дефекты протоколов (например, протокола IP)	Предупреждение	Использование межсетевых экранов (фильтрация) Контроль доступа к системным ресурсам Ограничение доступа к программам или сервисам, реализующим уязвимые протоколы
		Обнаружение	Аудит функционирования системы
	Нарушение безопасности системы вследствие несанкционированной замены системной программы	Предупреждение	Контроль доступа к библиотеке системных программ Управление функционированием (разработка документации по использованию системных программ)
		Обнаружение	Аудит доступа к библиотеке программ
		Реагирование	Резервное копирование программ

Окончание таблицы Б.1

Активы	Угрозы	Цели безопасности	
Системные службы и данные	Обслуживание прекращено из-за разрушения системной программы	Предупреждение	Дублирование библиотеки системных программ Контроль носителей программ и эксплуатации программ
	Несанкционированная системная операция	Предупреждение	Управление правами на выполнение операций Управление эксплуатацией (ограничения выполнения операций)
		Обнаружение	Аудит эксплуатации
Информационное оборудование	Повреждение или изъятие	Предупреждение	Дублирование Управление доступом в помещение, где расположено оборудование Управление конфигурацией оборудования в период хранения
	Отключение питания	Предупреждение	Использование резервных источников электропитания Использование источников бесперебойного питания
		Реагирование	Возобновление электропитания

Б.8 Примеры функциональных требований безопасности

Данный подраздел в качестве примера идентифицирует функции безопасности и функциональные компоненты, описанные в ГОСТ Р ИСО/МЭК 15408-2, которые могут быть использованы для формулирования соответствующих ФТБ.

Функции безопасности объединены в следующие группы:

- идентификация и аутентификация;
- управление доступом;
- аудит;
- целостность;
- доступность;
- приватность;
- обмен данными.

Б.8.1 Требования идентификации и аутентификации

В таблице Б.2 приведены требования идентификации и аутентификации.

Таблица Б.2 — Функциональные компоненты для требований идентификации и аутентификации

Требования безопасности		Функциональные компоненты
Управление доступом в систему (регистрацией)	Идентификация пользователей	FIA_UID.1–2
	Аутентификация пользователей	FIA_UAU.1–2
	Ограничение числа неудачных входов в систему	FIA_AFL.1
	Доверенный маршрут для входа в систему	FTP_TRP.1
	Управление доступом по времени и местоположению	FTA_TSE.1
Выбор паролей	Управление выбором сгенерированных пользователями паролей (например, минимальная длина, фильтры пароля, история пароля)	FIA_SOS.1
	Автоматическая генерация пароля ОО	FIA_SOS.2
	Окончание действия пароля	FMT_SAE.1

Окончание таблицы Б.2

Требования безопасности		Функциональные компоненты
Защита аутентификационных данных	Скрытие пароля во время его ввода	FIA_UAU.7
	Защита от несанкционированной модификации и наблюдения	FMT_MTD.1
	Защита от повторной передачи	FPT_RPL.1
	Защита от копирования и подделки	FIA_UAU.3
	Защита от повторного использования аутентификационных данных (например, одноразовое использование пароля)	FIA_UAU.4
	Защищенный маршрут для изменения пароля	FTP_TRP.1
Блокирование сеанса	Блокирование вследствие бездействия пользователя	FTA_SSL.1
	Блокирование по запросу пользователя	FTA_SSL.2
	Завершение вследствие бездействия пользователя	FTA_SSL.3
Учетные записи и профили пользователей	Управление созданием, удалением и использованием учетных записей пользователя	FMT_MTD.1
	Определение атрибутов безопасности пользователя, содержащихся в его профиле	FIA_ATD.1
	Управление модификацией профилей пользователя (то есть атрибутами безопасности пользователя)	FMT_MTD.1

Б.8.2 Требования управления доступом

В таблице Б.3 приведены требования управления доступом.

Таблица Б.3 — Функциональные компоненты для требований управления доступом

Требования безопасности		Функциональные компоненты
Дискреционное управление доступом	Область действия политики безопасности (объекты, субъекты и действия, охватываемые политикой)	FDP_ACC.1–2
	Правила управления доступом субъектов к объектам	FDP_ACF.1
	Отмена прав в соответствии с политикой дискреционного управления доступом	FDP_ACF.1
Управление, основанное на атрибутах дискреционного управления доступом	Изменение прав доступа к объекту	FMT_MSA.1
	Задание атрибутов по умолчанию для вновь создаваемых объектов	FMT_MSA.3
	Изменение владельца объекта	FMT_MSA.1
	Изменение принадлежности к группе пользователей	FMT_MSA.1
Мандатное управление доступом	Область действия политики безопасности (объекты, субъекты и действия, охватываемые политикой)	FDP_IFC.1–2
	Правила управления доступом/информационными потоками	FDP_IFC.2
	Отмена прав в соответствии с политикой мандатного управления доступом	FDP_IFF.7–8
	Ограничение скрытых каналов	FDP_IFF.3–6
Управление, основанное на атрибутах мандатного управления доступом	Изменение меток объекта	FMT_MSA.1

Окончание таблицы Б.3

Требования безопасности		Функциональные компоненты
Управление, основанное на атрибутах мандатного управления доступом	Задание меток по умолчанию для вновь создаваемых объектов	FMT_MSA.3
	Изменение разрешений пользователям	FMT_MSA.1
	Выбор разрешения на установление сеанса связи при входе в систему	FTA_LSA.1
Экспорт/импорт	Импорт немаркированных данных	FDP_ITC.1
	Экспорт с использованием каналов/устройств связи	FDP_ETC.1–2
	Маркировка отпечатанных выходных данных	FDP_ETC.2
Информационные метки	Ограничения на значения информационных меток	FDP_IFF.2.3
	Правила, управляющие «плавающими» метками	FDP_IFF.2.3
Повторное использование объекта	Защита остаточной информации в файлах, памяти и т. д.	FDP_RIP.1–2
Ролевое управление доступом	Область действия политики безопасности (на основе ролей, операций)	FDP_ACC.1–2
	Правила контроля выполнения операций	FDP_ACF.1
	Идентификация ролей	FMT_SMR.1–2
	Осуществление управления доступом на основе разделения действий по доступу между несколькими субъектами	FDP_ACF.1 FMT_SMR.2.3
Управление на основе атрибутов ролей	Управление полномочиями/авторизацией пользователей	FMT_MSA.1
	Изменение возможностей ролей	FMT_MSA.1
	Изменение ролей пользователей	FMT_MSA.1
Управление доступом на основе межсетевого экрана	Представление информационного потока в виде субъект-объект (например, на основе адресов и портов источника/адресата)	FDP_IFC.1–2 FDP_IFF.1
	Представление информационного потока по отношению к сеансу связи (предполагает использование proxy-серверов)	FTA_TSE.1

Б.8.3 Требования аудита

В таблице Б.4 приведены требования аудита.

Таблица Б.4 — Функциональные компоненты для требований аудита

Требования безопасности		Функциональные компоненты
События аудита	Спецификация подлежащих аудиту событий и информации, подлежащей регистрации	FAU_GEN.1
	Управление выбором подлежащих аудиту событий	FMT_MTD.1
	Обоснование выбора подлежащих аудиту событий	FAU_SEL.1
	Учет действий отдельных пользователей (после получения доступа в систему)	FAU_GEN.2
Обнаружение вторжений и ответная реакция	Генерация сигнала нарушения и ответная реакция на неизбежное нарушение безопасности	FAU_ARP.1
	Определение правил, событий, последовательности событий или моделей (шаблонов), по которым можно предположить о возможности нарушения безопасности	FAU_SAA.1–4

Окончание таблицы Б.4

Требования безопасности		Функциональные компоненты
Защита журнала аудита	Защита от потери данных, например, при переполнении журнала аудита, прерывании функционирования	FAU_STG.2–4
	Защита от несанкционированного доступа к данным аудита	FAU_STG.1
Анализ журнала аудита	Использование инструментальных средств анализа журналов аудита	FAU_SAR.1–3

Б.8.4 Требования целостности

В таблице Б.5 приведены требования целостности (включая данные аутентификации).

Таблица Б.5 — Функциональные компоненты для требований целостности

Требования безопасности		Функциональные компоненты
Целостность данных	Обнаружение ошибок в хранимых данных	FDP_SDI.1
	Генерация и верификация значений контрольных сумм, односторонних хэш-функций, дайджестов сообщений и т. д.	FDP_DAU.1
	Откат транзакций (например, для баз данных)	FDP_ROL.1
Целостность ОО	Обнаружение несанкционированных изменений	FPT_PHP.1–2
	Противодействие несанкционированным изменениям	FPT_PHP.3

Б.8.5 Требования доступности

В таблице Б.6 приведены требования доступности.

Таблица Б.6 — Функциональные компоненты для требований доступности

Требования безопасности		Функциональные компоненты
Использование ресурсов	Введение ограничений (квот) на использование общих ресурсов отдельными пользователями	FRU_RSA.1–2
	Ограничение числа сеансов, открываемых одним пользователем	FTA_MCS.1–2
Обработка ошибок	Поддержание функционирования ОО в случае отказа (отказоустойчивость)	FRU_FLT.1–2
	Обнаружение ошибки	FPT_TST.1
	Устранение ошибки	FPT_RCV.1
Планирование	Планирование действий/процессов согласно установленным приоритетам обслуживания	FRU_PRS.1–2

Б.8.6 Требования приватности

В таблице Б.7 приведены требования приватности.

Таблица Б.7 — Функциональные компоненты для требований приватности

Требования безопасности		Функциональные компоненты
Приватность идентификационной информации пользователей	Защита от раскрытия идентификационной информации пользователя при использовании им сервисов или ресурсов	FPR_ANO.1

Окончание таблицы Б.7

Требования безопасности		Функциональные компоненты
Приватность идентификационной информации пользователей	Анонимное, но подотчетное использование сервисов или ресурсов путем применения псевдонимов пользователей	FPR_PSE.1
Приватность использования ресурсов/сервисов	Защита от раскрытия фактов использования конкретным пользователем определенных сервисов или ресурсов	FPR_UNL.1
	Скрытное использование определенных сервисов или ресурсов	FPR_UNO.1

Б.8.7 Требования обмена данными

В таблице Б.8 приведены требования обмена данными.

Таблица Б.8 — Функциональные компоненты для требований обмена данными

Требования безопасности		Функциональные компоненты
Конфиденциальность обмена данными	Пользовательские данные	FDP_UCT.1
	Критичные по безопасности данные (например, ключи и пароли)	FPT_ITC.1
Целостность передаваемых данных	Пользовательские данные	FDP_UIT.1–3
	Критичные по безопасности данные (например, ключи и пароли)	FPT_ITI.1–2
Невозможность отрицания фактов обмена информацией	Доказательство отправления передаваемой информации	FCO_NRO.1–2
	Доказательство получения передаваемой информации	FCO_NRR.1–2

Библиография

[1] Перечень профилей защиты на портале Common Criteria, commoncriteriaportal.org

[2] ISO/IEC 15292, Information technology — Security techniques — Protection Profile registration procedures

[3] Методический документ ФСТЭК России «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» (ИТ.СКН.П4.ПЗ), 2014

[4] Методический документ ФСТЭК России «Профиль защиты средств контроля подключения съемных машинных носителей информации пятого класса защиты» (ИТ.СКН.П5.ПЗ), 2014

[5] Руководящий документ ФСТЭК (Гостехкомиссии) России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (РД БИТ), 2002

[6] Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. Приказом ФСТЭК России 11.02.2013 № 17)

[7] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Приказом ФСТЭК России 18.02.2013 № 21)

[8] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утв. Приказом ФСТЭК России от 14.03.2014 № 31)

[9] Руководящий документ ФСТЭК (Гостехкомиссии) России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей» (РД НДВ), 1999

УДК 351.864.1:004:006:354 ОКС 35.240 П80

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

БЗ 10—2017/56

Редактор *О.А. Стояновская*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Половой*

Сдано в набор 09.08.2017. Подписано в печать 15.09.2017. Формат 60 × 84 1/8 Гарнитура Ариал.
Усл. печ. л. 11,63. Уч.-изд. л. 10.52. Тираж 25 экз. Зак. 1658.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Набрано в ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11
www.jurisizdat.ru y-book@mail.ru

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001, Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru