ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК ТО 15446— 2008

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
(IDT)

Издание официальное

БЗ 12—2008/540

Москва
Стандартинформ
2010

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ») на основе собственного аутентичного перевода стандарта, указанного в пункте 5

2 ВНЕСЕН Управлением технического регулирования и стандартизации Федерального агентства по техническому регулированию и метрологии

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 526-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК ТО 15446:2004 «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»).

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

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

Содержание

Введение

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

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

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

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

c) цели безопасности ОО, основанные на описании среды 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 и обеспечить поддержание политики безопасности организации, в интересах которой ведется разработка ПЗ;

d) функциональные требования безопасности и требования доверия к безопасности, направленные на решение проблемы безопасности в соответствии с описанием среды безопасности ОО и целями безопасности для ОО и ИТ-среды. Функциональные требования безопасности выражают то, что должно выполняться ОО и ИТ-средой для удовлетворения целей безопасности. Требования доверия к безопасности определяют степень уверенности в правильности реализации функций безопасности ОО;

e) обоснование функциональных требований и требований доверия к безопасности, являющихся надлежащими для удовлетворения сформулированной потребности в безопасности. Посредством целей безопасности должно быть показано, что необходимо сделать для решения проблем безопасности, имеющихся в описании среды безопасности ОО. Функциональные требования безопасности и требования доверия к безопасности должны соответствовать целям безопасности.

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

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

b) дополнительный раздел, который включается в ЗБ в случаях, если утверждается о соответствии ЗБ одному или более ПЗ;

c) дополнительные свидетельства в разделе «Обоснование», устанавливающие, что краткая спецификация ОО обеспечивает соответствие требований безопасности, а любые утверждения о соответствии ПЗ — действительны.

Профиль защиты может использоваться для определения типового набора требований безопасности, которым должны соответствовать один или более продуктов или которым должны соответствовать системы ИТ, предназначенные для использования в определенных целях. Профиль защиты может применяться к определенному виду продуктов (например, операционным системам, системам управления базами данных, смарт-картам, межсетевым экранам и т.д.) или к совокупности продуктов, образующих систему (например, к инфраструктуре открытых ключей, виртуальным частным сетям).

Поставщики продукта ИТ в соответствии с потребностями безопасности, сформулированными в ПЗ, могут разработать ЗБ, которое будет демонстрировать то, как их продукт ИТ соответствует потребностям безопасности. Тем не менее, соответствие задания по безопасности профилю защиты не является обязательным; например, в ЗБ могут быть определены функции безопасности, заявляемые разработчиком продукта ИТ и представляющие собой основу для оценки продукта ИТ.

Также в ПЗ могут быть определены требования безопасности для конкретной системы ИТ. В этом случае ЗБ разрабатывается на основе ПЗ. Таким образом, ПЗ и ЗБ могут использоваться как средства взаимодействия между организацией, осуществляющей руководство разработкой системы, организацией, заинтересованной в этой системе, и организацией, ответственной за создание системы (далее — разработчик). Содержание ПЗ и ЗБ может быть согласовано между данными сторонами. Оценка конкретной системы ИТ на соответствие ЗБ, которое в свою очередь соответствует ПЗ, может являться частью процесса приемки системы ИТ.

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 — 2009 — 10— 01

1 Область применения

Настоящий стандарт представляет собой руководство по разработке профилей защиты и заданий по безопасности продуктов и систем ИТ в соответствии с комплексом стандартов ИСО/МЭК 15408 (общие критерии).

Руководство предназначено для разработчиков и оценщиков профилей защиты (ПЗ) и заданий по безопасности (ЗБ), а также может представлять интерес для пользователей ПЗ и ЗБ, позволяя им понять, чем руководствовались авторы ПЗ и ЗБ при их разработке, и на какие части ПЗ и ЗБ следует обратить особое внимание.

Предполагается, что пользователи настоящего стандарта хорошо знакомы с требованиями ИСО/МЭК 15408-1 и, в частности, с приложениями В и С к нему, в которых приведено описание ПЗ и ЗБ. Авторам ПЗ и ЗБ, конечно, следует быть хорошо знакомыми с другими стандартами комплекса ИСО/МЭК 15408, включая введение, например, с парадигмой функциональных требований, описанной в ИСО/МЭК 15408-2 (подраздел 1.3).

Настоящий стандарт представляет собой информационный технический отчет ИСО, предназначенный для использования только в качестве руководства. По своему содержанию и структуре его не следует рассматривать как стандарт для оценки ПЗ и ЗБ. Предполагается, что настоящий стандарт полностью соответствует ИСО/МЭК 15408; тем не менее, в случае любого несоответствия между настоящим стандартом и ИСО/МЭК 15408 последнему в качестве нормативного следует отдавать предпочтение.

В настоящем стандарте не рассматриваются такие вопросы, как регистрация ПЗ и связанные с этим задачи — обращение с защищаемой интеллектуальной собственностью (например, патентами) в ПЗ. Информацию по регистрации ПЗ см. в [1].

2 Нормативные ссылки

В настоящем документе использованы ссылки на следующие международные стандарты:

ИСО/МЭК 2382-8:1998 Информационная технология — Словарь — Часть 8: Безопасность

ИСО/МЭК 15408-1 — 2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ИСО/МЭК 15408-2 — 2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ИСО/МЭК 15408-3 — 2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. — Часть 3. Требования доверия к безопасности

Издание официальное

3 Термины и определения

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

4 Сокращения

В настоящем стандарте применяются сокращения, приведенные в ИСО/МЭК 15408-1, подраздел 2.3, а также следующие сокращения:

ПБОр (OSP) — политика безопасности организации;
СУБД (DBMS) — система управления базами данных;
ТДБ (SAR) — требование доверия к безопасности;
ФТБ (SFR) — функциональное требование безопасности;
ЗП (RFP) — запрос предложения;
КСО (TSS) — краткая спецификация ОО;
ТДС (TTP) — третья доверенная сторона.

5 Цель

Настоящий стандарт представляет собой детальное руководство по разработке различных частей ПЗ или ЗБ и дает исчерпывающее представление об их взаимосвязи. Наиболее важные аспекты настоящего стандарта представлены в приложении А в виде памятки (или резюме), что в значительной степени облегчает знакомство и работу со стандартом.

В остальных приложениях приводятся примеры, иллюстрирующие применение настоящего стандарта.

Разделы 1—4 содержат вводные и ссылочные материалы.

Раздел 5 содержит цели и направленности настоящего стандарта.

Раздел 6 содержит краткий обзор ПЗ и ЗБ, который включает в себя оглавления и отображает содержание, а также потенциальных пользователей различных частей ПЗ или ЗБ. Данный раздел содержит, а также комментирует соотношение между ПЗ и ЗБ и проблемы, связанные с процессом их разработки.

В разделе 7 более глубоко рассматриваются содержащие описание части ПЗ и ЗБ, включая введение ПЗ и ЗБ, описание объекта оценки (в большей степени ориентированные на пользователей), а также замечания по применению ПЗ (в большей степени ориентированные на авторов ЗБ и разработчиков ОО).

Разделы 8—13 придерживаются той структуры ПЗ и ЗБ, которая установлена в ИСО/МЭК 15408-1 (см. приложение В, рисунок В.1, приложение С, рисунок С.1).

Раздел 8 представляет собой руководство по определению среды безопасности ОО в ПЗ и ЗБ в виде исходных «потребностей в безопасности» ОО.

Раздел 9 представляет собой руководство по определению и спецификации целей безопасности в ПЗ или ЗБ в соответствии со сформулированными ранее исходными «потребностями в безопасности». Оба этих раздела представляют интерес не только для авторов ПЗ и ЗБ, но также и для других лиц — пользователей ПЗ и ЗБ.

Раздел 10 представляет собой руководство по выбору и спецификации требований безопасности информационных технологий в ПЗ. В данном разделе подробно описывается использование функциональных компонентов и компонентов доверия к безопасности в соответствии с требованиями стандартов серии ИСО/МЭК 15408, а также компонентов, не предусмотренных стандартами серии ИСО/МЭК 15408, для обеспечения более точного определения требований безопасности ИТ.

Разделы 11 и 12 представляют собой руководство по разработке ЗБ в части краткой спецификации ОО и утверждений о соответствии ПЗ. Разделы 10—13 будут в основном представлять интерес для авторов и оценщиков ПЗ и ЗБ.

Раздел 13 представляет собой руководство по составлению и представлению разделов «Обоснование» в ПЗ и ЗБ.

В разделе 14 рассматриваются проблемы разработки ПЗ и ЗБ для сложных ОО, то есть ОО, состоящих из двух или более ОО-компонентов, для каждого из которых имеются собственные ПЗ и ЗБ.

Раздел 15 представляет собой руководство по формированию функциональных пакетов и пакетов доверия к безопасности, определенных таким образом, чтобы эти пакеты можно было многократно использовать при разработке различных ПЗ и ЗБ. Пакет при этом рассматривается как потенциально полезный инструмент, предназначенный для облегчения процесса разработки ПЗ и ЗБ.

Как упоминалось выше, в приложении А руководство вкратце представлено в виде инструкции.

Примеры угроз, политики безопасности организации, предположений и целей безопасности представлены в приложении В, которое также устанавливает соответствие между общими функциональными требованиями и соответствующими функциональными компонентами из стандартов серии ИСО/МЭК 15408. Предполагается, что эти примеры являются достаточно широкомасштабными, но не исчерпывающими.

Приложение С представляет собой руководство, имеющее отношение к ПЗ и ЗБ для ОО, которые реализуют криптографические функциональные возможности.

Возможности применения настоящего стандарта при разработке ПЗ и ЗБ для различных типов ОО представлены в приложениях D — F. Так, в приложении D рассмотрена возможность использования настоящего стандарта при разработке ПЗ и ЗБ для межсетевых экранов, в приложении Е — для СУБД, в котором подчеркивается особая важность решения вопросов, связанных с ИТ-средой. В приложении F рассматриваются вопросы, связанные с разработкой ПЗ для третьей доверенной стороны (ТДС).

6 Краткий обзор профилей защиты и заданий по безопасности

6.1 Введение

В настоящем разделе приводится краткий обзор и содержание ПЗ и ЗБ. Рассматриваются взаимосвязи между ПЗ и ЗБ и процесс их разработки (см. также ИСО/МЭК 15408-1, приложения В и С).

6.2 Содержание профилей защиты и заданий по безопасности

Требуемое содержание ПЗ и ЗБ приведено в ИСО/МЭК 15408-1, приложение В. Пример содержания ПЗ представлен ниже:

1 Введение ПЗ
1.1 Идентификация ПЗ
1.2 Аннотация ПЗ
2 Описание ОО
3 Среда безопасности ОО
3.1 Предположения безопасности
3.2 Угрозы
3.3 Политика безопасности организации
4 Цели безопасности
4.1 Цели безопасности для ОО
4.2 Цели безопасности для среды
5 Требования безопасности ИТ
5.1 Функциональные требования безопасности ОО
5.2 Требования доверия к безопасности ОО
5.3 Требования безопасности для ИТ-среды
6 Замечания по применению
7 Обоснование
7.1 Обоснование целей безопасности
7.2 Обоснование требований безопасности.

В разделе «Введение ПЗ» идентифицируется ПЗ и приводится его аннотация в форме, наиболее подходящей для включения в каталоги и реестры ПЗ. Данный раздел ПЗ более подробно рассматривается в разделе 7 настоящего стандарта.

В раздел «Описание ОО» включают сопроводительную информацию об ОО (или типе ОО), предназначенную для пояснения его назначения и требований безопасности.

В раздел ПЗ «Среда безопасности ОО» включают описание аспектов среды безопасности ОО, которые должны учитываться для объекта оценки, в частности — детальное описание предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), и ПБОр, которой должен соответствовать ОО. Этот раздел ПЗ более подробно рассмотрен в разделе 8.

В раздел ПЗ «Цели безопасности» включают краткое изложение предполагаемой реакции на аспекты среды безопасности как с точки зрения целей безопасности, которые должны быть удовлетворены ОО, так и с точки зрения целей безопасности, которые должны быть удовлетворены ИТ- и не ИТ-мерами в пределах среды ОО. Данный раздел ПЗ более подробно рассмотрен в разделе 9.

В раздел ПЗ «Требования безопасности ИТ» включают функциональные требования безопасности ОО, требования доверия к безопасности, а также требования безопасности программного, программно-

аппаратного и аппаратного обеспечения ИТ-среды ОО. Требования безопасности ИТ должны быть определены путем использования, где возможно, функциональных компонентов и компонентов доверия к безопасности в соответствии с ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3. Раздел ПЗ «Требования безопасности ИТ» более подробно рассмотрен в разделе 10.

В раздел ПЗ «Замечания по применению» допускается включать любую дополнительную информацию, которую разработчик ПЗ считает полезной. Отметим, что замечания по применению могут быть распределены по соответствующим разделам ПЗ. Раздел ПЗ «Замечания по применению» более подробно рассмотрен в разделе 7.

В разделе ПЗ «Обоснование» демонстрируется то, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ и соответствующий ОО учитывает идентифицированные аспекты среды безопасности. Раздел ПЗ «Обоснование» более подробно рассмотрен в разделе 12.

Существует также целый ряд необязательных разделов и подразделов, которые могут включаться в ПЗ. Возможны разные уровни детализации некоторых подразделов. Раздел «Обоснование» может быть оформлен в виде отдельного документа. На практике дополнительные разделы могут быть необходимы для предоставления полезной информации, например:

a) раздел «Введение ПЗ» может включать в себя подраздел, описывающий организацию ПЗ, а также ссылки на другие ПЗ и другие документы;

b) раздел «Среда безопасности ОО» может включать в себя отдельные подразделы для различных доменов в ИТ-среде для ОО;

c) раздел «Требования безопасности ИТ» может быть расширен за счет включения, где необходимо, требований безопасности для не ИТ-среды.

В случае если подраздел не используется (например, политика безопасности организации, требования безопасности ИТ для среды ОО), необходимо включить в ПЗ соответствующее пояснение.

Содержание ЗБ приведено в ИСО/МЭК 15408-1, приложение С. Пример содержания ЗБ представлен в таблице 2.

В разделе «Введение ЗБ» идентифицируется ЗБ и ОО (включая номер версии) и приводится аннотация ЗБ в форме, наиболее подходящей для включения в перечень оцененных (сертифицированных) продуктов ИТ. Раздел «Введение ЗБ» более подробно рассмотрен в разделе 7.

В раздел ЗБ «Описание ОО» включают сопроводительную информацию об ОО, предназначенную для пояснения его назначения и требований безопасности. Раздел ЗБ «Описание ОО» должен также включать в себя описание конфигурации, в которой ОО подлежит оценке. Раздел ЗБ «Описание ОО» более подробно рассмотрен в разделе 7.

В раздел ЗБ «Среда безопасности ОО» включают описание аспектов среды безопасности ОО, которые должны учитываться объектом оценки, в частности, предположений безопасности, определяющих границы среды безопасности, угроз активам, требующим защиты (включая описание этих активов), ПБОр, которой должен соответствовать ОО. Раздел ЗБ «Среда безопасности ОО» более подробно рассмотрен в разделе 8.

Пример содержания задания по безопасности представлен ниже:

1.1 Идентификация ЗБ
1.2 Аннотация ЗБ
2 Описание ОО
3 Среда безопасности ОО
3.1 Предположения безопасности
3.2 Угрозы
3.3 Политика безопасности организации
4 Цели безопасности
4.1 Цели безопасности для ОО
4.2 Цели безопасности для среды ОО
5 Требования безопасности ИТ
5.1 Функциональные требования безопасности ОО
5.2 Требования доверия к безопасности ОО
5.3 Требования безопасности для ИТ-среды
6 Краткая спецификация ОО
6.1 Функции безопасности ОО
6.2 Меры обеспечения доверия к безопасности

7 Утверждения о соответствии ПЗ
7.1 Ссылка на ПЗ
7.2 Уточнение ПЗ
7.3 Дополнение ПЗ
8 Обоснование
8.1 Обоснование целей безопасности
8.2 Обоснование требований безопасности
8.3 Обоснование краткой спецификации ОО
8.4 Обоснование утверждений о соответствии ПЗ.

В раздел ЗБ «Цели безопасности» включают краткое изложение предполагаемой реакции на аспекты среды безопасности как с точки зрения целей безопасности, которые должны соответствовать ОО, так и с точки зрения целей безопасности, которые должны соответствовать ИТ- и не ИТ-мерам в пределах среды ОО. Данный раздел ЗБ более подробно рассмотрен в разделе 9.

В раздел ЗБ «Требования безопасности ИТ» включают функциональные требования безопасности ОО, требования доверия к безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды ОО. Требования безопасности ИТ должны быть определены путем использования, где это возможно, функциональных компонентов и компонентов доверия к безопасности в соответствии с ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3. Раздел ЗБ «Требования безопасности ИТ» более подробно рассмотрен в разделе 10.

В раздел «Краткая спецификация ОО» включают описание функций безопасности ИТ, реализуемых ОО и соответствующих специфицированным функциональным требованиям безопасности, а также любых мер доверия к безопасности, соответствующих специфицированным требованиям доверия к безопасности. Раздел ЗБ «Краткая спецификация ОО» более подробно рассмотрен в разделе 11.

В разделе «Утверждения о соответствии ПЗ» идентифицируются ПЗ, о соответствии которым заявляется в ЗБ, а также любые дополнения или уточнения целей или требований из этих ПЗ. Раздел ЗБ «Утверждения о соответствии ПЗ» более подробно рассмотрен в разделе 13.

В разделе ЗБ «Обоснование» демонстрируют, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, соответствующий ОО учитывает определенные аспекты среды безопасности ИТ и функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО. Раздел ЗБ «Обоснование» более подробно рассмотрен в разделе 13.

Как и для ПЗ (см. 6.1) при разработке ЗБ допускается отступать от вышеуказанной структуры путем включения дополнительных и исключения необязательных разделов (и/или подразделов) ЗБ.

6.3 Взаимосвязь между профилями защиты и заданиями по безопасности

При сопоставлении таблиц 1 и 2 становится очевидной взаимосвязь между ПЗ и ЗБ вследствие высокой степени общности данных документов, в особенности разделов «Среда безопасности ОО», «Цели безопасности», «Требования безопасности ИТ» и, частично, — раздела «Обоснование». Если в ЗБ утверждается о соответствии ПЗ и при этом не специфицируются дополнительные функциональные требования и требования доверия к безопасности, то содержание упомянутых выше разделов ЗБ может быть идентично содержанию соответствующих разделов ПЗ. В таких случаях рекомендуется ссылка в ЗБ на содержание ПЗ с добавлением (там, где необходимо) деталей, отличающих ЗБ от ПЗ.

Следующие разделы ЗБ не имеют аналогов в ПЗ и, таким образом, являются специфичными для ЗБ:

a) раздел «Краткая спецификация ОО» — включает в себя функции безопасности ИТ, механизмы и способы обеспечения безопасности, а также меры доверия к безопасности;

b) раздел «Утверждения о соответствии ПЗ» — мотивирует и детализирует требования соответствия ПЗ;

c) подразделы раздела «Обоснование» — демонстрируют адекватность функций безопасности ИТ и мер доверия к безопасности требованиям безопасности ОО.

6.4 Учет информационных потребностей потенциальных пользователей профилей защиты и заданий по безопасности

В ПЗ и ЗБ необходимо учитывать следующие информационные потребности потенциальных пользователей этих документов:

- потребители (дистрибуторы и покупатели) нуждаются в информации, дающей общее представление о том, как ОО решает проблемы безопасности;

- разработчики нуждаются в однозначном понимании требований безопасности с тем, чтобы создавать (формировать) соответствующие ОО;

- оценщики нуждаются в информации, которая будет мотивировать правильность и эффективность ПЗ или ЗБ с технической точки зрения.

Структура ПЗ и ЗБ должна быть разработана так, чтобы разные разделы содержали информацию, предназначенную для разных категорий пользователей.

Разделы «Введение ПЗ и ЗБ», «Описание ОО» и «Среда безопасности ОО» предназначены, прежде всего, для потребителей. Раздел «Цели безопасности» также может быть изложен в первую очередь для потребителей. Вместе с тем следует помнить, что и разработчики ОО должны принять во внимание информацию, находящуюся в разделах «Среда безопасности ОО» и «Цели безопасности».

Раздел «Требования безопасности ИТ», относящийся к ПЗ, предназначен прежде всего для разработчиков ОО, хотя информация, содержащаяся в этом разделе, вероятно, также будет интересна потребителям. Раздел ЗБ «Краткая спецификация ОО» предназначен прежде всего для оценщиков и потребителей. Если последние два раздела ПЗ не содержат достаточного количества информации, то в них необходимо поместить ссылку на другие разделы (подразделы) ПЗ (например, «Аннотация ПЗ») и документы, необходимые для полного и точного понимания представленных требований безопасности ИТ.

В раздел ПЗ и ЗБ «Обоснование» включают информацию, предназначенную преимущественно для оценщиков. В то же время оценщикам целесообразно ознакомиться со всеми разделами ПЗ и ЗБ.

6.5 Процесс разработки профилей защиты и заданий по безопасности

Анализ приложений В и С ИСО/МЭК 15408-1 и разделов 3 — 5 ИСО/МЭК 15408-3 показывает, что разработка ПЗ и ЗБ осуществляется в следующей (нисходящей) последовательности:

a) идентификация аспектов среды безопасности;

b) определение целей безопасности, учитывающих идентифицированные аспекты среды безопасности;

c) формирование требований безопасности ИТ, направленных на удовлетворение целей безопасности.

В общем случае, хотя и с учетом данной последовательности действий, процесс разработки ПЗ и ЗБ носит итеративный характер. Например, формирование требований безопасности может способствовать корректировке целей безопасности или даже потребностей в безопасности. В целом, 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 «Обоснования» ПЗ и ЗБ. При этом только когда все проблемы формирования «Обоснования» ПЗ и ЗБ решены, процесс разработки ПЗ и ЗБ можно считать завершенным.

Процесс разработки ПЗ и ЗБ может также включать внесение изменений в документ с тем, чтобы отразить изменения условий применения, например:

a) идентификацию новых угроз;

b) изменение ПБОр;

c) связанные со стоимостными и временными ограничениями изменения в разделении ответственности обеспечения безопасности, возлагаемой соответственно на ОО и среду ОО;

d) корректировку требований безопасности ИТ, функций безопасности и/или мер доверия к безопасности, связанную с изменениями в технологии и затратах на разработку ОО.

Также возможно (например, для существующего продукта ИТ), что разработчики ПЗ и ЗБ имеют четкое представление относительно ФТБ, которым соответствует ОО (даже если эти требования не были выражены в стандартах серии ИСО/МЭК 15408). В таких случаях определение аспектов среды безопасности и целей безопасности будет осуществляться, исходя из этих ФТБ. Процесс разработки ПЗ и ЗБ в таком случае будет «восходящим».

6.6 Семейства профилей защиты

Семейство ПЗ представляет собой совокупность тесно связанных ПЗ, которые обычно относятся к одному и тому же типу продукта или системы ИТ (например, операционная система, межсетевой экран и т.д.). Разработка ПЗ может, таким образом, рассматриваться как часть процесса разработки семейства ПЗ. Разработка семейств ПЗ может идти по следующим направлениям:

a) разработка совокупности иерархически связанных ПЗ для одного и того же типа ОО (ПЗ можно считать иерархическим по отношению к другому ПЗ семейства, если он включает в себя все требования безопасности ИТ, специфицированные в другом ПЗ);

b) разработка совокупности ПЗ, каждый из которых относится к различным компонентам системы ИТ, например, семейство «смарт-карты» могло бы включать в себя ПЗ для платы интегральной схемы, ПЗ для операционной системы, ПЗ для приложения, ПЗ считывателя смарт-карт и т.д.

Если семейство ПЗ относится к конкретному типу ОО, важно, чтобы было четкое различие между различными членами семейства. Другими словами, должны быть четкие различия в требованиях безопасности ОО. Это связано с тем, что ПЗ должен, по крайней мере, отличаться целями безопасности, которые определяют выбор требований безопасности ИТ. В качестве примера можно рассмотреть случай, когда два ПЗ специфицируют одну и ту же совокупность ФТБ, но разные ТДБ. Допускается мотивировать более низкое требование безопасности возрастанием безопасности среды ОО. Такие различия должны быть отражены в целях безопасности. Там же, где семейство ПЗ применяется к различным компонентам системы ИТ (в конкретной или предполагаемой среде), должны быть четко определены ПЗ, включенные в семейство (см. также раздел 14, в котором рассматриваются вопросы разработки ПЗ для компонентов системы ИТ).

7 Описательные разделы профилей защиты и заданий по безопасности

7.1 Введение

Настоящий раздел содержит рекомендации по формированию следующих описательных разделов ПЗ и ЗБ:

a) «Введение ПЗ и ЗБ»;

b) «Описание ОО» в ПЗ и ЗБ;

c) «Замечания по применению в ПЗ».

7.2 Описательные части профиля защиты и задания по безопасности

7.2.1 Раздел «Введение»

7.2.1.1 Подраздел «Идентификация»

Назначение данного подраздела состоит в предоставлении информации для идентификации ПЗ, например, в целях последующей регистрации ПЗ. Идентификация, как минимум, должна включать в себя название ПЗ и идентификатор, который является уникальным для данной версии ПЗ. В подраздел «Идентификация ПЗ» также целесообразно включить следующую информацию:

a) ключевые слова;

b) оценочный уровень доверия (ОУД), если применяется в ПЗ;

c) утверждение о соответствии версии конкретному стандарту серии ИСО/МЭК 15408;

d) состояние оценки ПЗ.

7.2.1.2 Подраздел «Аннотация»

В соответствии со стандартами серии ИСО/МЭК 15408 подраздел «Аннотация ПЗ» должен быть представлен в форме резюме, используемого также в реестрах и каталогах ПЗ. В данный раздел необходимо включить высокоуровневый обзор проблемы безопасности, которая подлежит решению в ПЗ. Также желателен краткий обзор того, как ПЗ способствует решению проблемы безопасности. Этот обзор должен соответствовать техническому содержанию ПЗ. В случае необходимости «Аннотация ПЗ» может быть расширена до «Резюме для руководителя» или «Резюме для менеджера». Однако если предполагается, что ПЗ будет включен в реестр ПЗ, то соответствующий краткий обзор (обычно один-два параграфа) должен быть сформирован так, чтобы его можно было перенести в реестр.

При формировании раздела ЗБ «Введение» целесообразно руководствоваться рекомендациями по формированию раздела ПЗ «Введение», за исключением того, что:

a) утверждение о соответствии ИСО/МЭК 15408 является необязательным для ЗБ;

b) к ЗБ неприменимы процедуры регистрации ПЗ;

c) может потребоваться идентификация ЗБ, связанных с рассматриваемым ЗБ, если ОО представляет собой составной ОО либо является частью составного ОО.

7.2.2 Раздел «Описание объекта оценки»

В раздел «Описание ОО» ПЗ включают информацию о следующих видах (первые два вида информации — предписаны ИСО/МЭК 15408, два последних — являются необязательными):

a) тип продукта ИТ;

b) основные функциональные возможности ОО;

c) границы ОО (необязательная информация);

d) среда функционирования ОО (необязательная информация).

Описание «основных функциональных возможностей ОО» включает в себя описание функциональных возможностей ОО, а не только характеристик безопасности (в случае, если обеспечение безопасности не является единственным предназначением ОО).

Описание «границ ОО» (необязательное) — это описание того, что включает и чего не включает в себя ОО. При этом ПЗ может оставлять возможность разработчику соответствующего ЗБ установить окончательные границы между ОО и средой ОО. Тем не менее диапазон допустимого выбора таких границ должен быть в явном виде установлен в ПЗ.

Описание «среды функционирования ОО» (необязательное) — это описание того, где функционирует ОО, включая важные предположения, ограничения, накладываемые процессами деятельности, и другие ключевые параметры, важные с точки зрения пользователей ПЗ.

При формировании раздела «Описание ОО» необходимо стремиться к тому, чтобы максимально исключить возможность неправильного понимания пользователями ПЗ и ЗБ предназначения ОО и его возможностей по обеспечению безопасности информации (то есть необходимо исключить те детали описания ОО, которые не представляют интереса в свете предполагаемой оценки ОО).

При формировании раздела ЗБ «Описание ОО» целесообразно руководствоваться рекомендациями по формированию раздела ПЗ «Описание ОО», за исключением того, что «границы ОО» должны быть определены как в части аппаратных и программных компонентов (физические границы), так и в части функциональных характеристик безопасности ОО.

7.2.3 Раздел «Замечания по применению»

Раздел «Замечания по применению» является необязательным. Замечания по применению могут быть оформлены как отдельный раздел ПЗ либо сопровождать различные части ПЗ, например, отдельные требования безопасности ОО. В замечания по применению целесообразно включать сопроводительную информацию, которая может оказаться полезной при проектировании, оценке и эксплуатации ОО. Основное назначение раздела «Замечания по применению» — пояснить, как конкретные требования безопасности необходимо интерпретировать для рассматриваемого ОО, а также предоставить разработчикам ЗБ рекомендации по выполнению операций (выбор, назначение, уточнение) над функциональными компонентами.

Если замечания по применению распределены по всему тексту ПЗ, то в этих случаях их необходимо однозначно идентифицировать как таковые, чтобы пользователь ПЗ интерпретировал их именно как «Замечания по применению», а не как, например, уточнения для ФТБ и ТДБ.

8 Среда безопасности объекта оценки

8.1 Введение

В данном разделе представлены рекомендации по спецификации раздела ПЗ и ЗБ «Среда безопасности ОО». Требования к содержанию этого раздела ПЗ и ЗБ определены в ИСО/МЭК 15408-1, приложение В, подраздел В.2.4 и приложение С, подраздел С.2.4.

Содержание разделов «Среда безопасности ОО» в ПЗ и «Среда безопасности ОО» в ЗБ не имеют серьезных различий.

Цель раздела «Среда безопасности ОО» состоит в определении аспектов безопасности среды ОО (см. рисунок 1).

Рисунок 1 — Определение аспектов среды безопасности объекта оценки

В данном разделе предметом рассмотрения становятся следующие аспекты:

a) предположения относительно среды безопасности ОО;

b) активы, требующие защиты (обычно информация или ресурсы в пределах ИТ-среды или непосредственно ОО), идентифицированные источники угроз и сами угрозы, которые они порождают для активов;

c) ПБОр или правила, которым должен соответствовать ОО.

Следующие разделы ПЗ и ЗБ показывают, как аспекты безопасности среды ОО будут удовлетворяться объектом оценки и его средой. Именно поэтому важно обеспечить ясную и краткую формулировку аспектов безопасности среды ОО.

При определении аспектов среды безопасности следует избегать (где возможно) описания того, как ОО учитывает аспекты безопасности среды. Такой подход позволяет акцентировать внимание пользователя ПЗ и ЗБ на наиболее важных аспектах безопасности среды ОО.

8.2 Идентификация и спецификация предположений безопасности

В соответствии со стандартами серии ИСО/МЭК 15408 в раздел «Среда безопасности ОО» ПЗ и ЗБ необходимо включать перечень предположений относительно среды безопасности ОО или предполагаемого использования ОО.

Для формирования такого перечня необходимо определить характер предположений относительно среды безопасности ОО и ее границы. Например, может потребоваться сформулировать предположения, связанные с тем, что потенциальные угрозы практически не оказывают влияния на безопасность активов среды ОО.

В ПЗ и ЗБ целесообразно включать следующие группы предположений:

a) предположения относительно будущего использования ОО;

b) предположения, связанные с защитой любой части ОО со стороны среды (например, физическая защита);

c) предположения связности [например, межсетевой экран должен быть единственным сетевым соединением между частной (защищаемой) и внешней (потенциально враждебной) сетью];

d) предположения, имеющие отношение к персоналу [например, предполагаемые пользовательские роли, основные обязанности (ответственность) пользователей и степень доверия этим пользователям].

Кроме того, в ПЗ и ЗБ целесообразно включать и другие предположения, оказывающие существенное влияние на содержание ПЗ и ЗБ, например, предположения, определяющие выбор требований доверия к безопасности. Необходимо помнить, что все идентифицированные предположения безопасности должны быть учтены при формировании целей безопасности. Предположения безопасности, которые по какой-либо причине не могут быть учтены при формировании целей безопасности, целесообразно включать в ПЗ и ЗБ в качестве сопроводительной информации.

Чаще всего с первого раза невозможно полностью идентифицировать все предположения. Поэтому предположения могут быть дополнительно идентифицированы на протяжении всего периода разработки ПЗ или ЗБ. В частности, при формировании раздела ПЗ и ЗБ «Обоснование» (например, при демонстрации пригодности целей безопасности для противостояния идентифицированным угрозам) необходимо установить, были ли сделаны предположения, не нашедшие своего отображения в ПЗ и ЗБ.

Наряду с использованием итерационного подхода к идентификации предположений безопасности, необходимо избегать включения в раздел «Среда безопасности ОО» любых предположений, связанных с эффективным использованием конкретных функций безопасности ОО (ФБО), которые идентифицированы в процессе формирования раздела «Обоснование». Соответствующую этим «предположениям» информацию целесообразно включать в ПЗ и ЗБ в виде требований безопасности для не ИТ-среды (см. 10.5.2).

Однако в раздел «Среда безопасности ОО» целесообразно включать следующего вида предположения, имеющие отношение к персоналу: «для ОО определены один или несколько администраторов, в обязанности которых входит обеспечение надлежащей настройки и соответствующего использования ФБО».

Для упрощения осуществления ссылок рекомендуется, чтобы каждое предположение было пронумеровано или имело уникальную метку.

Примеры предположений приведены в приложении В.

8.3 Идентификация и спецификация угроз

8.3.1 Краткий обзор

Согласно ИСО/МЭК 15408-1, приложения В, подраздел В.2.4 необходимо включать в ПЗ и ЗБ описание всех угроз для активов, подлежащих защите. Тем не менее формулировка угроз может быть опущена, если цели безопасности сформулированы, исходя исключительно из ПБОр, то есть формулировка угроз может быть опущена в случае, если аспекты среды безопасности ОО полностью определяются ПБОр и предположениями безопасности.

При этом рекомендуется, чтобы формулировка угроз была включена в ПЗ и ЗБ, поскольку она обеспечивает лучшее понимание аспектов среды безопасности ОО, чем соответствующая им совокупность правил ПБОр. Более того, достаточно опасно полагаться исключительно на ПБОр, так как она не всегда может надлежащим образом отразить текущие угрозы. Если полная совокупность правил ПБОр уже

сформулирована, тем не менее, является целесообразным формулирование угроз с целью максимального облегчения использования ПЗ и отражения более глубокого понимания аспектов среды безопасности ОО.

Важным этапом обеспечения безопасности ОО является анализ рисков, так как, если он не выполнен должным образом, ОО будет не в состоянии обеспечить адекватную защиту активов, в результате чего активы организации могут остаться подверженными неприемлемому уровню риска. Следует отметить, что подробные рекомендации по организации процесса идентификации угроз активам (являющегося одним из самых трудоемких этапов анализа риска организации) в настоящий стандарт не включены. Тем не менее, ниже излагаются общие принципы идентификации угроз.

8.3.2 Идентификация угроз

8.3.2.1 Понятие угрозы

Угрозы характеризуются следующими аспектами: источник угрозы; предполагаемый метод нападения; уязвимости, которые могут быть использованы для нападения (реализации угрозы); и активы, подверженные нападению.

Примечание — Нарушения ПБОр не должны трактоваться как угрозы.

В целях идентификации угроз необходимо выяснить:

a) какие активы требуют защиты;

b) кто или что является источником угрозы;

c) от каких методов нападения или нежелательных событий активы должны быть защищены.

8.3.2.2 Идентификация активов

Активы представляют собой информацию или ресурсы, которые должны быть защищены средствами ОО. Активы имеют определенную ценность для их владельцев (человека или организации), а также (очень часто) — и для источников угроз. Последние могут пытаться, вопреки желаниям и интересам владельцев активов, скомпрометировать их, например, путем нарушения конфиденциальности, целостности и доступности данных активов.

Активы, которые надлежит учесть разработчику ПЗ и ЗБ, могут быть представлены в виде первичных активов организации (например, денежные активы, персонал и репутация организации). Под владельцем активов понимают субъекты, ответственные за сохранность активов в пределах системы ИТ (в которой размещен ОО). Различают владельцев первичных активов (их может быть много) и владельца ОО, а также владельцев информации, хранимой и обрабатываемой ОО. Поэтому в ПЗ и ЗБ целесообразно при описании активов идентифицировать владельцев первичных активов.

В примере ПЗ для третьей доверенной стороны (ТДС) (см. приложение F) различные криптографические ключи будут иметь разных владельцев: подписчиков ТДС и владельца самого ТДС. Другой пример — медицинские системы ИТ. Хранимая и обрабатываемая в них информация не имеет одного владельца, а предназначена для использования всеми заинтересованными сторонами в соответствии с заданным набором правил ее использования и контроля такого использования.

Активы обычно включают в себя информацию, которая хранится, обрабатывается или передается в системе ИТ. При этом активы могут являться внешними по отношению к самому ОО (но находиться в пределах его ИТ-среды). В качестве примера можно привести информацию и ресурсы, защищаемые межсетевыми экранами или системами обнаружения вторжений.

В качестве активов, подлежащих защите, необходимо идентифицировать информацию авторизации и реализацию ИТ, которые косвенно относятся к предметам задания требований безопасности. Идентификацию таких активов можно рассматривать как составляющую процесса идентификации контрмер, необходимых для защиты первичных активов (или их представления). Нецелесообразно на данной стадии разработки ПЗ и ЗБ идентифицировать как активы информацию и ресурсы, связанные с представлением самого ОО, и только косвенно связанные с первичными активами. Такая детализация может привести к:

a) нечеткому пониманию основного предназначения ОО (обеспечение защиты первичных активов или их представлений в пределах ИТ-среды);

b) слишком раннему (еще до описания угроз и целей безопасности) ознакомлению пользователя ПЗ и ЗБ с деталями реализации.

8.3.2.3 Идентификация источников угроз

Источником угроз могут быть люди либо иные не связанные с деятельностью человека факторы. При этом основное внимание обычно уделяется угрозам, связанным со злонамеренной или другой деятельностью человека.

При идентификации источников угроз необходимо рассмотреть:

a) кто и по каким причинам может быть заинтересован в компрометации идентифицированных активов;

b) кто (с учетом занимаемой должности) имеет возможность компрометации идентифицированных активов. Другими словами, кто может получить доступ к системе ИТ, в которой хранятся, обрабатываются и передаются идентифицированные активы;

c) каковы предполагаемые уровень технической компетентности, уровень возможностей нарушителя, доступные ресурсы для реализации угрозы (например, автоматические инструментальные средства взлома и исследования сетей) и мотивация.

Источники угроз, не связанные с деятельностью человека, а также угрозы, возникшие в результате неумышленных действий человека (то есть случайно), также должны быть рассмотрены, так как могут привести к компрометации активов.

8.3.2.4 Идентификация методов нападения

Следующим этапом после идентификации активов, подлежащих защите, и источников угроз является идентификация возможных методов нападения, приводящих к компрометации активов. Идентификация возможных методов нападения основывается на информации о среде безопасности ОО, например, на:

a) потенциальных уязвимостях активов, которые могут быть использованы источниками угроз;

b) возможности нарушителей, имеющих доступ к среде безопасности ОО.

Потенциальные уязвимости активов организации могут быть идентифицированы путем анализа уязвимостей среды безопасности ОО с учетом идентифицированных предположений о среде. Тем не менее следует помнить, что такой анализ может не выявить всех уязвимостей, и поэтому нельзя недооценивать возможность наличия новых и необнаруженных угроз.

8.3.2.5 Влияние результатов анализа рисков на идентификацию угроз

Проведение анализа рисков целесообразно на этапе идентификации угроз, но методы анализа рисков не определены в ИСО/МЭК 15408. Процесс анализа рисков также необходим на этапе идентификации целей безопасности для ОО и его среды (см. раздел 8) и требуемого уровня доверия к контрмерам, направленным на противостояние возможным угрозам (см. раздел 9). Методы анализа риска должны учитывать следующее:

a) вероятность и последствия компрометации активов с учетом:

1) возможности реализации идентифицированных методов нападения,

2) вероятности успешной реализации нападения,

3) возможного ущерба (включая величину материального ущерба, явившегося результатом успешного нападения);

b) другие ограничения, например правовые нормы и стоимость.

8.3.3 Спецификация угроз

Следующим этапом после идентификации угроз, которые должен учитывать ОО и его среда, является спецификация данных угроз в ПЗ и ЗБ. Как отмечалось в предыдущих разделах, в разделе «Среда безопасности ОО» формулировка аспектов среды безопасности ОО и, в частности, — спецификация угроз должна быть четкой и краткой.

Для обеспечения четкой спецификации угроз необходимо учитывать следующие аспекты (идентифицированные в соответствии с 8.2.1):

a) источники угроз (например, уполномоченный пользователь ОО);

b) активы, подверженные нападению (например, конфиденциальные данные);

c) используемый метод нападения (например, маскировка под уполномоченного пользователя ОО).

Ниже приведены примеры формулирования угроз:

Угроза 1: нарушитель может получить неуполномоченный доступ к конфиденциальной информации либо ресурсам ограниченного использования, выдав себя за уполномоченного пользователя ОО.

Угроза 2: уполномоченный пользователь ОО может получить доступ к конфиденциальной информации или ресурсам ограниченного использования, выдав себя за другого уполномоченного пользователя ОО.

Если описание угрозы сопровождается объяснением всех используемых терминов, описанием активов, подверженных риску компрометации, и спецификацией конкретных методов нападения, то это будет способствовать более глубокому осознанию пользователем ПЗ и ЗБ сущности угрозы. Так, в примерах угроз, изложенных выше, целесообразно пояснить, что активами, подверженными риску компрометации, являются информация и ресурсы, к которым пользователь (в том числе выдававший себя за конкретного уполномоченного пользователя) имеет доступ.

Для того, чтобы обеспечить, насколько это возможно, краткое изложение (формулировку) угроз, необходимо исключить совпадение описаний угроз, что поможет избежать потенциальных недоразумений

при использовании ПЗ и ЗБ, а также ненужных повторений, обеспечив тем самым более простое обоснование ПЗ и ЗБ.

Совпадение описаний угроз можно легко избежать, если специфицировать все угрозы на одинаковом уровне детализации. Например, нет необходимости при спецификации угрозы конкретным активам детально описывать метод нападения, если конкретный сценарий нападения связан с более общими угрозами, ранее изложенными в ПЗ или ЗБ.

Каждая угроза должна иметь уникальную метку. Это необходимо для упрощения использования ссылок (например, в тех частях раздела ПЗ «Обоснование», которые показывают связь изложенных целей безопасности и угроз). Угрозы маркируют одним из перечисленных ниже способов:

a) последовательная нумерация угроз (например, У1, У2, У3 и т.д.);

b) присвоение уникальной метки, обеспечивающей краткое, но значащее «имя» (см. примеры в приложении В).

Преимущество подхода b) перед a) заключается в том, что уникальная метка является более информативной, так как несет в себе более значимую информацию, чем просто цифра. Неудобство подхода b) заключается в том, что не всегда удается нанести уникальную метку (из-за практических ограничений, связанных с ограничением числа символов в метке); так, в некоторых случаях метка может ввести в заблуждение, или ее можно толковать по-разному.

Описание угроз должно затрагивать только те потенциальные события, которые непосредственно могут привести к компрометации активов, требующих защиты. Поэтому не рекомендуется включать в описание угрозы, например, следующего вида: «В ОО могут существовать недостатки обеспечения безопасности ОО». Такая формулировка угрозы не способствует пониманию пользователем ПЗ и ЗБ проблем безопасности. Кроме того, учитывать сформулированную таким образом угрозу должны не ОО и его среда, а разработчики и оценщики ОО.

Применение контрмер для угроз может привести к атакам другого вида, что в свою очередь также может привести к компрометации активов (например, обход или вмешательство в работу механизмов, реализующих функции безопасности ОО). При рассмотрении в ПЗ и ЗБ такого рода угроз необходимо стремиться к тому, чтобы:

a) в результате их включения в раздел «Среда безопасности ОО» преждевременно не рассматривались детали реализации ОО, нарушающие системный подход к решению проблем безопасности;

b) они (угрозы) не попадали в область действия существующих угроз.

Например, из существования угрозы X, направленной на компрометацию актива Y, следует, что любая попытка обхода контрмер угрозе X может привести к компрометации актива Y. Следовательно, обход контрмер угрозе X может рассматриваться в качестве метода нападения, который уже находится в области действия угрозы X и, следовательно (в целях краткости формулировки аспектов безопасности ОО), не должен быть явно описан как отдельно реализуемая угроза.

При выборе требований безопасности ИТ, к которым (согласно стандартам серии ИСО/МЭК 15408) в свою очередь предъявляются требования взаимной поддержки, существует необходимость рассмотрения атак (например обход или вмешательство в процесс функционирования), направленных против контрмер, реализуемых ОО. Любые возможные атаки также должны быть раскрыты на этапе оценки ОО. Также должны быть выявлены все потенциально реализуемые атаки, направленные против функций безопасности ОО.

Примеры угроз приведены в приложении В.

8.3.4 Окончательное формулирование угроз

В раздел «Среда безопасности ОО» необходимо включать описание возможных угроз, влияющих на безопасное функционирование ОО. Наибольший интерес представляют угрозы, которым должен противостоять ОО (часто вместе с организационными и другими мерами нетехнического характера). Однако в целях полноты описания в ПЗ и ЗБ могут включаться угрозы, которым ОО непосредственно не противостоит.

Ниже приведены примеры угроз, оказывающих влияние на безопасное функционирование ОО, но которым ОО может не противостоять:

a) физическое нападение на ОО;

b) злоупотребление правами со стороны привилегированных пользователей;

c) неправильное администрирование и функционирование ОО вследствие ненадлежащего исполнения обязанностей или недостаточной подготовки администраторов.

Окончательное решение о том, каким угрозам должен противостоять ОО, а каким — среда, может быть принято только после завершения формирования целей безопасности.

Необходимо отметить, что сформулированные предположения о среде могут быть направлены на противостояние некоторым угрозам, которые могли бы повлиять на безопасное функционирование ОО. Из этого следует, что у разработчика ПЗ и ЗБ имеется некоторая свобода действий в принятии решения о том, какие аспекты безопасности необходимо рассматривать при формулировании предположений о среде, а какие — при формулировании угроз, которым должна противостоять среда ОО. Приемлемо любое решение, так как предположения и угрозы в дальнейшем отражаются на целях безопасности. При выборе между двумя возможными решениями необходимо стремиться к тому, чтобы обеспечить наилучшее понимание пользователем ПЗ и ЗБ аспектов среды безопасности ОО. Как правило, конкретные нападения должны трактоваться как угрозы, в то время как более общие формы нападений — учитываться при формулировании предположений. При этом важно, чтобы каждый аспект среды безопасности был сформулирован только один раз — в виде предположения безопасности либо в виде угрозы.

8.4 Идентификация и спецификация политики безопасности организации

Раздел «Среда безопасности ОО» должен содержать описание правил ПБОр, которым должен следовать ОО. В то же время, формулировка ПБОр может не включаться, если цели безопасности формулируются исключительно на основе угроз: другими словами, в случае, если аспекты среды безопасности ОО полностью определяются угрозами.

Под ПБОр понимается совокупность правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности. При необходимости, ПБОр может реализовываться ОО его средой либо некоторой их комбинацией.

Если ПЗ и ЗБ определяет и ПБОр, и угрозы, то следует кратко излагать в разделе «Среда безопасности ОО» аспекты среды безопасности ОО. Так, например, нецелесообразно включать в ПЗ и ЗБ правило ПБОр, являющееся простой переформулировкой угрозы.

Например, если идентифицирована угроза «Неуполномоченный субъект может получить логический доступ к ОО»,то не имеет смысла включать в ПЗ и ЗБ следующее правило ПБОр: «Пользователи должны быть идентифицированы до предоставления им доступа».

Вышесказанное связано с тем, что сформулированное таким образом правило ПБОр не только просто переформулирует угрозу, но и заранее описывает цели безопасности.

Специфицировать соответствующие правила ПБОр имеет смысл в случаях, если ОО предполагается использовать в конкретных организациях, а также, если существует необходимость следования ОО ряду правил, которые не являются очевидными из описания угроз. Например:

a) идентификация применяемых правил управления информационными потоками;

b) идентификация применяемых правил управления доступом;

c) определение правил ПБОр для аудита безопасности;

d) решения, предписанные организацией, например, использование определенных криптографических алгоритмов или следование определенным стандартам.

Каждое правило ПБОр должно иметь уникальную метку.

Примеры правил ПБОр приведены в приложении В.

9 Цели безопасности

9.1 Введение

Данный раздел содержит рекомендации по идентификации и спецификации целей безопасности в ПЗ или ЗБ.

Цели безопасности представляют собой краткую формулировку предполагаемой реакции на проблему безопасности. Краткость формулирования целей безопасности предполагает отсутствие необходимости глубокого рассмотрения деталей их достижения.

При этом цели безопасности следует расценивать как промежуточное звено, помогающее пользователю ПЗ и ЗБ отследить взаимосвязь между аспектами среды безопасности ОО и требованиями безопасности (см. рисунок 2).

В ПЗ и ЗБ необходимо различать два типа целей безопасности (см. рисунок 2):

a) цели безопасности для ОО, которые должны достигаться применением контрмер, реализуемых ОО;

b) цели безопасности для среды ОО, которые должны достигаться применением технических мер, реализуемых ИТ-средой, или не ИТ-мер (например, организационных).

Деление целей безопасности на два типа (для ОО и его среды) позволяет в контексте среды безопасности ОО вкратце изложить, решение каких аспектов проблемы безопасности возлагается на ОО. Разделе-

ние ответственности за решение отдельных аспектов проблемы безопасности между ОО и его средой позволяет в некоторой степени снизить риск компрометации активов, требующих защиты. Более того, такое разделение ответственности при формулировании целей безопасности позволяет определить границы оценки безопасности ОО, так как цели безопасности ОО влияют как на выбор необходимых функциональных требований безопасности ОО, так и на определение уровня доверия к обеспечению безопасности ОО.

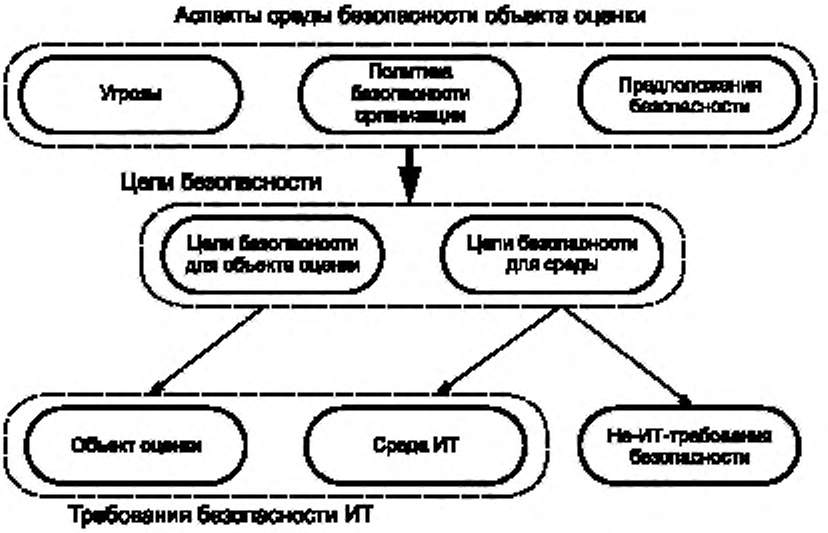

Рисунок 2 — Роль и место целей безопасности в структуре профиля защиты и задания по безопасности

9.2 Спецификация целей безопасности для объекта оценки

Цели безопасности ОО должны установить (в заданном разработчиком ПЗ и ЗБ объеме) возлагаемую на ОО ответственность за противостояние угрозам и следование ПБОр. Цели безопасности ОО (см. рисунок 2) можно рассматривать как промежуточный этап формирования требований безопасности ИТ, исходя из идентифицированных аспектов среды безопасности ОО, что необходимо всегда учитывать при спецификации целей безопасности для ОО.

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

a) с одной стороны, цели безопасности должны помочь пользователю ПЗ и ЗБ без углубленного изучения деталей реализации понять объем решения объектом оценки проблемы безопасности (степень учета аспектов среды безопасности ОО). 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, как это решение достигается;

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

Окончательную проверку правильности выбора уровня детализации формулировки целей безопасности проводят на этапе обоснования целей безопасности и требований безопасности ИТ. Если какой-либо из шагов на этапе обоснования (обоснование целей безопасности или обоснование требований безопасности) является несложным, в то время как другой вызывает значительные затруднения, то вероятнее всего формулировка целей безопасности является слишком детализированной либо слишком абстрактной.

Сформированный надлежащим образом набор целей безопасности для ОО дает определенную уверенность в том, что формулируемые на его основе требования безопасности ИТ не будут избыточными (в части ФТБ см. 10.1.1; в части ТДБ см. 10.2.1), что в свою очередь служит основой для минимизации средств и времени, затрачиваемых на оценку ОО.

С точки зрения противостояния идентифицированным угрозам существует три типа целей безопасности для ОО:

1) цели предупредительного характера, направленные на предотвращение реализации угроз либо на перекрытие возможных путей реализации данных угроз;

2) цели обнаружения, определяющие способы обнаружения и постоянного мониторинга событий, оказывающих влияние на безопасное функционирование ОО;

3) цели реагирования, определяющие необходимость каких-либо действий ОО в ответ на потенциальные нарушения безопасности или другие нежелательные события с целью сохранения или возврата ОО в безопасное состояние и/или ограничения размера причиненного ущерба.

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 относят к категории 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 следующая цель, определяющая необходимость обеспечения ОО невозможности отказа контрагентов от факта передачи или приема сообщения:

объект оценки должен включать в себя средства, позволяющие получателю информации подготовить свидетельство, доказывающее происхождение этой информации.

Примером 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.

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

Количественная оценка может быть сформулирована как в относительных, так и в абсолютных числовых значениях. Очевидно, что применение абсолютных числовых значений для количественной оценки является более предпочтительным, но в то же время и более трудным вариантом.

Если ПЗ и ЗБ разрабатывается после определения функциональных требований безопасности, то каждую цель безопасности целесообразно формулировать, исходя из соответствия конкретной группе функциональных требований безопасности, которые предполагается включить в ПЗ и ЗБ. Основное преимущество данного подхода заключается в простоте построения обоснования требований безопасности. При этом необходимо контролировать полное соответствие определенных таким образом целей безопасности изложенным в данном разделе требованиям и рекомендациям по их формулированию. В частности, необходимо убедиться в том, что цели безопасности не содержат лишних деталей реализации.

Примеры формулировок целей безопасности приведены в приложении В.

Соответствие целей безопасности для ОО угрозам и ПБОр достигается с учетом:

a) каждой идентифицированной угрозы, направленной против ОО, по крайней мере, одной целью безопасности для ОО;

b) каждого правила идентифицированной ПБОр, которому должен соответствовать ОО, по крайней мере, одной целью безопасности для ОО.

Наглядность такого соответствия может быть достигнута, например, за счет использования перекрестных ссылок или отображения рассматриваемого соответствия в форме таблицы. Несмотря на то, что демонстрация соответствия целей безопасности угрозам и ПБОр будет приведена в разделе «Обоснование» (см. разделы 12 и 13), для пользователя ПЗ и ЗБ было бы полезно отображение такого соответствия уже в разделе «Цели безопасности». В случае, если цель безопасности предполагает реализацию какого-либо правила ПБОр, предпочтительнее в раздел «Цели безопасности» включить ссылку на соответствующее правило ПБОр, а не повторять установленные ПБОр правила, подлежащие реализации (см. пример цели безопасности O.DAC, приведенный в приложении В).

Цели безопасности для ОО должны быть уникально маркированы. Маркировка может быть основана на последовательной нумерации (например, Ц1, Ц2, Ц3 и т.д.) либо на использовании значащих меток (см. примеры, приведенные в приложении В).

9.3 Спецификация целей безопасности для среды объекта оценки

Цели безопасности для среды ОО включают в себя цели безопасности, ответственность за достижение которых возлагается на ИТ-среду, а также связанные с реализацией в пределах среды функционирования ОО организационных и других нетехнических мер.

Цели безопасности для среды ОО должны быть сформулированы для учета тех аспектов среды безопасности ОО, которые по тем или иным причинам не попадают в сферу ответственности ОО. В частности, цели безопасности для среды ОО должны быть направлены на:

a) противостояние угрозам (или отдельным аспектам угроз), которым ОО не противостоит;

b) поддержку реализации правил ПБОр, которые не соответствуют или не полностью соответствуют ОО;

c) поддержку идентифицированных целей безопасности для ОО в плане противостояния угрозам и реализации соответствующих правил ПБОр;

d) поддержку идентифицированных предположений о среде.

Таким образом, формулирование целей безопасности для среды ОО необходимо начинать с формирования списка угроз, ПБОр и предположений, которые не были учтены либо были учтены не полностью при формулировании целей безопасности для ОО. Для каждого такого аспекта среды безопасности ОО необходимо:

a) сформулировать новую цель безопасности для учета рассматриваемого аспекта среды безопасности ОО;

b) поставить в соответствие рассматриваемому аспекту среды безопасности ОО ранее уже сформулированную цель безопасности, если соответствующая цель уже была сформулирована (при этом может потребоваться доработка формулировки цели безопасности с тем, чтобы расширить ее область действия).

В дальнейшем, при формулировании обоснования целей безопасности, список целей безопасности может быть уточнен путем формулирования дополнительных целей безопасности, необходимых для полного учета всех аспектов среды безопасности ОО (угроз, ПБОр и предположений безопасности).

Цели безопасности для среды ОО целесообразно формулировать параллельно с формулированием целей безопасности для ОО. При этом процесс формулирования целей безопасности в целом следует рассматривать как важный этап в разделении ответственности за обеспечение безопасности, возлагаемой на ОО и его среду. В связи с этим необходимо придерживаться следующих правил:

a) цели безопасности для ОО должны быть сформулированы так, чтобы соответствующие им требования ИТ не требовали чрезмерно больших затрат на оценку их выполнения;

b) цели безопасности для среды ОО должны быть сформулированы так, чтобы соответствующие им требования к организационным мерам и не ИТ-средствам были практически реализуемы, а также не накладывали чрезмерные ограничения на действия пользователей ОО.

Типовые не ИТ-цели безопасности для среды могут предусматривать:

a) разработку и применение организационных мер (методик, процедур, приемов), обеспечивающих эксплуатацию ОО так, чтобы его безопасность не нарушалась (в частности, соблюдались все предположения о среде);

b) включение целей, связанных с обучением администраторов и пользователей практическим вопросам обеспечения информационной безопасности.

Таким образом, в состав целей безопасности для среды необходимо включать в том числе цели безопасности, связанные с действиями управления, направленными на обеспечение эффективности функций безопасности, предоставляемых объектом оценки. В некоторых случаях требуемые действия управления являются очевидными и могут быть выражены в форме не ИТ-целей безопасности для среды (например, при рассмотрении вопроса о необходимости надлежащего управления функциями аудита). В других случаях требуемые действия управления могут зависеть от детализованных требований безопасности, используемых для реализации целей безопасности ОО. Например, цель безопасности «идентификация и аутентификация» (см. цель Ц1 в 9.1) может быть реализована путем использования механизма пользовательских паролей. Использование механизма пользовательских паролей предполагает необходимость формулирования соответствующего требования к пользователям, связанного с обеспечением последними недоступности паролей для других лиц. Данное требование безопасности представляет собой требование

безопасности для не ИТ-среды (см. 10.5.2) и, в свою очередь, уточняет соответствующую цель безопасности для среды ОО.

Если противостояние угрозе или проведение ПБОр частично возлагается на ОО, а частично на его среду, соответствующая цель безопасности должна повторяться в каждой категории (цели безопасности — для ОО, цели безопасности для среды). Так, цель Ц1 «идентификация и аутентификация» (см. 9.1) для включения в состав целей безопасности как для ОО, так и для среды ОО может быть переформулирована следующим образом:

«Объект оценки с учетом действий поддержки со стороны его среды должен уникально идентифицировать и выполнять процедуру аутентификации идентифицированного пользователя до предоставления ему доступа к функциональным возможностям ОО».

В случаях, если имеется возможность четко разделить ответственность между ОО и его средой, отпадает необходимость включения одной и той же цели в состав угроз обеих категорий целей безопасности. Например, при идентификации целей безопасности, связанных с аудитом безопасности, ОО ответственен за генерацию и сбор данных, а на среде ОО лежит ответственность за поддержку действий управления (например, анализ сгенерированных данных).

Типичным примером цели безопасности для ИТ-среды является цель безопасности «Идентификация и аутентификация пользователей ОО» для операционной системы, под управлением которой работает СУБД. Далее (см. 10.4.2) путем уточнения целей безопасности для ИТ-среды формулируются требования безопасности для ИТ-среды.

Цели безопасности для среды, как и цели безопасности для ОО, должны быть уникально маркированы. При этом целесообразно принять соглашение о маркировке, которое четко различало бы цели безопасности для ОО и цели безопасности для среды. Например, если маркировка основана на последовательной нумерации, то цели безопасности для среды могут быть пронумерованы следующим образом: ЦС1, ЦС2, ЦС3 и т.д. Примеры целей безопасности для среды приведены в приложении В.

10 Требования безопасности

10.1 Введение

Данный раздел содержит рекомендации по формированию в ПЗ и ЗБ требований безопасности ИТ как для ОО, так и для ИТ-среды. Кроме того, в данном разделе кратко излагаются вопросы формирования требований безопасности для не ИТ-среды (требования для не ИТ-среды не являются обязательными для ПЗ и ЗБ).

В ПЗ и ЗБ формулируют следующие типы требований безопасности ИТ:

a) функциональные требования безопасности ОО. Функциональные требования безопасности определяют требования для функций безопасности, обеспечивающих достижение целей безопасности для ОО;

b) требования доверия к безопасности ОО. Требования доверия к безопасности определяют требуемый уровень уверенности в надлежащей реализации ФТБ;

c) требования безопасности для ИТ-среды. Требования данного типа определяют функциональные требования и требования доверия к безопасности, выполнение которых возлагается на ИТ-среду (то есть на внешние по отношению к ОО аппаратные, программные или программно-аппаратные средства) с тем, чтобы обеспечить достижение целей безопасности для ОО (см. рисунок 3).

Как показано на рисунке 3, требования безопасности ИТ могут быть сформированы, где это возможно, с использованием каталога функциональных компонентов, определенных в ИСО/МЭК 15408-2, и каталога компонентов доверия к безопасности, определенных в ИСО/МЭК 15408-3.

Использование каталогов требований, определенных в стандартах серии ИСО/МЭК 15408, позволяет достичь определенного уровня стандартизации в области представления требований безопасности, что значительно облегчает сравнение ПЗ и ЗБ между собой.

Если в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 отсутствуют 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, подлежать оценке и излагаться в соответствии с требованиями стандартов серии ИСО/МЭК 15408.

Рекомендации по спецификации ФТБ и ТДБ в случаях, если в ИСО/МЭК 15408-2 и ИСО/МЭК 15408-3 соответственно нет подходящих компонентов требований для формулирования рассматриваемых ФТБ и ТДБ, приведены в 10.1.5 и 10.2.3.

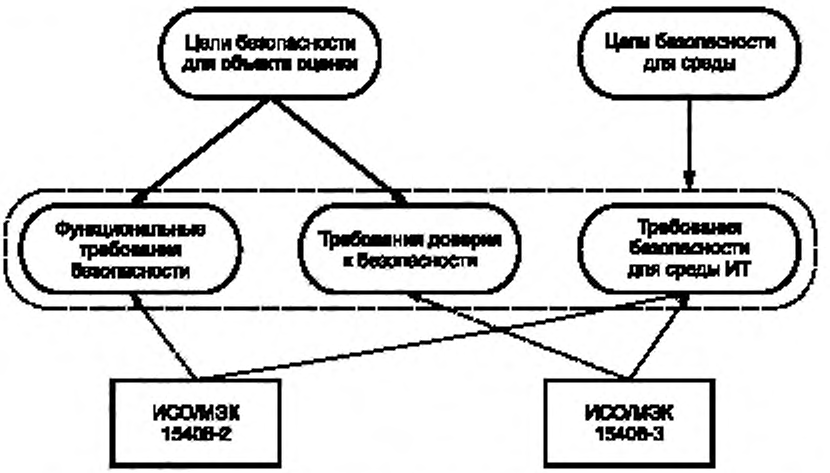

Рисунок 3 — Формирование требований безопасности информационных технологий

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

Рекомендации по выполнению операций над функциональными компонентами, определенных в ИСО/МЭК 15408, включены в 10.1.2; компонентами доверия к безопасности — в 10.2.2.

Следует отметить, что в ИСО/МЭК 15408 каждому компоненту требований безопасности назначена предусмотренная на определенной классификации уникальная метка. Например, для FAU_GEN.1.2 компонента FAU_GEN.1 метка имеет вид:

a) 'F'-метка указывает на то, что это — функциональное требование;

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

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

d) '1'-метка указывает на то, что ФТБ принадлежит компоненту «Генерация данных аудита» семейства FAU_GEN;

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

Требования ФТБ и ТДБ выбирают на уровне компонентов: элементы, входящие в компонент, должны быть включены в ПЗ и ЗБ, если в ПЗ и ЗБ включается данный 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. Иерархия предполагает, что один компонент включает в себя все элементы требований, 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 разрабатываемые ПЗ и ЗБ обоих этих компонентов;

2) компоненты могут зависеть от компонентов других семейств. Например, компонент FIA_UAU.1 (связанный с требованием аутентификации пользователей) зависит от компонента FIA_UID.1 (связанный с требованием идентификации пользователей).

При формировании ПЗ и ЗБ все зависимости компонентов требований безопасности ИТ должны быть, как правило, удовлетворены, что достигается включением в ПЗ и ЗБ компонентов, от которых зависят уже включенные в ПЗ и ЗБ компоненты. Зависимости могут не удовлетворяться в случаях, если в ПЗ и ЗБ показано, что зависимости не соответствуют целям безопасности и угрозам.

В дополнение к ФТБ и ТДБ в разделе ПЗ и ЗБ «Требования безопасности ИТ» требуется (где необходимо) определить минимальный уровень стойкости функции безопасности ОО, а также (где необходимо) требования к точному значению стойкости.

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

10.2.1 Выбор функциональных требований безопасности

Определив цели безопасности, необходимо уточнить, как эти цели безопасности будут достигаться. Для этого осуществляется спецификация ФТБ, например, путем выбора подходящих ФТБ, сгруппированных в компоненты. При этом процесс выбора ФТБ значительно упрощается, если используются предопределенные функциональные пакеты, соответствующие конкретным целям безопасности для ОО (см. раздел 15).

В процессе формирования ФТБ выделяют несколько этапов. Исходя из них, различают следующие два типа ФТБ:

a) основные ФТБ, непосредственно удовлетворяющие конкретные цели безопасности для ОО;

b) 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 ПЗ не обязательно делить ФТБ на основные и поддерживающие, такое деление может оказаться полезным при формировании раздела ПЗ «Обоснование».

Первой стадией в процессе выбора ФТБ, соответствующего конкретным целям безопасности для ОО, является идентификация основных ФТБ, непосредственно соответствующих данным целям безопасности. После формирования полной совокупности основных ФТБ начинается итерационный процесс формирования полной совокупности поддерживающих ФТБ. Все ФТБ (основные и поддерживающие) целесообразно, где это возможно, формировать на основе функциональных компонентов, определенных в ИСО/МЭК 15408-2. При выборе функциональных компонентов, определенных в ИСО/МЭК 15408, целесообразно учитывать рекомендации, содержащиеся в приложениях к ИСО/МЭК 15408-2 и связанные с интерпретацией данных компонентов.

Взаимосвязь между основными и поддерживающими ФТБ показана на рисунке 4. Данную взаимосвязь учитывают при формировании раздела ПЗ «Обоснование», в котором требуется показать взаимную поддержку ФТБ (см. 12.2.4). При этом требуется раскрыть характер поддержки, выполняемой поддерживающими ФТБ для достижения целей безопасности ОО.

Формирование полной совокупности поддерживающих ФТБ подразделяют на следующие стадии:

1) идентификация дополнительных ФТБ, необходимых (с точки зрения разработчика ПЗ) для удовлетворения зависимостей всех основных ФТБ;

2) идентификация 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);

3) идентификация дополнительных ФТБ, необходимых для удовлетворения зависимостей тех поддерживающих ФТБ, которые были выбраны на предыдущих стадиях.

Рисунок 4 — Взаимосвязь основных и дополнительных функциональных требований безопасности

Идентификация поддерживающих ФТБ представляет собой итерационный процесс, например:

a) предположим, что ПЗ включает в себя цель безопасности, требующую, чтобы ОО определенным образом реагировал на события, являющиеся показателем предстоящего нарушения безопасности. Наличие в ПЗ подобной цели предполагает идентификацию основного ФТБ на базе компонента FAU_ARP.1 «Сигналы нарушения безопасности»;

b) компонент FAU_ARP.1 имеет зависимость от компонента FAU_SAA.1 «Анализ потенциальных нарушений», который также должен быть включен в ПЗ в качестве поддерживающего ФТБ;

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

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

e) 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 удовлетворения 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 потенциального нарушения безопасности, которое определено применением FAU_SAA.1.2).

Для других компонентов согласованность может быть более проблематичной. Например, при включении в ПЗ компонента FDP_ACC.1 одновременно идентифицируется конкретная политика 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 уменьшения 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:

a) ФТБ, основанные на соответствующих компонентах того же класса, что и основные ФТБ. Например, если компонент FAU_GEN.1 «Генерация данных аудита» включен в ПЗ, то может возникнуть необходимость в создании и ведении журнала аудита безопасности для хранения сгенерированных данных (для формулирования подобного требования необходим один или более функциональных компонентов из семейства FAU_STG), а также потребность в средствах просмотра сгенерированных данных аудита (для формулирования подобного требования 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;

b) ФТБ, основанные на соответствующих компонентах класса FPT «Защита функций 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 модификаций в ПЗ могут быть включены ФТБ на основе компонента FPT_AMT.1 «Тестирование абстрактной машины» и компонентов семейства FPT_SEP «Разделение домена»;

c) 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 с тем, чтобы сформировать целостный набор поддерживающих друг друга ФТБ. Таким образом, на выбор поддерживающих ФТБ существенное влияние может оказывать процесс построения раздела ПЗ «Обоснование». Необходимо избегать включения в ПЗ поддерживающих ФТБ, не направленных на достижение целей безопасности, так как включение подобных ФТБ приведет к ограничению сферы применения ПЗ вследствие следующих обстоятельств:

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

b) 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 (где необходимо) ФТБ, отличные от ФТБ базового ПЗ, для учета любых различий в среде безопасности ОО и/или целях безопасности в разрабатываемом и базовом профилях защиты.

10.2.2 Выполнение операций над функциональными требованиями безопасности

10.2.2.1 Разрешенные операции

Над функциональными компонентами могут выполняться разрешенные операции. Выполняя операции над функциональными компонентами, разработчик ПЗ может сформировать соответствующее данному ПЗ требование безопасности. Допустимыми операциями являются:

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

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

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

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

10.2.2.2 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. Подобным образом может потребоваться неоднократное использование компонентов семейств FDP_ACC и FDP_ACF в случаях, если 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 и ЗБ (см. 10.1.6).

Для каждого ФТБ, включаемого в ПЗ, необходимо принять следующее решение:

a) выполнить операции «назначение» и «выбор», предусмотренные функциональным компонентом для изложения ФТБ;

b) специфицировать операцию «уточнение» для ФТБ.

Выполнение операций над функциональными компонентами должно выделяться в тексте ПЗ и ЗБ в соответствии с обозначениями, принятыми в подразделе «Соглашения» раздела «Введение». Рекомендуется следующий подход к выделению результатов выполнения операций.

Результат операции «уточнение» выделяют полужирным шрифтом.

Результат операции «выбор» выделяют подчеркиванием и курсивом.

Результат операции «назначение» значение параметра заключают в квадратные скобки [например (назначаемое значение)].

Выполнение операции «итерация» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, например (номер итерации).

10.2.2.3 Операции «назначение» и «выбор»

Операции «назначение» и «выбор» выполняются (завершаются) в ПЗ в том случае, если разработчику ЗБ не представляется возможность спецификации (кроме «уточнения») того, как функциональный компонент используется для удовлетворения целей безопасности, то есть сужается область ответственности разработчика ЗБ.

При принятии решения о необходимости выполнения операций «назначение» и «выбор» в каждом конкретном случае необходимо учитывать следующие факторы:

a) с одной стороны, ПЗ должен быть максимально независимым от реализации: чрезмерно детальная спецификация вследствие выполнения операций может стать причиной необоснованного сокращения числа ОО, которые могли бы соответствовать данному ПЗ;

b) с другой стороны, если выбраны компоненты требований, в которых специфицированы разрешенные операции (назначение, выбор), то эти операции должны использоваться в ПЗ для конкретизации требований до уровня детализации, необходимого для демонстрации достижения 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.

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

По первому примеру 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».

Второй пример — ФТБ (основанное на компоненте FPT_ITT.1), которое показывает, как частичное выполнение операции «выбор» предписывает применение одного из вариантов выбора. Компонент FPT_ITT.1 допускает спецификацию требования защиты передаваемых данных ФБО от раскрытия и/или модификации. В рассматриваемом примере разработчик ПЗ определил, что для достижения целей безопасности требуется защита передаваемых данных ФБО от раскрытия. Наряду с этим разработчик ПЗ не преследует цели запретить наличие в ЗБ для соответствующего ОО специфицированной защиты от модификации. Таким образом, частичное выполнение операции «выбор» заключается в исключении нежелательного варианта (защита только от модификации):

«ФБО должны защитить свои данные от [выбор: раскрытие, раскрытие и модификация] при их передаче между разделенными частями ОО».

Исходя из рассмотренных примеров, можно сделать вывод, что частичное выполнение операции «выбор» является надлежащим, если результирующее ФТБ представляет подмножество вариантов выбора, которые являются разрешенными для исходного функционального компонента. Подобным образом, частичное выполнение операции «назначение» является надлежащим, если допустимые значения выполнения операции «назначение» для 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 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]».

Если операция остается невыполненной, то необходимо 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 это необходимо, сопровождать рекомендациями разработчику ЗБ о том, каким образом следует выполнять операции (например, в виде замечаний по применению).

10.2.2.4 Операция «уточнение»

Операция «уточнение» может быть выполнена для любого элемента любого функционального компонента и заключается в добавлении некоторых технических деталей. Например, если для конкретного ОО требуется объяснение смысла терминов «субъект» и «объект» в рамках ЗБ, то для этих терминов выполняется операция «уточнение». Дополнительные уточнения не налагают новых требований, они ограничивают совокупность возможных функций или механизмов для реализации специфицированного требования безопасности.

Считается, что операция «уточнение» выполнена надлежащим образом, если выполнение уточненного требования приводит к выполнению данного требования, как если бы оно не было уточнено. Как правило, операция «уточнение» должна использоваться в ПЗ рационально, чтобы не ограничивать сферу действия ПЗ.

Ниже приведен 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, 6 символов.

Рекомендации по использованию операции «уточнение» для улучшения читабельности ФТБ приведены в 10.1.6.

10.2.3 Спецификация требований аудита

Если в ПЗ включены требования аудита (основанные на компоненте FAU_GEN.1), то при формировании остальных функциональных требований, включаемых в ПЗ, 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:

a) определенные в ПБОр требования к аудиту безопасности;

b) значимость аудита безопасности для достижения целей безопасности;

c) значимость некоторых событий и их характеристик для целей безопасности;

d) анализ «стоимость — эффективность».

Например, если ОО предназначен для защиты от злоумышленных пользователей или хакеров, то аудиту должны подлежать события, связанные с нарушением политики управления доступом. В то же время в состав событий, подлежащих аудиту, можно не включать события, связанные с администрированием ОО со стороны администратора. Множество таких событий зависит от степени доверия к администратору.

При проведении анализа «стоимость — эффективность» должны быть рассмотрены следующие вопросы:

a) является ли регистрируемая информация полезной для ее последующего анализа;

b) имеет ли администратор необходимые ресурсы (например, инструментальные средства поддержки) для эффективного анализа собранной информации;

c) каковы предполагаемые затраты на хранение и обработку собираемых данных.

В стандартах серии ИСО/МЭК 15408 определены три предопределенных уровня аудита: минимальный, базовый и детализированный. Для каждого предопределенного уровня в ИСО/МЭК 15408-2 определен минимальный набор событий, подлежащих аудиту, а также минимальный объем подлежащей регистрации информации с привязкой к функциональным компонентам.

Предопределенные уровни аудита могут быть охарактеризованы следующим образом:

a) 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, представляющие наибольший интерес);

b) базовый уровень аудита требует, чтобы аудиту подвергались все действия или события, связанные с данным функциональным компонентом (например, успешные и неудачные попытки доступа к ОО);

c) детализированный уровень аудита отличается от базового наличием требований регистрации дополнительной информации (детализированный уровень необходим в тех случаях, когда объем генерируемых данных аудита недостаточен или анализ данных аудита предполагается проводить с использованием оборудования или средств обнаружения вторжения).

Если ни один из перечисленных уровней не является надлежащим, то целесообразно выбрать неопределенный уровень аудита и в явном виде перечислить все подлежащие аудиту события в элементе FAU_GEN.1.1. Например, допускается принять за основу минимальный уровень аудита, но в ряде случаев отклониться от минимальных требований вследствие того, что какое-либо подмножество действий или событий является более значимым для достижения целей безопасности. Например, если компонент FDP_ACF.1 включен в ПЗ, то может потребоваться более детальный аудит неудачных попыток доступа по сравнению с успешными.

Для того, чтобы сформировать список событий, подлежащих аудиту, необходимо проанализировать каждый используемый в ПЗ функциональный компонент; если назначен один из предопределенных уровней аудита (минимальный, базовый или детализированный), то подлежащие аудиту события в явном виде идентифицируются в разделе «Аудит» описания семейства компонентов. Рекомендуется сформировать таблицу, идентифицирующую события и (при необходимости) дополнительную подлежащую регистрации информацию.

10.2.4 Спецификация требований управления

В подразделе «Управление» для каждого семейства (см. ИСО/МЭК 15408-2) определен список действий управления применительно к компонентам данного семейства. Наличие списка действий управления может предполагать включение в ПЗ отдельных компонент из класса FMT «Управление безопасностью». Подраздел «Управление» определен в стандартах серии ИСО/МЭК 15408 как информативный, и поэтому мотивировать 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, если функциональные компоненты ссылаются на конфигурированные данные ФБО, которые подлежат управлению и контролю. Например, цели безопасности для ОО могут быть не достигнуты в том случае, если администраторы ОО не были ограничены в возможности модификации данных ФБО по своему усмотрению. Поэтому компоненты класса FMT часто включаются в ПЗ для того, чтобы сформировать на их основе поддерживающие ФТБ, способствующие достижению целей безопасности для ОО, и чтобы ФТБ в целом являлись взаимно поддерживающими (см. 12.1.1 и 12.1.4).

10.2.5 Спецификация стойкости функции безопасности

В ИСО/МЭК 15408-3 идентифицированы три предопределенных уровня СФБ (стойкости функции безопасности), а именно «базовая», «средняя» и «высокая» для всех функций безопасности ИТ, которые реализуются вероятностными или перестановочными механизмами (например, пароль или хэш-функция), идентифицированных в ПЗ или ЗБ (см. также ИСО/МЭК 15408-1, приложение В, раздел В.2). Эти уровни характеризуются следующим образом:

a) функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения;

b) функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения;

c) функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

Выбор уровня должен основываться на ряде факторов, относящихся к источнику (источникам) угрозы:

a) затрачиваемое время;

b) компетентность;

c) знание ОО;

d) доступ к ОО;

e) оборудование.

Значение этих факторов получаются на основе анализа потенциала нападения источников угроз, идентифицированных в изложении угроз. Характеристика этих факторов должна определяться в процессе полной оценки рисков реализации угроз.

Для некоторых вероятностных и перестановочных механизмов могут быть определены дополнительные явные метрики, а не более общие заявления «базовая», «средняя» и «высокая».

10.2.6 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 ФТБ, которых нет в ПЗ, либо отличающиеся от специфицированных в ПЗ.

Предпочтителен последний подход, так как при этом упрощается ЗБ. Пользователей ЗБ больше интересуют функции безопасности ИТ, чем ФТБ так же, как и оценщиков 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 в ЗБ функциональным требованиям соответствующих ПЗ и функциональным требованиям, определенным в 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) понять, какие операции и каким образом были выполнены, а также облегчает формирование раздела «Обоснование ЗБ» (см. 13.3.6).

10.2.7 Спецификация функциональных требований, отсутствующих в профиле защиты

В некоторых случаях необходимо специфицировать ФТБ, которые отсутствуют в соответствующем ПЗ. Это может быть в случае, если:

a) для ОО отсутствует подходящее ПЗ, соответствие которому может быть заявлено в ЗБ;

b) 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 10.1. 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 «Обосновании» необходимо продемонстрировать отсутствие противоречия).

10.2.8 Спецификация в профиле защиты функциональных требований, не изложенных в ИСО/МЭК 15408-2

Если при разработке ПЗ требуется включить в документ функциональное требование, для которого в стандартах серии ИСО/МЭК 15408 отсутствует соответствующий функциональный компонент, то в качестве формы представления рассматриваемого ФТБ необходимо использовать форму представления функциональных компонентов в соответствии со стандартами серии ИСО/МЭК 15408.

Принятие решения о наличии либо отсутствии соответствующего функционального компонента в ИСО/МЭК 15408-2 может оказаться сложным, т. к. предполагает хорошее знание стандартов серии ИСО/МЭК 15408. С учетом этого рекомендуется использовать приложение В настоящего стандарта, идентифицирующее функциональные компоненты функциональных требований, соответствующие основным функциональным требованиям безопасности. В большинстве случаев надлежащее 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 надлежащего 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 стандартов серии ИСО/МЭК 15408.

Спецификация ФТБ в явном виде включает в себя:

a) определение ФТБ на том же уровне абстракции, что и функциональные компоненты стандартов серии ИСО/МЭК 15408;

b) использование стиля и фразеологии (языка) функциональных компонентов стандартов серии ИСО/МЭК 15408.

Подобие нового ФТБ другим ФТБ, которые уже имеются в составе существующего в стандартах серии 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 стандартов серии ИСО/МЭК 15408 предусматривает:

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

b) использование устоявшихся терминов, таких как «атрибуты безопасности» и «уполномоченный пользователь»;

c) самостоятельность и понятность каждого элемента требований без каких-либо ссылок на другие элементы требований;

d) оцениваемость каждого требования безопасности, то есть должна существовать возможность дать заключение о том, соответствует ли ОО рассматриваемому требованию.

При формировании ФТБ в явном виде необходимо решить:

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

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

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

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

Именование ФТБ, не основанных на компонентах ИСО/МЭК 15408-2, должно показывать, что это — дополнительное по отношению к стандартам серии ИСО/МЭК 15408 требование безопасности.

С тем, чтобы не возникло противоречия с возможными именами классов, семейств и компонентов будущих версий стандартов серии ИСО/МЭК 15408, следует избегать краткой формы именования XXX_YYY. Однако если компонент расширения сформирован на основе существующего компонента стандартов серии ИСО/МЭК 15408, то и именовать его целесообразно уникальным, но схожим с компонентом стандартов серии ИСО/МЭК 15408 образом.

Разработчик ЗБ также может сформулировать ФТБ в ЗБ в явном виде, то есть без ссылки на функциональные компоненты, определенные в ИСО/МЭК 15408-2. Также нет необходимости для формулируемых в явном виде ФТБ определять операции, описанные в стандартах серии ИСО/МЭК 15408 («назначение», «выбор»), если не предполагается их повторное использование в ПЗ, других ЗБ, функциональных пакетах.

10.2.9 Представление функциональных требований безопасности

При формировании перечня ФТБ разработчик ПЗ должен представить их так, чтобы обеспечить наилучшее понимание требований безопасности пользователями и согласование ФТБ с требованиями стандартов серии 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 ИСО/МЭК 15408-2.

Во-вторых, значительно повысить читабельность ФТБ можно за счет надлежащего 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.

Ниже 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 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 F.

10.3 Спецификация в профилях защиты или заданиях по безопасности требований доверия к безопасности

10.3.1 Выбор требований доверия к безопасности

Выбор требований доверия к безопасности зависит от следующих факторов:

a) ценности активов, подлежащих защите, и риска их компрометации;

b) технической реализуемости;

c) стоимости разработки и оценки;

d) требуемого времени для разработки и оценки ОО;

e) требований рынка (для продуктов ИТ);

f) зависимостей функциональных компонентов и компонентов доверия к безопасности.

Чем выше ценность активов, подлежащих защите, и больше риск компрометации этих активов, тем выше требуется уровень доверия к безопасности для функций безопасности, используемых для защиты рассматриваемых активов, что следует отразить при формировании целей безопасности. Организации могут устанавливать 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.

Другие факторы, такие как «стоимость» и «затраты времени», целесообразно рассматривать как ограничения уровня доверия к безопасности, который является практически достижимым. Техническая реализуемость рассматривается в случае, если считается практически нецелесообразной подготовка свидетельства, требуемого конкретными компонентами доверия к безопасности, что актуально также для наследуемых систем (в случаях, если конструкторская документация недоступна), а также если в идеальном случае требуется высокий уровень доверия к безопасности, но технически невозможно за приемлемое время подготовить требуемое формальное либо полуформальное свидетельство. В случаях, если имеются ограничения для практически достижимого уровня доверия к безопасности, целесообразно согласиться с тем, что максимально достижимый уровень доверия к безопасности меньше, чем теоретически возможный. Такое принятие 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:

a) цели безопасности для ОО могут устанавливать, что ОО должен быть стойким к нарушителям с высоким потенциалом нападения;

b) цели безопасности могут требовать анализа скрытых каналов, что однозначно определяет включение в ПЗ и ЗБ компонента из семейства AVA_CCA «Анализ скрытых каналов», требующего проведения анализа скрытых каналов;

c) 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 (см. раздел 15), например, ОУД, определенный в стандартах серии 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. раздел 6 ИСО/МЭК 15408-3).

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 расширен путем использования компонента AVA_VLA.2 «Независимый анализ уязвимостей», то в ПЗ также необходимо включить компоненты ADV_LLD.1 «Описательный проект нижнего уровня» и ADV_IMP.1 «Подмножество реализации ФБО».

10.3.2 Выполнение операций над требованиями доверия к безопасности

В отличие от функциональных компонентов, к компонентам доверия к безопасности неприменимы операции «назначение» и «выбор». Однако возможны следующие операции:

a) «итерация», допускающая многократное использование одного и того же компонента доверия к безопасности;

b) «уточнение», позволяющее добавить детали к требованию доверия к безопасности.

На практике выполнение операции «итерация» может потребоваться в тех случаях, когда требуются разные «уточнения» для того же компонента доверия к безопасности, который используется для разных частей ОО, либо, если в ПЗ и ЗБ определены различные наборы ТДБ для разных компонентов составного ОО (см. 14.2.4). В последнем случае 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 выполнены:

a) предписания разработчику использовать конкретные инструментальные средства разработки, методики, модели жизненного цикла, методы анализа, системы обозначений, определенные стандарты и т.д.;

b) предписания действий оценщика, например:

1) компонент ADV_IMP.1 определяет, какие части представления реализации ОО должны быть оценены,

2) компонент ADV_IMP.1 идентифицирует известные уязвимости, которые необходимо рассматривать как «явные» уязвимости в контексте данного ОО.

10.3.3 Спецификация в профиле защиты требований доверия к безопасности, не включенных в ИСО/МЭК 15408-3

Если в ПЗ включается ТДБ, для которого в стандартах серии ИСО/МЭК 15408 нет соответствующего компонента доверия к безопасности, то рассматриваемое ТДБ должно быть определено в стиле компонентов из стандартов серии ИСО/МЭК 15408.

Сформулированные в явном виде ТДБ должны содержать определение:

a) действий разработчика;

b) требований к содержанию и представлению свидетельств, которые должен представить разработчик;

c) действий оценщика.

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.

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

Целесообразно излагать формулируемые в явном виде ТДБ так же, как изложены компоненты доверия к безопасности, определенные в ИСО/МЭК 15408-3. Поэтому отдельное требование необходимо оформлять в виде отдельного элемента требований (см. 2.1.4 ИСО/МЭК 15408-3). При этом необходимо использовать терминологию, приведенную в 2.4 ИСО/МЭК 15408-3.

Принципы спецификации ТДБ в ЗБ аналогичны принципам спецификации ТДБ в ПЗ. В большинстве случаев ТДБ в ЗБ определяется ПЗ, о соответствии которому заявляется в ЗБ, а также общепринятым пакетом доверия к безопасности (например, ОУД из стандартов серии ИСО/МЭК 15408).

Тем не менее, возможны случаи, когда разработчик ЗБ специфицирует требования доверия к безопасности, которые расширяют пакет доверия к безопасности или набор ТДБ из ПЗ. Расширение последних может иметь место в случаях, если заявитель оценки считает, что получаемые преимущества оправдывают дополнительные расходы на оценку. В этих случаях спецификация ТДБ должна быть выполнена с использованием описанных для ПЗ инструкций и соответствовать целям безопасности. Требования доверия к безопасности, не основанные на компонентах доверия к безопасности, определенных в стандартах серии ИСО/МЭК 15408, могут быть включены в ЗБ аналогично тому, как они включаются в ПЗ.

10.4 Требования безопасности для среды

10.4.1 Требования безопасности для ИТ-среды

В ПЗ и ЗБ должны включаться требования безопасности для ИТ-среды. Ниже приведены примеры случаев, когда необходимость задания требований безопасности для ИТ-среды очевидна:

a) в целях обеспечения безопасности системы управления базами данных (СУБД) идентификация и аутентификация пользователей СУБД может быть возложена на операционную систему (ОС), под управлением которой функционирует СУБД. На ОС также может быть возложена задача защиты от обхода пользователями механизмов управления доступом СУБД при непосредственном обращении к файлам базы данных;

b) безопасность приложений, использующих смарт-карту, может зависеть в том числе от возможности ОС, под управлением которой работает смарт-карта, изолировать друг от друга отдельные приложения (так, чтобы одно приложение не могло повредить данные и код другого приложения), а также может непосредственно зависеть от характеристик стойкости платы интегральной схемы.

Требования безопасности для ИТ-среды могут быть сформулированы в процессе удовлетворения зависимостей включенных в ПЗ и ЗБ функциональных компонентов, определенных в ИСО/МЭК 15408-2, в том случае, если включаемые для удовлетворения зависимостей требования безопасности с бóльшим успехом могут быть выполнены ИТ-средой по сравнению с ОО.

Отличия требований безопасности для ИТ-среды и предположения о среде состоят в следующем:

a) предположения не требуют доказательств (являются очевидными) при анализе;

b) требования безопасности необходимы для обеспечения достижения целей безопасности, и поэтому они должны быть верифицированы.

В отличие от требований безопасности ОО, требования безопасности для ИТ-среды не анализируются (при оценке ОО) на предмет подтверждения требуемого уровня доверия тому, что ИТ-среда обеспечивает надлежащее выполнение предписанных ей ФТБ.

При оценке ОО предполагается, что среда ОО выполняет предписанные ей ФТБ, хотя некоторые требования безопасности для ИТ-среды все же могут подлежать проверке. Поэтому требуемый уровень доверия к безопасности может быть окончательно установлен в ходе проведения отдельной оценки компонентов ИТ-среды, которые реализуют требуемые функциональные возможности безопасности.

Требования безопасности для ИТ-среды, как и требования безопасности ОО, целесообразно формировать (где это возможно) на основе функциональных компонентов и компонентов доверия к безопасности, определенных в стандартах серии ИСО/МЭК 15408. Любое отклонение от этих компонентов должно сопровождаться строгим обоснованием в ПЗ и ЗБ.

В некоторых случаях нецелесообразно формулировать функциональные требования безопасности для ИТ-среды на основе функциональных компонентов, определенных в ИСО/МЭК 15408-2. Например, может потребоваться, чтобы ФТБ были сформулированы в ПЗ на более абстрактном уровне с тем, чтобы возложить на разработчика ЗБ ответственность за определение того, каким образом будут удовлетворены эти высокоуровневые (независимо от конкретной реализации) функциональные требования безопасности.

Для разработчика ЗБ зависимости ОО и ИТ-среды должны быть известными, так как они имеют отношение к конкретному ОО и конкретной ИТ-среде. Напротив, разработчик ПЗ должен учитывать, что соответствующие профилю защиты объекты оценки могут различаться степенью зависимости от ИТ-среды. Ниже рассмотрены два основных случая, связанных с разделением ответственности между ОО и ИТ-средой:

1) разделение ответственности между ОО и ИТ-средой полностью определено. В этом случае требования безопасности для ИТ-среды должны быть специфицированы в одном или более (по числу компонентов ИТ-среды) подразделе ПЗ;

2) разделение ответственности между ОО и ИТ-средой не определено в ПЗ. В этом случае не делается различий между ФТБ для ОО и ФТБ для ИТ-среды. При этом разработчик ПЗ должен максимально исключить возможность для разработчика ЗБ утверждать о соответствии ПЗ, в то время как ОО реализует незначительное число ФТБ, а ИТ-среда — все остальные ФТБ.

Во втором из описанных случаев злоупотребления утверждением о соответствии ПЗ можно избежать, если в ПЗ заявить, что все ФТБ относятся к ОО. Тогда, если продукт ИТ удовлетворяет всем ФТБ только при поддержке ИТ-среды, то в качестве ОО, соответствующего ПЗ, может быть признан составной ОО, включающий в себя сам продукт ИТ и его ИТ-среду.

В первом из описанных случаев разработчик ПЗ должен специфицировать минимальный перечень функциональных возможностей, которые обеспечиваются ОО. Решение о разделении ответственности между ОО и ИТ-средой должно основываться на анализе технической выполнимости требований, а также функциональных возможностей продуктов ИТ, которые должны соответствовать ПЗ. Тем не менее, ПЗ должен разрешать соответствующему ОО реализовывать любые идентифицированные в ПЗ требования безопасности для ИТ-среды.

Уровень доверия к реализации ФТБ для ИТ-среды должен быть не ниже уровня доверия к реализации ФТБ объектом оценки. Например, если уровень доверия к реализации функциональных возможностей СУБД по управлению доступом должен соответствовать ОУД4, то будет считаться недостаточным уровень доверия к реализации функций идентификации и аутентификации, ответственность за реализацию которых возложена на ОС (ИТ-среду), соответствующий ОУД2.

10.4.2 Требования безопасности для не ИТ-среды

Требования безопасности для не ИТ-среды в ПЗ и ЗБ могут не включаться, вследствие того что данные требования не имеют непосредственного отношения к реализации ОО.

Необходимость во включении в ПЗ и ЗБ требований безопасности для не ИТ-среды появится в тех случаях, когда сформулированы нетривиальные, с точки зрения реализации, не ИТ-цели безопасности или когда «Обоснование» непосредственно зависит от способа реализации не ИТ-целей безопасности. Последний случай имеет место, если появляется необходимость в детальном согласовании требований безопасности ИТ в ПЗ и ЗБ и соответствующих методов управления безопасностью, с тем чтобы два вида требований (ИТ и не ИТ) находились на одинаковом уровне абстракции.

Следует также отметить, что если какие-либо требования безопасности для не ИТ-среды необходимы, но не включены в ПЗ (вследствие того что они в явном виде не вытекают из не ИТ-целей безопасности), то может стать затруднительной демонстрация пригодности требований безопасности ИТ (см. 13.3.1).

Предпочтительнее (для исключения смешивания различных уровней абстракции) представлять требования безопасности для не ИТ-среды в отдельном разделе «Требования безопасности для не ИТ-среды», а не трактовать их как цели или предположения безопасности. Раздел «Требования безопасности для не ИТ-среды» может охватывать такие аспекты как защита аутентификационных данных, используемых механизмом идентификации и аутентификации (например, пароли), а также конкретные административные требования (например, процедуры расследования обнаруженных вторжений).

Четкая идентификация в ПЗ и ЗБ требований безопасности для не ИТ-среды в дальнейшем будет способствовать включению данных требований в пользовательскую документацию (если соответствующие требования к документации из класса AGD включены в ПЗ и ЗБ).

11 Краткая спецификация объекта оценки

11.1 Введение

Настоящий раздел представляет собой руководство по формированию раздела ЗБ «Краткая спецификация ОО». При этом необходимо учитывать, что аналогичный раздел в ПЗ отсутствует. В раздел «Краткая спецификация ОО» необходимо включать:

a) определение функций безопасности ИТ;

b) ссылки на механизмы или методы защиты, используемые для осуществления функций безопасности ИТ (необязательно);

c) изложение мер доверия к безопасности, которые соответствуют сформулированным требованиям доверия к безопасности.

Содержание раздела «Краткая спецификация ОО» представлено на рисунке 5:

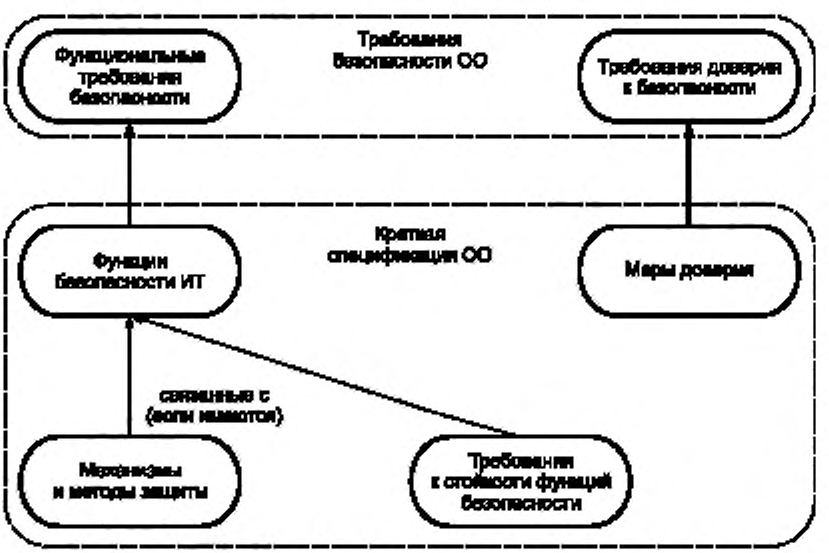

Рисунок 5 — Содержание раздела «Краткая спецификация объекта оценки»

Основное назначение раздела ЗБ «Краткая спецификация ОО» состоит в том, чтобы показать, как конкретным объектом оценки обеспечивается выполнение функций безопасности и мер доверия к безопасности для удовлетворения требований безопасности ИТ. Исходя из этого, должна быть сформирована краткая спецификация ОО, определяющая, каким образом ОО обеспечивает выполнение требований безопасности.

В разделе ЗБ «Краткая спецификация ОО» целесообразно формулировать функции безопасности ИТ так, чтобы представить функциональные возможности безопасности ОО в более понятном для пользователя ЗБ виде по сравнению с ФТБ. В частности:

a) функции безопасности ИТ могут быть изложены так, чтобы показать, что ОО предпринимает для обеспечения безопасности;

b) функции безопасности ИТ могут быть специфицированы так, чтобы более точно отражать документацию ОО, например, путем использования специфической для ОО терминологии. Данное обстоятельство может повысить рентабельность оценки ОО, облегчая верификацию уровней представления ФБО (ЗБ, проектная документация). Один из возможных методов заключается в спецификации одной функции безопасности ИТ, удовлетворяющей нескольким ФТБ, если известно, что эти ФТБ выполняются теми же основными механизмами при проектировании и реализации (разработке) ОО. Данный подход выгоден для сокращения числа доказательств соответствия представления, которое должен обеспечить разработчик;

c) специфическая для конкретного ОО терминология может быть учтена для того, чтобы описания, например, функций безопасности ИТ лучше соотносились с терминологией проекта руководства пользователя или администратора. Может потребоваться введение характерных терминов — таких как «субъект», «объект» или «роль администратора». Поэтому раздел «Краткая спецификация ОО» может быть охарактеризован как развитие требований, которым должен соответствовать конкретный ОО. При этом отсутствует необходимость в описании деталей реализации ОО, его архитектуры или принципов проектирования, или в подробном описании того, как, например, разработчик проводит функциональное тестирование безопасности ОО.

11.2 Спецификация функций безопасности информационных технологий

Как проиллюстрировано в рисунке 5, раздел ЗБ «Краткая спецификация ОО» должен включать в себя спецификацию функций безопасности ОО. Задание по безопасности должно демонстрировать, что функции безопасности ИТ включают в себя все ФТБ, а также то, что каждая функция безопасности ИТ отображается, по крайней мере, на одном ФТБ.

Функции безопасности ИТ, которые определяют основное назначение ОО с точки зрения обеспечения безопасности информации, должны быть рассмотрены более детально. При рассмотрении функций безопасности, соответствующих поддерживаемым ФТБ, функция безопасности ИТ могла бы быть изложена аналогично соответствующему ФТБ. Тем не менее, там, где необходимо, целесообразно пояснить функциональную возможность, например, используя специфическую для ОО терминологию.

При необходимости, функции безопасности могут быть организованы иначе, чем соответствующие ФТБ, и иметь обозначение, отличное от данных ФТБ, что может быть направлено на то, чтобы упростить спецификацию функциональной возможности и облегчить соответствующую оценку, например:

a) функция безопасности ИТ может отображаться более чем на одно ФТБ (например, в случае с поддерживающими функциями) или

b) ФТБ может отображаться более чем на одну функцию безопасности ИТ (например, в случае с функциями, которые определяют основное назначение ОО с точки зрения обеспечения безопасности информации).

При выполнении таких преобразований необходимо:

a) не потерять детали, содержащиеся в ФТБ;

b) не допустить слишком сложного отображения ФТБ на функции безопасности ИТ, увеличения стоимости рассмотрения и оценки ЗБ, а также увеличения вероятности ошибок.

11.3 Спецификация механизмов безопасности

В разделе ЗБ «Краткая спецификация ОО» должно быть показано соответствие функций безопасности ИТ механизмам или методам безопасности, упоминаемым в ЗБ. Типичные механизмы и методы безопасности, упоминаемые в ЗБ, включают в себя алгоритмы шифрования и генерации паролей или заявления соответствия действующему международному или отечественному стандарту.

Необходимо отметить, что ссылки на механизмы безопасности в ЗБ необязательны.

На механизмы безопасности целесообразно ссылаться в следующих случаях:

a) для системы ИТ существует требование использования конкретного механизма безопасности;

b) для продукта ИТ есть необходимость в реализации конкретных механизмов безопасности (например, с учетом рыночного спроса на такие механизмы и методы).

11.4 Спецификация мер доверия к безопасности

В разделе ЗБ «Краткая спецификация ОО» должно быть показано соответствие мер доверия к безопасности и требований доверия к безопасности. При этом должно быть показано, что все требования доверия к безопасности удовлетворены.

Там, где это возможно, меры доверия к безопасности следует определять путем ссылки на соответствующие планы обеспечения качества, жизненного цикла или управления.

На практике, вероятно, для более низких уровней доверия к безопасности раздел ЗБ «Краткая спецификация ОО» не будет содержать значительного объема дополнительной информации, кроме общих утверждений о том, что используются (или будут использоваться) необходимые для удовлетворения требований доверия к безопасности меры доверия. Один из рекомендуемых подходов заключается в демонстрации отображения документации или свидетельств разработчика на соответствующие требования доверия к безопасности.

На более высоких уровнях доверия к безопасности (ОУД 5 и выше) возможно более подробное изложение, например, ссылками на конкретные инструментальные средства, методы или подходы, используемые разработчиком для удовлетворения требований доверия к безопасности, такие как:

a) обозначения, которые необходимо использовать в требуемых формальных спецификациях;

b) методики разработки и модели жизненного цикла;

c) инструментальные средства управления конфигурацией;

d) инструментальные средства анализа покрытия тестами;

e) методы анализа скрытых каналов.

12 Утверждения о соответствии профилей защиты

12.1 Введение

Данный раздел представляет собой руководство по формированию раздела ЗБ «Утверждения о соответствии ПЗ».

В соответствии с приложением С, подраздел С.2.8, ИСО/МЭК 15408-1 требуется включение в каждое ПЗ, о соответствии которому сделано утверждение, следующей информации:

a) ссылки, идентифицирующая ПЗ, о соответствии которому сделано утверждение;

b) конкретизации, выполненной по отношению к ПЗ;

c) дополнения в ЗБ в составе целей и требований безопасности ОО, определенных в ПЗ.

Примечание — частичное соответствие ПЗ неприемлемо; в ЗБ необходимо удовлетворение всех требований ПЗ. Конечно, довольно часто бывает для некоторых целей и требований безопасности из ПЗ, что они удовлетворяются аппаратным обеспечением или другими продуктами безопасности, которые находятся за рамками области оценки в ЗБ. В этом случае необходимо отразить в разделе ЗБ «Обоснование», что сочетанием характеристик безопасности ОО и его среды достигается полное покрытие ПЗ, а также четко отразить эту зависимость в утверждении о соответствии.

Если утверждений о соответствии ПЗ нет, то утверждение об этом — это все, что требуется для данного раздела ЗБ.

12.2 Ссылка на профили защиты

Каждый ПЗ должен быть идентифицирован так, чтобы позволить пользователям ЗБ найти соответствующую спецификацию ПЗ. Рекомендованный способ сделать это — ссылка на запись в реестре пакетов и профилей защиты ИСО (см. [1]); однако, этот реестр не является широко распространенным и используемым. Различные национальные системы оценки ведут реестры ПЗ, что, несомненно, удобнее. Необходимо обеспечить идентификацию конкретной версии и источника ссылки для каждого ПЗ, на который дается ссылка.

12.3 Конкретизация профилей защиты

Если в ПЗ в формулировках требований безопасности ИТ содержат разрешенные операции, которые требуют дальнейшей конкретизации, в этом подразделе ЗБ необходимо поместить результаты конкретизации (замен). Если требуется существенная конкретизация, лучше полностью изложить в ЗБ определенное содержание ПЗ.

12.4 Дополнение профилей защиты

Если в ЗБ удовлетворены цели ОО, не предусмотренные разработчиком ПЗ, в этот подраздел ЗБ необходимо поместить информацию о дополнительных угрозах, политиках, целях и т.д. При этом необходимо отразить покрытие этих дополнительных целей в разделе ЗБ «Обоснование».

13 Разделы «Обоснование» профилей защиты и заданий по безопасности

13.1 Введение

Настоящий раздел представляет собой руководство по формированию раздела ПЗ «Обоснование».

Назначение раздела ПЗ «Обоснование» заключается в том, чтобы показать, как соответствующий профилю защиты ОО обеспечивает эффективный набор контрмер безопасности ИТ в пределах среды безопасности. В частности, раздел ПЗ «Обоснование» показывает, что требования безопасности ИТ удовлетворяют целям безопасности, которые, в свою очередь, учитывают все аспекты среды безопасности ОО. Раздел ПЗ «Обоснование» представляет наибольший интерес для оценщика ПЗ и в то же время может быть полезен для других пользователей ПЗ.

Требования к разделу ПЗ «Обоснование» представлены на рисунке 6.

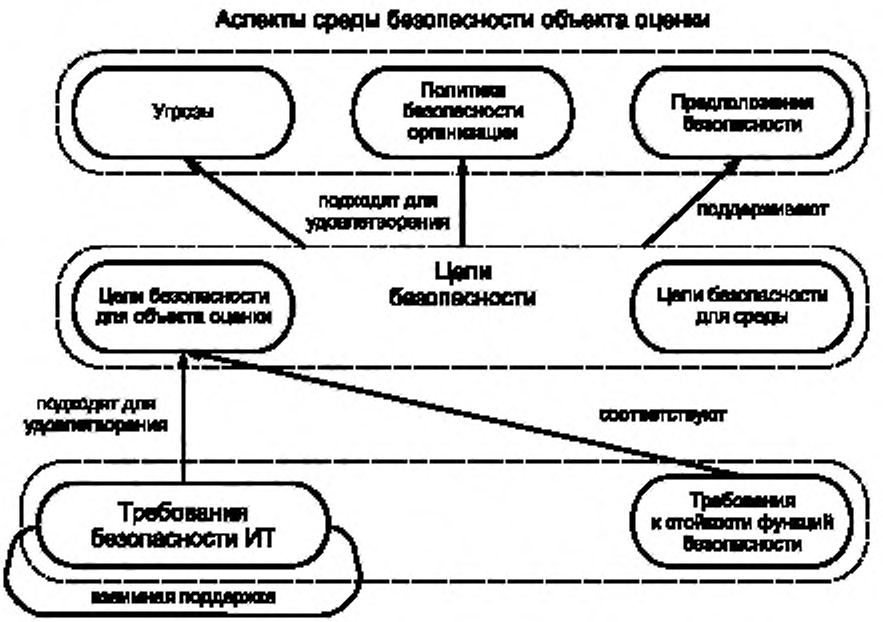

Рисунок 6 — Требования к разделу «Обоснование профиля защиты»

Дополнительно раздел «Обоснование ПЗ» должен показать, что:

a) формулировка требований доверия к безопасности является надлежащей;

b) неудовлетворенные зависимости требований безопасности ИТ, включенных в ПЗ, не являются необходимыми.

В разделе «Обоснование ПЗ» настоятельно рекомендуется использовать таблицы, сопровождаемые, где необходимо, необязательным объяснением, что делает раздел более кратким и упрощает его использование.

13.2 Представление в профилях защиты и заданиях по безопасности обоснования целей безопасности

Обоснование целей безопасности должно показывать, что изложенные цели безопасности охватывают все установленные в разделе ПЗ «Среда безопасности ОО» аспекты среды безопасности ОО. При этом должно быть показано не только то, что цели безопасности охватывают все аспекты среды безопасности ОО, но и необходимость достижения этих целей.

Данные цели могут быть достигнуты следующим образом.

Во-первых, перекрестные ссылки: угрозы, ПБОр, предположения — цели безопасности, охватывающие аспекты среды безопасности ОО, целесообразно представить в форме таблиц.

При этом пользователю ПЗ при изучении этих таблиц должно быть наглядно показано, что:

a) каждая цель безопасности охватывает, по крайней мере, одну угрозу, правило ПБОр или предположение безопасности;

b) каждая угроза, правило ПБОр и предположение безопасности охвачены, по крайней мере, одной целью безопасности.

Во-вторых, необходимо показать, что цели безопасности достаточны для учета всех аспектов среды безопасности ОО. Для этого таблицу соответствия целей безопасности и аспектов среды безопасности ОО целесообразно дополнить следующими необязательными объяснениями:

a) для каждой угрозы — относительно того, что изложенные цели безопасности предусматривают эффективные контрмеры по отношению к угрозам, то есть цели безопасности показывают, что событие, указанное в спецификации угрозы, будет:

- обнаружено, и его последствия компенсированы (или ущерб от его наступления ограничен), либо
- предотвращено (или снижена до приемлемого уровня вероятность его наступления);

b) для ПБОр и всех предположений безопасности — относительно того, каким образом изложенные цели безопасности обеспечивают охват ПБОр и учитывают предположения безопасности.

Объяснение должно показать:

a) роль каждой цели безопасности в противостоянии угрозе или удовлетворении ПБОр;

b) как при помощи целей безопасности для среды безопасности ОО осуществляется поддержка целей безопасности для ОО.

Данный раздел нельзя рассматривать как раздел анализа риска. В то же время при положительной оценке ПЗ и ЗБ он может быть использован как основа для анализа риска организации.

13.3 Представление в профилях защиты и заданиях по безопасности обоснования требований безопасности

13.3.1 Демонстрация пригодности требований безопасности

Назначение этой части раздела ПЗ «Обоснование» заключается в том, чтобы показать, как сформулированные требования безопасности ИТ (в частности, ФТБ) подходят для удовлетворения целей безопасности. При этом необходимо показать, что требования безопасности ИТ являются необходимыми и достаточными. Данная задача может решаться следующим образом.

Во-первых, необходимо разработать таблицу, в которой сопоставить каждую цель безопасности с ФТБ, которое соответствует данной цели. В таблице должно быть показано, что:

a) каждая ФТБ учитывает, по крайней мере, одну цель безопасности;

b) каждая цель безопасности связана, по крайней мере, с одним ФТБ.

Пункта b) будет достаточно для обоснования необходимости каждого ФТБ (то есть будут исключены избыточные ФТБ).

Во-вторых, разработанная таблица должна сопровождаться неформальным объяснением достаточности ФТБ. Данное объяснение должно показать достаточность ФТБ для удовлетворения каждой цели безопасности. Данное объяснение должно охватывать все ФТБ, включенные в ПЗ, в том числе непосредственно удовлетворяющие цели безопасности (основные ФТБ), и предназначенные для их поддержки (поддерживающие ФТБ).

При формировании объяснения необходимо рассмотреть:

a) как и для чего были использованы операции выбора, назначения, итерации и уточнения;

b) как требования безопасности для ОО согласуются с требованиями безопасности для ИТ-среды.

Рекомендуется, но не обязательно, включать в ПЗ объяснение роли включенных в ПЗ требований безопасности для не ИТ-среды.

В следующем разделе приведены рекомендации по представлению обоснования пригодности ТДБ.

13.3.2 Демонстрация пригодности требований доверия к безопасности

Назначение данной части раздела «Обоснование ПЗ» — показать, что требования доверия к безопасности являются надлежащими для рассматриваемого ОО. В этой связи необходимо дать строгое обоснование того, почему набор ТДБ:

a) достаточен для удовлетворения целей безопасности. Например, если ОО должен обеспечивать защиту от нарушителя, обладающего высоким потенциалом нападения (что следует из анализа угроз и целей безопасности), то нецелесообразно в качестве набора требований доверия к безопасности использо-

вать ОУД1, так как требования данного ОУД не предусматривают анализ уязвимостей, которые могут использоваться нарушителями с высоким потенциалом (в частности, ОУД1 не содержит требования семейств AVA_VLA или AVA_SOF);

b) не является избыточным по отношению к среде безопасности и сформулированным целям безопасности;

c) является достижимым, то есть для данного типа ОО сформулированные требования доверия к безопасности являются технически выполнимыми (с точки зрения стоимости и затрат времени на оценку безопасности ОО).

13.3.3 Демонстрация пригодности требований к стойкости функций безопасности

В разделе «Обоснование ПЗ» необходимо показать, что требования к минимальной стойкости функций безопасности и требования к стойкости функций безопасности, заданные в явном виде, согласуются со сформулированными целями безопасности.

Практически это означает, что необходимо представить соответствующее обоснование, принимающее во внимание:

a) присутствующие в формулировках целей безопасности для ОО в явном и неявном видах требования к стойкости функций безопасности;

b) присутствующую в формулировках целей безопасности или в описании среды безопасности информацию о технической компетенции, ресурсах и мотивации нарушителей.

Если данные аспекты уже были учтены при обосновании пригодности требований безопасности, то учитывать их еще раз нет необходимости.

13.3.4 Демонстрация взаимной поддержки требований безопасности

13.3.4.1 Краткий обзор

Назначение данной части раздела «Обоснование ПЗ» заключается в том, чтобы показать, что требования безопасности ИТ (и, в частности, ФТБ) полны и внутренне непротиворечивы, что достигается демонстрацией их взаимной поддержки, а также того, что они представляют собой «интегрированное и эффективное целое». В этих целях рекомендуется следующий подход:

a) демонстрация того, что там, где необходимо, зависимости компонентов функциональных требований и требований доверия к безопасности удовлетворены;

b) демонстрация внутренней непротиворечивости (согласованности) между требованиями безопасности ИТ;

c) демонстрация того, что там, где необходимо, включены поддерживающие ФТБ, предназначенные для защиты механизмов безопасности, реализующих другие ФТБ, от таких нападений как «обход» и «несанкционированное изменение».

Далее рассмотрим каждый из перечисленных аспектов взаимной поддержки.

13.3.4.2 Анализ зависимостей компонентов

Данный анализ наиболее эффективно может быть представлен в форме таблицы или древовидной схемы. Если требования доверия к безопасности целиком базируется на ОУД либо на другом пакете доверия к безопасности, то анализ зависимостей сводится к анализу только зависимостей ФТБ (так как в пакетах доверия зависимости компонентов удовлетворены изначально).

Анализ зависимостей компонентов должен включать в себя:

a) демонстрацию на уровне ФТБ удовлетворения зависимостей для каждой итерации функционального компонента;

b) идентификацию каждой неудовлетворенной зависимости и обоснование отсутствия необходимости в ее удовлетворении.

Необходимость проведения анализа зависимостей на уровне ФТБ обусловлена тем, что, если компонент включают в ПЗ неоднократно путем выполнения операции итерации, то может возникнуть необходимость выполнения операции итерации над компонентами, от которых зависит рассматриваемый компонент. Например, компонент FMT_MSA.3 «Инициализация статических атрибутов» зависит от компонента FMT_MSA.1 «Управление атрибутами безопасности». Если компонент FMT_MSA.3 включают в ПЗ неоднократно в целях инициализации различных атрибутов безопасности, то, вероятно, и FMT_MSA.1 необходимо включить в ПЗ то же число раз в целях управления каждым из рассматриваемых атрибутов. В этом случае вывод о том, что зависимость компонента FMT_MSA.3 надлежащим образом удовлетворена в силу того, что функциональный компонент FMT_MSA.1 включен в ПЗ, будет не полон, так как ФТБ компонента FMT_MSA.1 могут не охватывать все атрибуты безопасности, упомянутые в ФТБ компонента FMT_MSA.3.

Удовлетворение зависимости может не потребоваться, если зависимость не соответствует ОО или не является необходимой, исходя из цели безопасности. Кроме того, зависимость может быть удовлетворена ИТ-средой или каким-либо не ИТ-средством.

Анализ зависимостей должен сопровождаться разработкой таблицы, которая:

a) включает в себя одну или несколько строк (по числу вхождений компонента в ПЗ) для каждого функционального компонента, включенного в ПЗ;

b) назначает уникальную метку или номер каждой строке с тем, чтобы каждое ФТБ было идентифицировано уникальным образом;

c) идентифицирует функциональный компонент, ассоциированный с каждой строкой;

d) для каждого функционального компонента формирует список зависимостей от других компонентов в соответствии со стандартами серии ИСО/МЭК 15408;

e) для каждой идентифицированной зависимости определяет в качестве ссылки метку или номер строки, в которой зависимость удовлетворяется либо объясняет, почему нет необходимости в удовлетворении зависимости.

Демонстрация удовлетворения зависимостей компонентов доверия к безопасности должна быть относительно простой.

Если в ПЗ используется какой-либо пакет доверия к безопасности (например, ОУД, соответствующий требованиям стандартов серии ИСО/МЭК 15408), то в разделе «Обоснование ПЗ» можно констатировать, что все зависимости компонентов доверия к безопасности удовлетворены.

Если в ПЗ включены расширенные требования доверия к безопасности, то в разделе «Обоснование ПЗ» должно быть показано, что все дополнительные зависимости удовлетворены. В стандартах серии ИСО/МЭК 15408 определено лишь небольшое число зависимостей «функциональные требования — требования доверия». Данные зависимости также могут быть представлены в описанной выше таблице. Например, если ПЗ включает FPT_RCV.1, который имеет зависимость от AGD_ADM.1, а заданный оценочный уровень доверия к безопасности — ОУД4, тогда запись в такой таблице должна быть ОУД4.

Анализ зависимостей некоторым образом демонстрирует взаимную поддержку требований безопасности. Так, если функциональный компонент А зависит от функционального компонента В, то компонент В является поддерживающим для компонента А.

13.3.4.3 Внутренняя непротиворечивость

Демонстрацию внутренней непротиворечивости требований безопасности ИТ рассмотрим на примере ФТБ. Так, если ПЗ включает в себя требования к подотчетности и, в то же время, анонимности действий пользователя, то в разделе «Обоснование ПЗ» должно быть показано, что эти требования не противоречат друг другу. В данном случае требуется показать, что в качестве событий аудита, требующих подотчетности пользователя, не рассматриваются те, для которых требуется анонимность.

13.3.4.4 Защита от атак на механизмы, реализующие ФТБ

Рассмотрение данного аспекта взаимной поддержки требований целесообразно только для ФТБ, так как демонстрация взаимной поддержки требований, имеющей отношение к требованиям доверия к безопасности, тривиальна:

a) по умолчанию ТДБ поддерживают ФТБ, так как они обеспечивают уверенность в том, что функциональные требования удовлетворены;

b) имеется незначительное число случаев, когда ФТБ поддерживают ТДБ, и это должно быть учтено при формировании «Обоснования ПЗ». Например:

компоненты семейства FPT_SEP «Разделение домена» поддерживают компоненты семейства ADV_HLD «Проект верхнего уровня», способствуя проведению соответствующего разбиения;

c) можно утверждать, что ТДБ являются взаимно поддерживающими и все их зависимости удовлетворены.

В соответствии с 10.2.1, поддерживающие ФТБ могут способствовать защите механизмов, реализующих основные ФТБ, от нападений, связанных со скрытыми мотивами нарушителя, способствующими возрастанию одной или нескольких угроз, которым должны противостоять механизмы, реализующие основные ФТБ. Взаимная поддержка охватывает как этот аспект взаимной поддержки, так и аспект поддержки, связанный с зависимостями требований безопасности, определенными в стандартах серии ИСО/МЭК 15408.

Рассмотрение взаимной поддержки между ФТБ, не охваченными анализом зависимостей, должно включать в себя рассмотрение:

a) ФТБ, направленных на предотвращение обхода механизмов, реализующих другие ФТБ;

b) ФТБ, направленных на предотвращение несанкционированного воздействия на механизмы, реализующие другие ФТБ (включая атрибуты безопасности и другие данные, целостность которых является критичной для ФТБ);

c) ФТБ, препятствующих несанкционированному отключению механизмов, реализующих другие ФТБ;

d) ФТБ, предназначенных как для обнаружения неправильной настройки механизмов, реализующих другие ФТБ, так и направленных на них нападений.

Для предотвращения обхода механизмов, реализующих ФТБ, в ПЗ обычно включают компонент FPT_RVM «Невозможность обхода ПБО». Если реализация функциональных требований безопасности включает в себя идентификацию пользователя, то требования аутентификации пользователя (использование компонентов семейства FIA_UAU) должны быть также направлены на предотвращение обхода механизмов, реализующих рассматриваемые ФТБ. Необходимо отметить, что для предотвращения обхода не все ФТБ нуждаются в поддержке со стороны других ФТБ. Приведем несколько таких случаев:

a) выдача разрешения на вызов функции возлагается не на ФБО, а на пользователя или администратора, например, при использовании ФТБ, базирующихся на компонентах семейства FDP_DAU «Аутентификация данных»;

b) формулировка ФТБ предусматривает вызов функции всегда, когда это необходимо, следовательно, ФТБ не может быть обойдено, если ФБО удовлетворяет ФТБ, например, если речь идет о ФТБ, базирующемся на компонентах семейства FDP_RIP «Защита остаточной информации».

Несанкционированное воздействие, в принципе, возможно для всех механизмов, реализующих ФТБ. Подобное воздействие может быть предотвращено посредством выполнения:

a) ФТБ на основе компонентов семейства FPT_SEP «Разделение домена», направленных на предотвращение вмешательства посторонних или воздействия недоверенных субъектов;

b) ФТБ на основе компонентов семейства FPT_PHP «Физическая защита ФБО», направленных на обнаружение и противодействие физическому вмешательству;

c) ФТБ, базирующихся на компонентах управления безопасностью, таких как FMT_MSA.1 «Управление атрибутами безопасности», ограничивающих возможность изменения данных конфигурации или атрибутов безопасности;

d) ФТБ, базирующихся на таких компонентах, как FMT_MTD.1 «Управление данными ФБО» или FAU_STG.1 «Защищенное хранение данных аудита», направленных на защиту целостности критичных по безопасности данных;

e) компонентов семейства FPT_TRP «Доверенный маршрут», направленных на предотвращение воздействий, основанных на обмане ФБО (например, путем использования программ захвата паролей).

Деактивация возможна по отношению не ко всем механизмам, реализующим ФТБ, которые определены в ПЗ. Деактивация возможна в случае проведения аудита безопасности; семейство FAU_STG «Хранение событий аудита безопасности» включает в себя требования, направленные на предотвращение возможности деактивации функций аудита безопасности, связанных с заполнением журнала аудита. ФТБ, основанные на использовании компонента FMT_MOF.1 «Управление поведением (режимом выполнения) функций безопасности», также могут быть направлены на предотвращение деактивации некоторых функций безопасности.

Функции обнаружения, так же, как и аудит безопасности, обеспечивают поддержку других ФТБ, способствуя обнаружению атак или неправильной конфигурации, которая делает ОО уязвимым для атак. Другие функции обнаружения включают в себя компоненты семейств FDP_SDI «Целостность хранимых данных» и FPT_PHP «Физическая защита ФБО».

13.3.5 Демонстрация соответствия мер доверия к безопасности требованиям доверия к безопасности

Назначение данной части «Обоснования ЗБ» заключается в том, чтобы показать, как изложенные меры доверия к безопасности надлежащим образом отвечают требованиям доверия к безопасности. Предлагаемый подход к решению данной задачи предусматривает представление соответствия мер доверия к безопасности требованиям доверия к безопасности, с целью показать, что каждое требование доверия к безопасности учтено. Если конкретные меры доверия к безопасности идентифицированы (см. 11.4), то рассматриваемое соответствие лучше всего может быть представлено в виде таблицы. Эта таблица должна сопровождаться кратким пояснением того, как предполагается выполнять требования доверия к безопасности. Следует отметить, что окончательный вывод о пригодности мер доверия к безопасности может быть сделан только в ходе оценки безопасности ОО. Поэтому в ЗБ нет необходимости представлять детальное обоснование приемлемости мер доверия к безопасности.

Особое внимание этой части «Обоснования ЗБ» будет уделяться в случае, если ЗБ включает в себя ТДБ, которые требуют применения конкретных методов, предполагающих высокий уровень доверия к безопасности (например, анализ скрытых каналов или использование формальных методов).

13.3.6 Демонстрация соответствия задания по безопасности профилям защиты

В данной части «Обоснования ЗБ» необходимо идентифицировать профили защиты, соответствие которым требуется для ЗБ, и показать, что:

a) все цели безопасности, сформулированные в профилях защиты, включены в задание по безопасности, а все уточнения целей безопасности обоснованы;

b) все требования безопасности, сформулированные в профилях защиты, включены в задание по безопасности, а все уточнения или другие операции над требованиями безопасности из ПЗ обоснованы;

c) требования безопасности, включенные в ЗБ, не противоречат требованиям безопасности, включенным в ПЗ.

Если ЗБ включает только требования безопасности из профилей защиты (дословно или в виде ссылки), то проведение дальнейшего анализа не требуется. Анализ необходим, если ЗБ включает в себя дополнительные детали. В этом случае необходимо показать, что эти детали обоснованы и не противоречат содержанию ПЗ.

Кроме того, если профили защиты содержат незавершенные операции над требованиями безопасности, предусматривая выполнения операций назначения и выбора разработчиком ЗБ, то из анализа ЗБ должно следовать, что все незавершенные в ПЗ операции завершены.

13.3.7 Демонстрация того, что функции безопасности удовлетворяют функциональным требованиям безопасности

Назначение данной части «Обоснования ЗБ» заключается в том, чтобы показать, что функции безопасности ИТ пригодны для удовлетворения всех ФТБ, включенных в ЗБ (а не только тех ФТБ, которые встречаются в профилях защиты, на которые ссылается ЗБ).

Отображение функций безопасности ИТ на ФТБ целесообразно представить в форме таблицы. Из таблицы должно следовать, что:

a) каждое ФТБ отображено, по крайней мере, на одну функцию безопасности ИТ;

b) каждая функция безопасности ИТ отображена, по крайней мере, на одно ФТБ.

В дополнение к таблице целесообразно пояснить, как удовлетворяются некоторые конкретные ФТБ. Такое пояснение может потребоваться, например, если сразу несколько функций безопасности ИТ отображаются на одно ФТБ.

14 Профили защиты и задания по безопасности для составных объектов оценки и объектов оценки, входящих в состав других объектов оценки

14.1 Введение

Настоящий раздел содержит рекомендации по решению конкретных проблем, связанных со следующими случаями композиции:

a) ПЗ и ЗБ формируют для составного ОО, который состоит из двух или более компонентов (которые также могут быть составными объектами), на каждый из которых имеются отдельные ПЗ или ЗБ (далее — ПЗ ОО-компонента или ЗБ ОО-компонента);

b) ПЗ и ЗБ формируют для ОО-компонента, в которых определяются зависимости от ИТ-среды, которая включает в себя другие ОО-компоненты, являющиеся частью составного ОО (заметим, что могут также существовать зависимости, связанные с требованиями для не ИТ-среды, однако их не обязательно включать в ПЗ и ЗБ).

Существует несколько возможных сценариев декомпозиции, например:

a) ЗБ составного ОО может формироваться, когда особенности ОО-компонентов уже известны, и ЗБ для этих компонентов уже существуют. В этом случае главная цель ЗБ сложного ОО будет заключаться в определении аспектов среды безопасности, которые должны быть учтены ОО-компонентами как единым целым, и демонстрации того, что все рассматриваемые аспекты среды безопасности учтены;

b) в ПЗ составного ОО может быть проведена декомпозиция задач для отдельных ОО-компонентов в целях последующего формирования ПЗ для них. Задания по безопасности ОО-компонентов должны быть согласованы с требованиями ПЗ ОО-компонентов.

Данный подход наиболее приемлем для больших систем, которые включают большое число компонентов. Выбор наилучшего способа декомпозиции составного ОО на ОО-компоненты в целях последующего формирования ПЗ или ЗБ ОО-компонентов возлагается на разработчика ПЗ и ЗБ.

14.2 Составной объект оценки

14.2.1 Описательные части профиля защиты и задания по безопасности

Описательные части ПЗ и ЗБ ОО-компонента и, в частности, раздел «Описание ОО», должны содержать описание составного ОО и всех его компонентов. Раздел ПЗ или ЗБ ОО-компонента «Описание ОО» должен содержать описание функциональных возможностей ОО-компонента; эта информация впоследствии обобщается в ПЗ и ЗБ составных ОО.

14.2.2 Среда безопасности объекта оценки

Раздел ПЗ или ЗБ составного ОО «Среда безопасности ОО» может:

a) целиком определять среду безопасности для составного ОО (посредством ссылки на один или более ПЗ, соответствие которым заявляется, с включением дополнительных подробностей, где это необходимо) либо

b) представлять описание среды безопасности лишь в общих чертах и содержать ссылку на ПЗ или ЗБ ОО-компонентов для детального изложения угроз, ПБОр и предположений безопасности.

Первый из перечисленных подходов предпочтителен в случае, если в первую очередь формируется ПЗ составного ОО и существует большая степень однородности ОО-компонентов по отношению к активам, подлежащим защите, и угрозам этим активам. В этом случае в ПЗ ОО-компонентов может быть помещена ссылка на описание среды безопасности ОО из ПЗ составного ОО для исключения повторения информации.

Второй подход является более предпочтительным, если ПЗ или ЗБ для ОО-компонентов уже существуют. Данный подход целесообразен, когда разным подмножествам компонентов составного ОО соответствуют разные подмножества активов, подлежащих защите. В этом случае их полное описание в ПЗ и ЗБ составного ОО было бы чрезвычайно сложным, а, следовательно, трудным для понимания пользователем ПЗ и ЗБ. Поэтому описание подлежащих защите активов и источников угроз предпочтительнее помещать в ПЗ или ЗБ ОО-компонентов.

Необходимо отметить, что в соответствии со стандартами серии ИСО/МЭК 15408, если ОО является физически распределенным, может возникнуть необходимость (для большей ясности) выделить отдельные домены среды безопасности ОО и анализировать аспекты среды безопасности (угрозы, ПБОр и предположения безопасности) отдельно для каждого домена.

Независимо от используемого подхода необходимо обеспечить непротиворечивость и согласованность между ПЗ и ЗБ составного ОО и ПЗ и ЗБ ОО-компонентов.

14.2.3 Цели безопасности

Изложение целей безопасности целесообразно осуществить в ПЗ и ЗБ ОО-компонентов. При этом нет необходимости повторять полные формулировки этих целей безопасности в ПЗ и ЗБ составного ОО, однако в ПЗ и ЗБ составного ОО необходимо показать соответствие компонентов требований и целей безопасности.

Если цели безопасности, изложенные в ЗБ составного ОО, не полностью эквивалентны целям безопасности для ОО-компонентов, то целесообразно представить отображение целей безопасности для составного ОО на цели безопасности для ОО-компонентов.

14.2.4 Требования безопасности

Изложение требований безопасности ИТ целесообразно осуществлять в ПЗ и ЗБ ОО-компонентов. При этом нет необходимости приводить полные формулировки этих требований в ПЗ и ЗБ составного ОО. Тем не менее в ПЗ и ЗБ составного ОО целесообразно представить отображение ФТБ на ОО-компоненты и уровень доверия к этим компонентам. Если для составного ОО был установлен единый уровень доверия к безопасности, то целесообразно сформулировать требования доверия к безопасности в ПЗ и ЗБ составного ОО, а в ПЗ и ЗБ ОО-компонентов поместить ссылки на эти требования.

В случаях, если ОО-компоненты имеют различные уровни доверия к безопасности, для ПЗ и ЗБ составного ОО может быть сформирован «профиль доверия к безопасности», что может быть целесообразно, например, если какой-либо ОО-компонент предназначен для защиты особо ценных либо наиболее привлекательных для нарушителя активов. Такой подход в явном виде не противоречит требованиям стандартов серии ИСО/МЭК 15408, но при этом необходимо контролировать, чтобы в ПЗ и ЗБ не было случая, когда ФТБ одного ОО-компонента зависели бы от ФТБ другого компонента, который подлежит проверке на соответствие более низкому уровню доверия к безопасности.

Отметим, что, если ПЗ и ЗБ составного ОО специфицирует «профиль доверия к безопасности», то нет необходимости определять общий уровень доверия к безопасности, за исключением, возможно, указания на минимальный уровень доверия к безопасности ОО-компонентов.

Целесообразно при разработке многокомпонентных систем минимизировать число ОО-компонентов с высокими требованиями доверия к безопасности, так как это связано со стоимостью разработки и оценки. Основной подход при этом заключается в изоляции активов, нуждающихся в наибольшей защите, в рамках небольшого числа ОО-компонентов с высокими требованиями доверия к безопасности (например, изоляция главного ключа центра сертификации).

При формировании ПЗ и ЗБ составного ОО необходимо обеспечить взаимное удовлетворение зависимостей ОО-компонентов, если, конечно, сам составной ОО не является компонентом большего ОО. Раздел «Требования безопасности ИТ» ПЗ и ЗБ составного ОО должен идентифицировать все неудовлетворенные зависимости (если имеются), которые должны быть удовлетворены ИТ-средой составного ОО (если ИТ-среда существует).

14.2.5 Краткая спецификация объекта оценки

Целесообразно в ЗБ составного ОО помещать ссылку на краткие спецификации из ЗБ ОО-компонентов, а не излагать все детали заново. Так как раздел ЗБ «Требования безопасности ИТ» составного ОО уже будет содержать информацию о соответствии требований безопасности ИТ и ОО-компонентов, то нет особой необходимости в перечислении функций безопасности ИТ, обеспечиваемых каждым ОО-компонентом.

Если краткие спецификации ОО в ЗБ ОО-компонентов идентифицируют дополнительные или более детальные зависимости от других ОО-компонентов, то необходимо в краткой спецификации составного ОО показать, что рассматриваемые зависимости удовлетворены для составного ОО в целом либо специфицировать неудовлетворенные зависимости в качестве требований безопасности для ИТ-среды составного ОО.

14.2.6 Обоснование профиля защиты

В профиле защиты для составного ОО необходимо показать, что набор целей безопасности учитывает все аспекты среды безопасности ОО, а требования безопасности ИТ удовлетворяют целям безопасности. Для некоторых аспектов раздела ПЗ «Обоснование» возможна ссылка на информацию из разделов «Обоснование» ПЗ ОО-компонентов. Целесообразно придерживаться следующих принципов:

1) для того, чтобы показать, что набор целей безопасности для составного ОО в целом учитывает аспекты среды безопасности для составного ОО, в первую очередь необходимо представить отображение каждой цели безопасности для ОО-компонентов на угрозы и ПБОр, приведенные в ПЗ составного ОО. Затем необходимо пояснить, почему цели безопасности направлены на то, чтобы противостоять угрозам и удовлетворять ПБОр. Ссылка на разделы «Обоснование» ПЗ отдельных ОО-компонентов возможна только в случае точного отображения угроз и/или ПБОр для составного ОО на угрозы и/или ПБОр для ОО-компонентов;

2) для того, чтобы показать, что набор требований безопасности ИТ является надлежащим для удовлетворения целей безопасности, целесообразно ссылаться на разделы «Обоснование» ПЗ для отдельных ОО-компонентов, если ОО-компонент удовлетворяет цели безопасности для составного ОО. В ПЗ для составного ОО необходимо показать, что все цели безопасности для составного ОО надлежащим образом удовлетворяются, по крайней мере, одним ОО-компонентом, или, что цель удовлетворяется благодаря взаимодействию двух или более ОО-компонентов;

3) для того, чтобы показать, что зависимости требований безопасности удовлетворяются, можно использовать ссылку на разделы «Обоснование» ПЗ отдельных ОО-компонентов. При этом необходимо обеспечить, чтобы в разделе «Обоснование» ПЗ составного ОО:

- демонстрировалось, что все зависимости, определенные в ПЗ ОО-компонентов как подлежащие удовлетворению ИТ-средой, удовлетворяются другими ОО-компонентами, входящими в составной ОО, либо идентифицированы (в ПЗ составного ОО) как зависимости, подлежащие удовлетворению ИТ-средой для составного ОО,

- рассматривались зависимости, которые в разделах «Обоснование» ПЗ ОО-компонентов обосновывались как не подлежащие удовлетворению, но с учетом среды безопасности составного ОО все-таки подлежат удовлетворению;

4) для демонстрации взаимной поддержки требований безопасности ИТ можно использовать результаты анализа взаимосвязей между требованиями безопасности ИТ в рамках каждого ОО-компонента, представленные в разделах «Обоснование» ПЗ ОО-компонентов. При этом в разделе «Обоснование» ПЗ составного ОО необходимо рассмотреть взаимосвязи и зависимости между требованиями безопасности ИТ различных ОО-компонентов, если они не были должным образом учтены в разделах «Обоснование» ПЗ для ОО-компонентов.

14.2.7 Обоснование задания по безопасности

Рекомендации по формированию раздела ЗБ «Обоснование» во многом подобны рекомендациям по формированию раздела «Обоснование» ПЗ составного ОО. В частности:

a) для демонстрации того, что функции безопасности ИТ и меры доверия подходят для удовлетворения требований безопасности ОО, можно просто использовать ссылку на разделы «Обоснование» ЗБ для ОО-компонентов;

b) для демонстрации взаимной поддержки функций безопасности ИТ можно использовать результаты анализа взаимной поддержки функций безопасности ИТ в рамках каждого ОО-компонента, представленные в разделах «Обоснование» ЗБ для ОО-компонентов. При этом в разделе «Обоснование» ЗБ составного ОО необходимо рассмотреть взаимосвязи и зависимости между функциями безопасности ИТ различных ОО-компонентов.

14.3 Объект оценки — компонент

14.3.1 Описательные части профиля защиты и задания по безопасности

Если ОО представляет собой компонент составного ОО, то на это должно быть ясно указано в описательных частях ПЗ и ЗБ (в частности, в разделе «Описание ОО»). Если ОО представляет собой компонент конкретного составного ОО, другие компоненты которого также известны, то в «Описании ОО» следует идентифицировать те ОО-компоненты, с которыми взаимодействует рассматриваемый ОО-компонент (и которые представляют собой всю ИТ-среду для рассматриваемого ОО-компонента или ее часть). В других случаях «Описание ОО» должно описывать типы составных ОО, которые могли бы использовать данный ОО-компонент.

14.3.2 Среда безопасности объекта оценки

Раздел ПЗ и ЗБ «Среда безопасности ОО» предназначен для определения границы среды безопасности ОО-компонента и, с точки зрения оценщика, границы оценки ОО-компонента. Например, среда безопасности ИТ для ОО-компонента может включать в себя в том числе другие ИТ-компоненты, с которыми предполагается взаимодействие ОО-компонента. В таких случаях наличие зависимостей ОО-компонента от ИТ-среды следует трактовать как предположение о среде безопасности ОО. При формулировании такого предположения следует избегать включения деталей реализации, которые специфицируются в ПЗ и ЗБ.

ОО-компоненту может быть предписана необходимость взаимодействия с другими устройствами в рамках ИТ-среды. В этом случае в ПЗ и ЗБ должно быть включено соответствующее положение ПБОр.

14.3.3 Цели безопасности

Любые зависимости от ИТ-среды следует трактовать как цели безопасности для ИТ-среды.

Следует отметить, что соответствующий профилю защиты ОО-компонент может сам по себе удовлетворять одной или более целям безопасности, ответственность за достижение которых возлагается в ПЗ на ИТ-среду. Например, СУБД может удовлетворять цели безопасности, связанной с идентификацией и аутентификацией, в то время как в ПЗ достижение данной цели безопасности возложено на операционную систему, под управлением которой работает СУБД.

Если ПБОр содержит предписание ОО взаимодействовать с другими устройствами ИТ-среды, то необходимо сформулировать соответствующую цель безопасности для ОО.

14.3.4 Требования безопасности

Требования безопасности для ИТ-среды ОО-компонента должны, где это возможно, идентифицировать конкретные ОО-компоненты, на которые возлагается удовлетворение данных требований безопасности.

Примечание — Требования безопасности для среды могут быть определены путем заявления о соответствии другим ПЗ.

14.3.5 Краткая спецификация объекта оценки

В виде подэтапа спецификации функций безопасности ИТ может потребоваться уточнение ряда требований безопасности для ИТ-среды. Например, ОО может использовать определенный интерфейс с операционной системой для регистрации генерируемых данных аудита безопасности. Таким образом, если ОО предполагает функционировать в составе конкретного составного ОО, то все уточненные требования должны отображаться на конкретные компоненты составного ОО.

14.3.6 Обоснование профиля защиты

Если в ПЗ определяются требования безопасности для ИТ-среды, то они должны быть рассмотрены в разделе ПЗ «Обоснование». В частности необходимо:

a) продемонстрировать, каким образом требования безопасности для ИТ-среды способствуют удовлетворению целей безопасности для ОО;

b) показать, что все зависимости требований безопасности для ИТ-среды удовлетворены;

c) продемонстрировать взаимную поддержку требований безопасности для ИТ-среды и показать поддержку с их стороны по отношению к требованиям безопасности ИТ.

14.3.7 Обоснование задания по безопасности

Если в ЗБ определяются требования безопасности для ИТ-среды, то они должны быть рассмотрены в разделе ЗБ «Обоснование». В частности, должны быть рассмотрены вопросы, аналогичные тем, которые рассматриваются в ПЗ (см. 14.2.6). Дополнительные детали, например, связанные с зависимостями, введенными в ЗБ, должны быть также рассмотрены в соответствующих частях ЗБ «Обоснование».

15 Функциональные пакеты и пакеты требований доверия к безопасности

15.1 Общая информация

Настоящий раздел содержит методические рекомендации по формированию пакетов требований безопасности. Концепция пакета требований представлена в 4.4.2.1 ИСО/МЭК 15408-1. Пакет можно охарактеризовать следующим образом:

a) представляет собой промежуточную комбинацию функциональных компонентов или компонентов требований доверия к безопасности;

b) предназначен для:

- многократного использования при создании более крупных пакетов, профилей защиты и заданий по безопасности,
- определения требований безопасности, которые считаются подходящими для удовлетворения определенного подмножества целей безопасности.

Основное преимущество пакетов требований заключается в снижении рабочей нагрузки на разработчиков ПЗ и ЗБ при формулировании требований безопасности ИТ (см. раздел 10).

Оценочные уровни доверия к безопасности, определенные в разделе 6 ИСО/МЭК 15408-3, необходимо рассматривать как пример оформления пакетов требований доверия к безопасности.

15.2 Формирование функционального пакета

15.2.1 Разработчики функциональных пакетов

В качестве разработчика функционального пакета (ФП) может выступать любая организация, заинтересованная в продвижении стандартизованной спецификации функциональных возможностей обеспечения безопасности. Разработка ФП может рассматриваться как первый шаг при формировании профиля защиты (или семейства ПЗ) либо как составная часть ЗБ. ФП может, например, быть использован организацией для спецификации стандартного набора функциональных требований безопасности, которые должны удовлетворить поставщики продукта.

15.2.2 Содержимое функционального пакета

ФП представляет собой спецификацию функциональных требований безопасности. Для формулирования данных ФТБ необходимо использовать рекомендации в соответствии с 10.1. Отдельные ФТБ, входящие в ФП, должны либо идентифицировать стандартизованные функциональные компоненты в соответствии со стандартами серии ИСО/МЭК 15408, либо представлять собой требования, сформулированные в явном виде и по форме представления соответствующие оформлению компонентов требований стандартов серии ИСО/МЭК 15408. При этом сформулированные в таком виде требования должны сопровождаться четким обоснованием того, почему их необходимо было формулировать в явном виде. Совокупность ФТБ, определенных в ФП, должна быть направлена на удовлетворение определенного подмножества целей безопасности.

При разработке ФП можно использовать один из двух подходов (или их комбинацию):

- формировать совокупность ФТБ, исходя из уже изложенных конкретных целей безопасности;
- формулировать цели безопасности, исходя из определенной совокупности ФТБ.

15.2.3 Информация, включаемая в функциональный пакет

Кроме собственно функциональных требований, в ФП следует включать следующую информацию, представляющую интерес при разработке больших ФП, ПЗ и ЗБ:

a) идентификацию целей безопасности, которым удовлетворяют ФТБ;

b) информацию об использовании функциональных компонентов в соответствии со стандартами серии ИСО/МЭК 15408 или об отклонениях от требований стандартов серии ИСО/МЭК 15408;

c) обоснование ФТБ, включая:

1) демонстрацию адекватности ФТБ для удовлетворения идентифицированных целей безопасности,

2) анализ зависимостей между ФТБ,

3) демонстрацию взаимной поддержки ФТБ.

Вместе с тем не рекомендуется, чтобы в ФП включалась формальная спецификация целей безопасности и полное обоснование требований безопасности, удовлетворяющие критериям доверия к безопасности в соответствии со стандартами серии ИСО/МЭК 15408. Это связано с тем, что цели безопасности для конкретного ОО будут зависеть от среды безопасности ОО. Целесообразно, чтобы ФП содержал в виде замечаний по применению любую информацию, полезную при формировании обоснований ПЗ или ЗБ.

15.3 Спецификация пакета требований доверия к безопасности

15.3.1 Разработчики пакетов требований доверия к безопасности

В качестве разработчиков пакетов требований доверия к безопасности (ПД) может выступать орган по сертификации, а также любая организация, которая проводит оценку продуктов и систем ИТ. Такие пакеты могут определять альтернативные уровни доверия к безопасности либо определять комбинацию компонентов класса АМА «Поддержка доверия к безопасности».

15.3.2 Содержание пакета требований доверия к безопасности

Пакет требований доверия к безопасности представляет собой спецификацию требований доверия к безопасности. Для формулирования этих требований необходимо использовать рекомендации в соответствии с 10.2. Отдельные ТДБ, входящие в ПД, должны идентифицировать стандартизованные компоненты доверия к безопасности, определенные в ИСО/МЭК 15408-3, либо представлять собой требования, сформулированные в явном виде и по форме представления соответствующие оформлению компонентов требований в соответствии со стандартами серии ИСО/МЭК 15408. При этом сформулированные в явном виде требования должны сопровождаться четким обоснованием того, почему их было необходимо формулировать в явном виде.

15.3.3 Информация, включаемая в пакет доверия

В целях многократного использования ПД должен включать в себя информацию о назначении ТДБ. Эта информация позволяет пользователю ПД определить, в каких случаях его целесообразно использовать и какие ТДБ к нему можно добавить.

Спецификацию ОУД, представленную в стандартах серии ИСО/МЭК 15408, необходимо рассматривать в качестве образца представления пакетов требований доверия к безопасности.

Приложение А
(рекомендуемое)

Резюме

А.1 Введение

Настоящее приложение содержит описание ключевых вопросов, изложенных в разделах 7—13.

А.2 Введение профиля защиты и задания по безопасности

В раздел «Введение ПЗ и ЗБ» необходимо включать обзор проблемы безопасности, которая подлежит решению в ПЗ и ЗБ, а также краткий обзор того, как ПЗ и ЗБ способствует решению проблемы безопасности. При этом необходимо обеспечить их соответствие содержанию ПЗ и ЗБ.

А.3 Описание объекта оценки

В раздел ПЗ и ЗБ «Описание ОО» необходимо включать описание всех функциональных возможностей ОО, а не только характеристик безопасности (если только обеспечение безопасности не является единственным предназначением ОО).

В раздел ПЗ «Описание ОО» описание «границ ОО» допускается не включать. Описание «границ ОО» – это описание того, что включает и не включает в себя ОО.

В раздел ЗБ «Описание ОО» описание «границ ОО» включают обязательно. «Границы ОО» должны быть определены как в части аппаратных и программных компонентов (физические границы), так и в части функциональных характеристик безопасности ОО.

Необходимо обеспечить соответствие раздела «Описание ОО» содержанию ПЗ и ЗБ.

А.4 Среда безопасности объекта оценки

А.4.1 Предположения безопасности

А.4.1.1 Идентификация

В подраздел «Предположения безопасности» необходимо включать перечень предположений относительно среды безопасности ОО, связанных с вопросами физической защиты, персоналом и вопросами связности среды и ОО.

А.4.1.2 Спецификация

Необходимо, по возможности, при формулировании предположений безопасности избегать включения любых деталей, касающихся функций безопасности ОО.

А.4.1.3 Представление

Для упрощения ссылок необходимо, чтобы каждое предположение безопасности было пронумеровано или имело уникальную метку.

А.4.2 Угрозы

А.4.2.1 Идентификация

При идентификации угроз необходимо описать активы ИТ, подлежащие защите, методы нападений и другие нежелательные события, которые необходимо учитывать при защите, и источники угроз.

А.4.2.2 Спецификация

При спецификации необходимо обеспечить четкое описание угроз путем представления детальной информации относительно источника угрозы, активов ИТ, подверженных нападению, и метода нападения.

При этом необходимо обеспечить краткость в описании каждой отдельной угрозы с тем, чтобы минимизировать перекрытие описания различных угроз.

Описание угроз должно затрагивать только те потенциальные события, которые непосредственно могут привести к компрометации активов, подлежащих защите. В ПЗ и ЗБ не рекомендуется включать описание угроз, связанных с недостатками в реализации ОО.

А.4.2.3 Представление

Для упрощения ссылок необходимо, чтобы каждая угроза имела уникальную метку.

А.4.3 Политика безопасности организации

А.4.3.1 Идентификация

Любые требования политики безопасности, которые не могут быть сформулированы исключительно на основе анализа угроз, необходимо трактовать как правила ПБОр.

А.4.3.2 Спецификация

Необходимо определить ПБОр в виде совокупности правил, предназначенных для реализации ОО и/или его средой (например, правила управления доступом).

А.4.3.3 Представление

Для упрощения ссылок необходимо, чтобы каждое правило ПБОр имело уникальную метку.

А.5 Цели безопасности

А.5.1 Идентификация

Если функциональные требования безопасности уже определены, то для каждого основного ФТБ (или группы ФТБ) необходимо поставить в соответствие некоторую цель безопасности для ОО.

Необходимо идентифицировать цели безопасности, ответственность за достижение которых возложено на ИТ-среду (например, на ОС, под управлением которой работает ОО, или на некоторую другую платформу, на базе которой работает ОО), как цели безопасности для среды.

Необходимо идентифицировать процедуры, связанные с использованием контрмер ОО, как цели безопасности для среды.

А.5.2 Спецификация

При изложении целей безопасности для ОО необходимо установить (в заданном разработчиком ПЗ и ЗБ объеме) возлагаемую на ОО ответственность за противостояние угрозам и следование ПБОр. При этом следует избегать того, чтобы формулировка целей безопасности являлась бы простым повторением, хотя и в несколько иной форме, информации, содержащейся в описании угроз и ПБОр, а также — деталей реализации.

Изложение целей безопасности для ОО, направленных на противостояние угрозам, должно ясно свидетельствовать, к какому типу (цели предупредительного характера, цели обнаружения или цели реагирования) принадлежит каждая цель безопасности.

А.5.3 Представление

А.6 Требования безопасности информационных технологий

А.6.1 Функциональные требования безопасности объекта защиты

А.6.1.1 Идентификация

В первую очередь необходимо идентифицировать основные ФТБ, которые непосредственно соответствуют конкретным целям безопасности для ОО. Далее необходимо сформировать полную совокупность поддерживающих ФТБ, которые играют поддерживающую (по отношению к основным ФТБ) роль в достижении целей безопасности для ОО.

Формирование полной совокупности поддерживающих ФТБ предусматривает учет зависимостей функциональных компонентов, определенных в ИСО/МЭК 15408-2. Некоторые зависимости могут быть оставлены неудовлетворенными. При этом необходимо привести объяснение, почему соответствующие ФТБ не используются для удовлетворения целей безопасности.

А.6.1.2 Спецификация

Необходимо выбрать уровень аудита безопасности, исходя из следующих основных факторов:

- значимости аудита безопасности для достижения целей безопасности;
- технической реализуемости.

Необходимо также использовать операцию «итерация» в случае необходимости неоднократного использования функционального компонента, определенного в ИСО/МЭК 15408-2.

В ПЗ необходимо осуществить полное или частичное выполнение операций «назначение» и «выбор» над функциональными компонентами, направленное на недопущение выбора разработчиком ЗБ таких решений, которые бы противоречили целям безопасности для ОО.

Рекомендуется использовать операцию «уточнение» в случаях, если замена общего термина (например, атрибут безопасности) на специфический для рассматриваемого ОО термин делает соответствующие ФТБ более разборчивыми и понятными.

Представление

В ПЗ и ЗБ результаты выполнения операций необходимо выделять принятым в подразделе «Соглашения» способом.

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 ИСО/МЭК 15408-2.

А.6.2 Требования доверия к безопасности объекта оценки

Выбор требований доверия к безопасности необходимо осуществлять с учетом следующих основных факторов:

a) ценность активов, подлежащих защите, и риска их компрометации;

b) техническая реализуемость;

c) стоимость разработки и оценки;

d) требуемое время для разработки и оценки ОО.

А.6.3 Требования безопасности для ИТ-среды

А.6.3.1 Идентификация

Для удовлетворения целей безопасности для среды необходимо сформулировать требования безопасности для ИТ-среды.

Требования безопасности для ИТ-среды могут быть сформулированы в процессе удовлетворения зависимостей ФТБ ОО, которые не удовлетворены ОО и для которых не представлено обоснование отсутствия необходимости в их удовлетворении (для достижения целей безопасности).

А.6.3.2 Спецификация

Формулировать требования безопасности для ИТ-среды необходимо на некотором приемлемом уровне абстракции. При этом необходимо учитывать, что определение в ПЗ требований безопасности для ИТ-среды на уровне абстракции, соответствующем уровню представления ФТБ, может оказаться слишком детальным с точки зрения их реализации.

А.7 Краткая спецификация объекта оценки (только для задания по безопасности)

А.7.1 Функции безопасности объекта оценки

А.7.1.1 Идентификация

Необходимо идентифицировать функции безопасности ИТ на основе ранее сформулированных ФТБ. Функции безопасности ИТ должны быть изложены так, чтобы максимально точно соответствовать документации ОО и наглядно отображаться на соответствующие ФТБ.

А.7.1.2 Спецификация

Необходимо специфицировать функции безопасности ИТ путем использования специфических для ОО терминологии и деталей. При этом нельзя упустить ни одну из существенных деталей, содержащихся в ФТБ.

А.7.2 Меры доверия к безопасности

При идентификации мер доверия к безопасности необходимо продемонстрировать, что они охватывают все требования доверия к безопасности.

Для низких уровней доверия к безопасности (не требующих использования специальных методов и способов) раздел ЗБ «Краткая спецификация ОО» не должен содержать значительного объема дополнительной информации, кроме общих утверждений о том, что используются (или будут использоваться) необходимые для удовлетворения требований доверия к безопасности меры доверия к безопасности.

На более высоких уровнях доверия к безопасности (ОУД 5 и выше) необходима большая детализация (идентификация конкретных детализированных мер доверия к безопасности), например, ссылки на конкретные инструментальные средства, методы или подходы, которые должен использовать разработчик для удовлетворения требований доверия к безопасности.

А.8 Обоснование профиля защиты

А.8.1 Обоснование целей безопасности

Необходимо продемонстрировать (в форме таблицы или другим способом), что цели безопасности охватывают все установленные в разделе ПЗ «Среда безопасности ОО» аспекты среды безопасности ОО (угрозы, ПБОр и предположения безопасности).

Таблицу соответствия целей безопасности и аспектов среды безопасности ОО целесообразно дополнить неформальным объяснением пригодности целей безопасности для учета угроз, ПБОр и предположений безопасности.

А.8.2 Обоснование требований безопасности

Необходимо продемонстрировать (в форме таблицы или другим способом), что каждая цель безопасности для ОО учтена, по крайней мере, одним ФТБ. Представление в форме таблицы должно быть дополнено неформальным объяснением достаточности ФТБ для удовлетворения каждой цели безопасности.

Для демонстрации взаимной поддержки ФТБ следует показать:

a) что (где необходимо) зависимости компонентов требований безопасности удовлетворены;

b) что ФТБ являются согласованными (не противоречат друг другу);

c) что (где необходимо) включены поддерживающие ФТБ, предназначенные для защиты механизмов безопасности, реализующих другие ФТБ, от таких нападений как «обход», «несанкционированное изменение» и «деактивация».

А.9 Обоснование задания по безопасности

А.9.1 Обоснование целей и требований безопасности

Формирование данных подразделов «Обоснования» в ЗБ аналогично формированию соответствующих подразделов «Обоснования» в ПЗ (см. А.7).

Если ЗБ требует согласования с одним или более ПЗ, то раздел ПЗ «Обоснование» наследуется ЗБ. При этом в разделе ЗБ «Обоснование» основное внимание должно акцентироваться на дополнительных (по отношению к ПЗ) деталях, введенных в цели безопасности и требования безопасности ИТ.

А.9.2 Обоснование краткой спецификации объекта оценки

Необходимо продемонстрировать (в форме таблицы или другим способом), что функции безопасности ИТ охватывают все ФТБ, а меры доверия к безопасности – все ТДБ. При этом необходимо показать, что каждое ФТБ или ТДБ учтено, по крайней мере, одной функцией безопасности ИТ или мерой доверия к безопасности соответственно.

Приложение В
(рекомендуемое)

Основные примеры

В.1 Введение

В настоящем приложении приведены примеры угроз, ПБОр, предположений безопасности, целей безопасности в форме, рекомендуемой для ПЗ и ЗБ. Кроме того, настоящее приложение содержит рекомендации по выбору функциональных компонентов, описанных в ИСО/МЭК 15408-2, для спецификации характерных требований безопасности.

Формулировки угроз, ПБОр, предположений безопасности, целей и требований безопасности из настоящего приложения могут быть адаптированы для использования в конкретных ПЗ и ЗБ. В приведенных примерах для указания на то, что определенный термин (например, источник угрозы, активы, подлежащие защите) может быть заменен термином, специфичным для конкретного ПЗ и ЗБ, соответствующий текст выделен курсивом.

При разработке ПЗ и ЗБ допускается использование формулировок угроз, ПБОр, предположений безопасности, целей и требований безопасности, отличных от приведенных в данном приложении.

В.2 Примеры угроз

При разработке ПЗ или ЗБ важным моментом является определение угроз. Ниже приведены примеры угроз:

T.ABUSE — необнаруженная компрометация активов ИТ (преднамеренная или нет) в результате санкционированных действий уполномоченного пользователя ОО.

T.ACCESS — уполномоченный пользователь ОО может получить доступ к информации или ресурсам без разрешения их владельца или лица, ответственного за данную информацию или данные ресурсы.

T.ATTACK — необнаруженная компрометация активов ИТ в результате попытки нарушителя (сотрудника организации или постороннего лица) выполнить действия, которые ему не разрешены.

T.CAPTURE — нарушитель может перехватить данные, передаваемые по сети.

T.CONSUME — уполномоченный пользователь ОО расходует общие ресурсы, ставя под угрозу возможность для других уполномоченных пользователей получить доступ к этим ресурсам или использовать эти ресурсы.

T.COVERT — уполномоченный пользователь ОО может (преднамеренно или случайно) передавать (по скрытому каналу) чувствительную информацию пользователям, которые не имеют допуска к работе с данной информацией.

T.DENY — пользователь может участвовать в передаче информации (как отправитель или получатель), а затем впоследствии отрицать данный факт.

T.ENTRY — компрометация активов ИТ в результате использования ОО уполномоченным пользователем в ненадлежащее время дня или в ненадлежащем месте.

T.EXPORT — 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).

T.IMPERSON — нарушитель (постороннее лицо или сотрудник организации) может получить несанкционированный доступ к информации или ресурсам, выдавая себя за уполномоченного пользователя ОО.

T.INTEGRITY — целостность информации может быть поставлена под угрозу из-за ошибки пользователя, аппаратных ошибок или ошибок при передаче.

T.LINK — 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.

T.MODIFY — целостность информации может быть нарушена вследствие несанкционированной модификации или уничтожения информации нарушителем.

T.OBSERVE — нарушитель может иметь возможность наблюдать законное использование ресурса или услуги пользователем, в то время как пользователь желает сохранить в секрете факт использование этого ресурса или услуги.

T.SECRET — 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:

TE.CRASH — 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.

TE.BADMEDIA — старение и износ носителей данных или ненадлежащее хранение и обращение со сменным носителем могут привести к его порче, ведущей к потере или искажению критичных по безопасности данных.

TE.PHYSICAL — критичные по безопасности части ОО могут быть подвергнуты физической атаке, ставящей под угрозу их безопасность.

TE.PRIVILEGE — компрометация активов ИТ может происходить в результате непреднамеренных или преднамеренных действий, предпринятых администраторами или другими привилегированными пользователями.

TE.VIRUS — целостность и/или доступность активов ИТ может быть нарушена в результате непреднамеренного занесения в систему компьютерного вируса уполномоченным пользователем ОО.

В.3 Примеры политики безопасности организации

Данный пункт содержит два типичных примера ПБОр.

ПБОр на основе дискреционного принципа управления доступом (P.DAC) — право доступа к конкретным объектам данных определяется на основе:

a) идентификационной информации владельца объекта;

b) идентификационной информации субъекта, осуществляющего доступ;

c) явных и неявных прав доступа к объекту, предоставленных субъекту владельцем данного объекта.

ПБОр на основе мандатного принципа управления доступом (P.MAC) — право доступа к информации, маркированной по степени секретности (уровню конфиденциальности), определяется следующим образом:

a) данному лицу разрешен доступ к информации, только если оно имеет соответствующий допуск;

b) 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 более подробное описание ПБОр, чем в приведенных выше примерах.

В.4 Примеры предположений безопасности

Данный раздел содержит примеры предположений безопасности, относящихся к физической защите, персоналу и связности ОО и его среды.

В.4.1 Примеры предположений, связанных с физической защитой

Предположение о расположении ресурсов ОО A.LOCATE — предполагается, что ресурсы ОО расположены в пределах контролируемой зоны, позволяющей предотвратить несанкционированный физический доступ.

Предположение о физической защите ОО A.PROTECT — предполагается, что аппаратные средства и программное обеспечение ОО, критичные по отношению к реализации политики безопасности, физически защищены от несанкционированной модификации со стороны потенциальных нарушителей.

В.4.2 Примеры предположений, связанных с персоналом

A.ADMIN — 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.

A.ATTACK — предполагается, что нарушители имеют высокий уровень специальных знаний, мотивации и необходимые ресурсы.

A.USER — предполагается, что пользователи ОО обладают необходимыми привилегиями для доступа к информации, которой управляет ОО.

В.4.3 Примеры предположений, имеющих отношение к связности

A.DEVICE — предполагается, что все соединения с периферийными устройствами находятся в пределах контролируемой зоны.

A.FIREWALL — предполагается, что межсетевой экран настроен так, что он является единственной точкой сетевого соединения между частной (приватной) сетью и (потенциально) враждебной сетью.

A.PEER — 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.

В.5 Примеры целей безопасности для объекта оценки

В данном подразделе приводятся примеры целей безопасности для ОО, которые могут использоваться при формировании ПЗ или ЗБ.

O.ADMIN — 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.

O.ANON — ОО должен предусматривать средства разрешения субъекту использовать ресурс или услугу без раскрытия идентификационной информации пользователя другим сущностям (объектам или субъектам).

O.AUDIT — 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.

O.DAC — 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 P.DAC.

O.ENCRYPT — ОО должен предусматривать средства защиты конфиденциальности информации при передаче последней по сети между двумя конечными системами.

O.ENTRY — ОО должен иметь возможность ограничения входа (доступа к ОО) пользователя на основе времени и расположения устройства входа (доступа).

O.I&A — ОО должен выполнять уникальную идентификацию всех пользователей и аутентификацию (проверку подлинности) идентификационной информации до предоставления пользователю доступа к сервисам ОО.

O.INTEGRITY — ОО должен иметь средства обнаружения нарушения целостности информации.

O.LABEL — 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).

O.MAC — ОО должен защищать конфиденциальность информации, за управление которой ОО отвечает, в соответствии с политикой безопасности P.MAC, основанной на непосредственном сравнении индивидуальных разрешений (полномочий) по отношению к информации и маркировки чувствительности (конфиденциальности и др.) информации (мандатный принцип контроля доступа).

O.NOREPUD — 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.

O.PROTECT — ОО должен иметь средства собственной защиты от внешнего вмешательства или вмешательства со стороны не пользующихся доверием субъектов или попыток не пользующихся доверием субъектов обойти функции безопасности ОО.

O.PSEUD — 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 (объект, субъект) подотчетной за это использование.

O.RBAC — ОО должен предотвращать доступ пользователей к выполнению операций над ресурсами ОО, на которые они явным образом не уполномочены.

O.RESOURCE — ОО должен иметь средства управления использованием ресурсов пользователями ОО и субъектами в целях предотвращения несанкционированного отказа в обслуживании.

O.ROLLBACK — ОО должен иметь средства возврата к состоянию правильного функционирования, позволяя пользователю отменить транзакции в случае неправильной последовательности транзакций.

O.UNLINK — 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.

O.UNOBS — ОО должен иметь средства, позволяющие пользователю использовать ресурс или услугу без раскрытия другим сущностям факта использования ресурса или услуги.

В.6 Примеры целей безопасности для среды

В данном разделе приводятся примеры целей безопасности для среды, которые могут использоваться при формировании ПЗ или ЗБ:

OE.AUDITLOG — администраторы ОО должны обеспечить эффективное использование функциональных возможностей аудита. В частности:

a) должны быть предприняты соответствующие 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);

b) 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.

OE.AUTHDATA — 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.

OE.CONNECT — ответственные за ОО должны обеспечить отсутствие подключения к внешним системам или пользователям, которые могут нарушить безопасность ИТ.

OE.INSTALL — ответственные за ОО должны обеспечить безопасность ОО на этапах его поставки, установки и эксплуатации.

OE.PHYSICAL — 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.

OE.RECOVERY — ответственные за ОО должны обеспечить, чтобы процедуры и/или механизмы были представлены так, чтобы после отказа системы или другой неисправности восстановление системы достигалось без ущерба для безопасности ИТ.

В.7 Пример соответствия целей безопасности и угроз

Пример соответствия целей безопасности и угроз приведен в таблице В.1. Формулировки угроз и целей безопасности не всегда соответствуют формулировкам, приведенным в разделах В2, В5 и В6.

Таблица В.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 (путем шифрования и т.д.)
		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 (путем шифрования и т.д.)
		Обнаружение	Аудит информации журнала эксплуатации
	Использование остаточной информации на носителе	Предупреждение	Очистка памяти при удалении данных. Предотвращение раскрытия данных (путем шифрования и т.д.)
	Незаконное копирование данных	Предупреждение	Управление эксплуатацией (например, ограничение использования функции копирования или терминала приложения). Контроль прав доступа к данным. Предотвращение раскрытия данных (путем шифрования и т.д.)
		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

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Данные на носителях	Данные получены незаконно путем фальсификации файла	Предупреждение	Управление эксплуатацией (например, ограничение использования функций создания и удаления файлов или рабочего терминала). Предотвращение раскрытия данных (путем шифрования и т.д.)
		Обнаружение	Аудит информации о владельцах файлов
	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
	Зашифрованные данные не могут быть дешифрованы из-за потери секретного ключа	Предупреждение	Строгий контроль за использованием секретного ключа
		Реагирование	Восстановление секретного ключа шифрования

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Данные на носителях	Данные ошибочно удалены уполномоченным лицом	Предупреждение	Обеспечение надлежащих 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 (например, путем шифрования передаваемых 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)
	Данные незаконно используются в результате подмены их адресата, отправителя или изменения атрибутов доступа в системе коммутации	Предупреждение	Защита передаваемых данных (путем шифрования и т.д.). 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

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Данные в телекоммуникационных линиях	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)
	Выполнение приложения неуполномоченным лицом	Предупреждение	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
	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

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
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 или функцию шифрования). Использование инструкций по эксплуатации
	Отказ от авторства данных	Предупреждение	Использование удостоверяющих сервисов (например, подтверждение авторства). Использование инструкций по эксплуатации
	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 В.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
			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
	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 эксплуатационных документов
	Несанкционированное копирование или печать	Предупреждение	Обеспечение защиты во время отсутствия уполномоченного лица. Ограничение использования функций копирования и печати. Обеспечение выполнения требований эксплуатационных документов
		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 эксплуатационных документов

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Вводимые данные	Введенные данные несанкционированно изъяты (или удалены)	Предупреждение	Контроль носителя, на котором хранятся введенные данные. Обеспечение выполнения требований эксплуатационных документов
		Реагирование	Резервное копирование вводимых данных
Данные, выводимые на печать	Ознакомление или изъятие данных неуполномоченным лицом	Предупреждение	Физическая защита печатаемых данных. Обеспечение выполнения требований эксплуатационных документов
	Несанкционированное копирование	Предупреждение	Защита от копирования. Обеспечение выполнения требований эксплуатационных документов
		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
	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 (однонаправленное шифрование)

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Данные пользователей	Маскировка путем использования незаконно раскрытой информации аутентификации	Предупреждение	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 длинного секретного ключа шифрования, синтаксических правил генерации аутентификационной информации и изменение ее начального значения)
		Обнаружение	Аудит доступа к системе
		Реагирование	Блокировка работы пользователя. Минимизация нежелательного воздействия (минимизация времени действия)
	Маскировка путем использования недействительной аутентификационной информации	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

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
Данные пользователей	Отрицание факта передачи данных	Предупреждение	Предотвращение отказа от факта передачи данных. Обеспечение выполнения требований эксплуатационных документов
		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 эксплуатационных документов
		Обнаружение	Аудит обмена данными
	Данные посланы несоответствующему получателю вследствие его маскировки под авторизованного пользователя или ошибки спецификации	Предупреждение	Аутентификация адресата. Обеспечение выполнения требований эксплуатационных документов
		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)
Системные службы и данные	Нарушение безопасности системы путем раскрытия секретного ключа шифрования	Предупреждение	Создание секретных ключей шифрования достаточной стойкости и длины и использование стандартных протоколов передачи ключей
		Обнаружение	Аудит функционирования системы
		Реагирование	Назначение нового секретного ключа
	Система незаконно используется пользователем, который выдает себя за оператора во время отсутствия оператора	Предупреждение	Обеспечение надлежащей защиты во время отсутствия оператора (например, временное прекращение работы, сеанса и проведение повторной аутентификации)

Продолжение таблицы В.1

Активы	Угрозы	Цели безопасности	
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)
	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)

Окончание таблицы В.1

Активы	Угрозы	Цели безопасности	
Системные службы и данные	Нарушение безопасности системы вследствие несанкционированной замены системной программы	Обнаружение	Аудит доступа к библиотеке программ
		Реагирование	Резервное копирование программ
	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

В.8 Примеры функциональных требований безопасности

Данный раздел в качестве примера идентифицирует функции безопасности, функциональные компоненты, описанные в 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.

В.8.1 Требования идентификации и аутентификации

Функциональные компоненты для требований идентификации и аутентификации представлены в таблице В.2.

Таблица В.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

Окончание таблицы В.2

Требования безопасности		Функциональные компоненты
Управление доступом в систему (регистрацией)	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
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

В.8.2 Требования управления доступом

Функциональные компоненты для требований управления доступом представлены в таблице В.3.

Таблица В.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

Продолжение таблицы В.3

Требования безопасности		Функциональные компоненты
Дискреционное управление доступом	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
	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
Информационные метки	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
Управление на основе атрибутов ролей	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

Окончание таблицы В.3

Требования безопасности		Функциональные компоненты
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

В.8.3 Требования аудита

Функциональные компоненты для требований аудита представлены в таблице В.4.

Таблица В.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
Защита журнала аудита	Защита от потери данных, например, при переполнении журнала аудита, прерывании функционирования	FAU_STG.2–4
Защита журнала аудита	Защита от несанкционированного доступа к данным аудита	FAU_STG.1
Анализ журнала аудита	Использование инструментальных средств анализа журналов аудита	FAU_SAR.1–3

В.8.4 Требования целостности

Функциональные компоненты для требований целостности представлены в таблице В.5 (включая данные аутентификации).

Таблица В.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
Данные аутентификации	Генерация и верификация цифровых подписей (сигнатур)	FDP_DAU.2
	Генерация и верификация цифровых сертификатов (например, сертификатов открытых ключей)	FDP_DAU.2

В.8.5 Требования доступности

Функциональные компоненты для требований доступности представлены в таблице В.6.

Таблица В.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

В.8.6 Требования приватности

Функциональные компоненты для требований приватности представлены в таблице В.7.

Таблица В.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 В.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

В.8.7 Требования обмена данными

Функциональные компоненты для требований обмена данными представлены в таблице В.8.

Таблица В.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

Приложение С
(рекомендуемое)

Спецификация криптографических функциональных возможностей

С.1 Введение

Данное приложение содержит руководство по разработке ПЗ и ЗБ в части криптографических аспектов ОО, в том числе не только для тех ОО, которые являются криптографическими модулями (которые, по существу, представляют собой наборы криптографических функций). Тем не менее данное руководство изложено так, чтобы оно могло использоваться для ОО, которые являются криптографическими модулями. Данное руководство включено в настоящий документ, чтобы покрыть (охватить) широкий диапазон таких ОО, и связано с вопросами, относящимися к спецификации подобных функциональных возможностей.

Цель настоящего приложения состоит в том, чтобы предоставить руководство по спецификации криптографических функциональных возможностей и сопровождающих их требований безопасности. Данное приложение не предназначено для предоставления руководства по криптографии или по построению безопасной системы с использованием криптографических функциональных возможностей.

Руководство по применению отдельных функциональных компонентов из класса FCS (Криптографическая поддержка) приведено в приложении Е ИСО/МЭК 15408-2. Криптографические функциональные возможности могут использоваться для удовлетворения ФТБ, определенных с использованием других классов и семейств (например, класса FCO и семейств FDP_DAU, FDP_SDI, FDP_UCT, FDP_UIT, FIA_SOS, и FIA_UAU). В этих случаях отдельные функциональные компоненты определяют требования безопасности, которые можно удовлетворить с использованием криптографических функциональных возможностей. Класс FCS следует использовать, если криптографические функциональные возможности ОО востребованы потребителями.

Хотя в настоящем стандарте и рассматриваются соответствующие требования доверия, в область применения стандарта не входит рассмотрение стойкости криптографии, а также фактических уровней доверия. Требования доверия для ОО следует определять с учетом чувствительности предметной области, ожидаемых угроз и уязвимостей, которым можно эффективно противостоять посредством требований доверия. Эти вопросы рассмотрены в разделе 10 настоящего стандарта.

Дополнительная информация и руководства по криптографии и криптографическим алгоритмам содержатся в [4] — [9].

С.2 Термины и определения

Терминология, используемая в настоящем приложении, базируется на терминах и определениях, приведенных в подразделе 2.3 ИСО/МЭК 15408-1 и в ИСО 2382-8. В целях обеспечения понимания представленных в настоящем стандарте понятий ниже определен ряд дополнительных терминов.

С.2.1 Режим доступа

Тип операции, определенный некоторым правом на доступ. Примеры: чтение, запись, выполнение, модификация, удаление, создание и т.д. Также см. «Тип доступа» в соответствии с ИСО 2382-8.

С.2.2 Закрытые данные

Данные, информационное содержание которых не доступно напрямую, так как защищено шифрованием. Примерами таких данных являются сообщения, файлы, криптографические ключи и т.д.

С.2.3 Криптографический алгоритм

Набор математических правил для преобразования исходных данных в выходные данные на основе других входных параметров, таких как криптографические ключи и векторы инициализации.

С.2.4 Криптографическая контрольная сумма

Относительно короткая последовательность, полученная из исходных данных посредством использования криптографического алгоритма, которая представляет собой функцию от данных, секретного ключа и, возможно, вектора инициализации и главным образом прикрепляется к данным для контроля целостности данных. Также см. «Код установления подлинности сообщения» по ИСО 2382-8.

С.2.5 Генерация криптографической контрольной суммы

Процесс генерации криптографической контрольной суммы в целях ее прикрепления к данным.

С.2.6 Проверка криптографической контрольной суммы

Процесс генерации криптографической контрольной суммы в целях проверки прикрепленной криптографической контрольной суммы.

С.2.7 Криптографическая функция

Одно из вычислений, выполняемое с использованием криптографического алгоритма, например, шифрование, расшифрование, генерация цифровой подписи, проверка цифровой подписи и т.д.

С.2.8 Криптографические функциональные возможности

Одна или более криптографических функций, реализованных в ОО.

С.2.9 Криптографический ключ

Цифровая последовательность, управляющая выполнением криптографического алгоритма и влияющая на его результат. Также см. «Ключ» по ИСО 2382-8.

С.2.10 Доступ к криптографическому ключу

Операция, выполняемая по отношению к криптографическому ключу. Примеры операции/доступа: чтение, запись, архивирование, резервное копирование, восстановление.

С.2.11 Согласование криптографических ключей

Криптографическая функция, которая позволяет двум сторонам вычислить общий секретный ключ.

С.2.12 Архивирование криптографического ключа

Операция, направленная на хранение криптографических ключей на постоянном или долговременном носителе информации.

С.2.13 Резервное копирование криптографического ключа

Операция, направленная на то, чтобы сделать резервную копию криптографического ключа с целью его использования в случае, если подлинник криптографического ключа удален, модифицирован, уничтожен или стал недоступен.

С.2.14 Уничтожение криптографического ключа

Процесс удаления (обнуления) криптографического ключа.

С.2.15 Распределение криптографических ключей

Процесс предоставления криптографических ключей пользователям, процессам, элементам ОО и др.

С.2.16 Депонирование (передача на хранение) криптографического ключа

Процесс предоставления криптографического ключа третьей доверенной стороне, которая обязана передать этот ключ уполномоченным сторонам.

С.2.17 Генерация криптографического ключа

Функция создания криптографического ключа.

С.2.18 Управление криптографическими ключами

Процесс управления жизненным циклом криптографических ключей, начиная от генерации, распределения и заканчивая архивированием и уничтожением.

С.2.19 Восстановление криптографического ключа

Процесс восстановления криптографического ключа из какого-либо источника, включая архив, резервную копию или депонент.

С.2.20 Криптографический механизм

Процесс или средство, реализующее одну или более криптографических функций.

С.2.21 Криптографическая операция

См. Криптографическая функция.

С.2.22 Криптографическая переменная

Цифровая последовательность или набор цифровых последовательностей, требуемых для выполнения криптографического алгоритма, чтобы преобразовать входные данные алгоритма в выходные. Примерами криптографических переменных являются криптографические ключи (секретные, публичные, частные и т.д.), параметры публичных ключей и векторы инициализации.

Примечание — Открытый, зашифрованный тексты и хэш-последовательности не рассматриваются в качестве криптографических переменных.

С.2.23 Маршрут данных

Логический или физический маршрут, по которому (или через который) проходят данные.

С.2.24 Цифровая подпись

См. «Цифровая подпись» в ИСО 2382-8.

С.2.25 Генерация цифровой подписи

Процесс генерации цифровой подписи.

С.2.26 Верификация (проверка) цифровой подписи

Процесс проверки цифровой подписи.

С.2.27 Хэширование или значение хэша

См. Безопасная хэш-последовательность.

С.2.28 Вектор инициализации

Вектор (последовательность битов), используемый совместно с криптографическим ключом для определения стартовой точки шифрования в рамках криптографического алгоритма.

С.2.29 Параметр обращения

«Секрет» (например, пароль или личный идентификатор), который предоставляется ОО для получения доступа к криптографической функции.

С.2.30 Дайджест сообщения

См. Безопасная хэш-последовательность.

С.2.31 Неотказуемость

Невозможность для некоторой сущности отрицать участие во взаимодействии.

С.2.32 Другой критичный параметр безопасности

См. Параметр обращения.

С.2.33 Частный ключ

Один из ключей публичной ключевой пары. Его конфиденциальность должна быть обеспечена, чтобы он мог использоваться для расшифровывания, генерации цифровой подписи или соглашения о криптографическом ключе.

С.2.34 Публичный ключ

Один из ключей публичной ключевой пары, который может быть сделан публичным. Некоторые общественные ключи используются для шифрования, некоторые — для цифровой проверки подписи, и некоторые — для криптографического ключевого соглашения.

С.2.35 Публичная ключевая пара

Пара математически связанных ключей, для которых получение частного ключа из связанного с ним публичного ключа должно быть в вычислительном плане неосуществимым.

С.2.36 Открытые данные

Данные, информационное содержание которых доступно напрямую, потому что не защищено шифрованием.

Например, сообщения, файлы, криптографические ключи и т.д.

С.2.37 Разделение отрытых/закрытых данных

Логическое и физическое разделение открытых и закрытых данных. Например, открытые данные и закрытые данные никогда не должны передаваться по общим физическим линиям связи и никогда не должны помещаться в одну и ту же область памяти.

С.2.38 Секретный ключ

Ключ, используемый в криптографическом алгоритме, как для зашифровывания, так и для расшифровывания.

С.2.39 Безопасная хэш-последовательность

Цифровая последовательность, являющаяся результатом применения некоторого алгоритма по отношению к сообщению, характеризуется тем, что в вычислительном плане невозможно получить сообщение из результата (хэш-последовательности), получить другое сообщение, которое дало бы ту же самую хэш-последовательность, что и первое сообщение, а также — найти два сообщения, дающие одну и ту же хэш-последовательность. Обычно безопасная хэш-последовательность значительно короче, чем сообщение или файл, из которого она получена. Также известна как значение хэша, дайджест сообщения.

С.2.40 Зона обнаружения вмешательств

Область, окружающая ОО, в которой вмешательство (нарушение или попытка вторжения) может быть обнаружено.

С.2.41 Обнуление

Метод электронного стирания хранимых данных путем изменения данных таким образом, чтобы первоначально хранимые данные не могли быть восстановлены.

С.2.42 Операции по обнулению

Последовательность электронных операций, направленных на обнуление.

С.2.43 Схема обнуления

См. «Операции по обнулению».

С.3 Краткий обзор криптографии

С.3.1 Понятие криптографии

Криптография — это наука или искусство, которая(ое) включает в себя принципы, средства и методы преобразования данных, чтобы скрыть их информационное содержание, предотвратить его необнаруженную модификацию и/или неправомочное использование. Научная составляющая криптографии основана на принципах математики, в то время как искусство является результатом многолетнего практического опыта. Криптография включает в себя (но не ограничивается):

a) генерацию и/или верификацию цифровой подписи;

b) генерацию криптографической контрольной суммы для контроля целостности и/или для проверки контрольной суммы;

c) вычисление безопасной хэш-последовательности (дайджест сообщения или файла);

d) шифрование и/или расшифровывание данных;

e) шифрование и/или расшифровывание криптографического ключа;

f) согласование криптографических ключей.

Криптографические функциональные возможности могут использоваться для удовлетворения нескольких высокоуровневых целей безопасности. Криптографические функциональные возможности включают в себя (но не ограничиваются):

a) конфиденциальность;

b) целостность;

c) идентификацию и аутентификацию;

d) неотказуемость;

e) доверенный маршрут;

f) доверенный канал;

g) разделение данных.

Для реализации криптографических функциональных возможностей должны использоваться соответствующие криптографические алгоритмы и размеры криптографических ключей, а также — безопасные криптографические протоколы и правильное проектирование криптографии.

С.3.2 Использование криптографии

Разработчики ПЗ и ЗБ должны обратить внимание на то, что криптографическая функциональная возможность может быть только одной из нескольких видов функциональных возможностей, которые могли бы использоваться для удовлетворения целей безопасности. Поэтому выбор криптографических функциональных возможностей, соответствующих целям безопасности, следует рассматривать в контексте определения полного хорошо сбалансированного набора процедурных, физических и ИТ-мер безопасности.

Для выбора криптографии из всех других видов функциональных возможностей безопасности могут существовать следующие причины:

a) только криптографические функции могут соответствовать требуемым целям безопасности. Например, передача информации по незащищенному проводному или беспроводному каналу (то есть через общедоступный домен). Таким образом, криптография является единственной функциональной возможностью, которая обеспечивает конфиденциальность или целостность передаваемых данных;

b) криптографические функции могут обеспечить соответствующий уровень безопасности для противостояния прогнозируемым угрозам, например, аутентификацию через небезопасную сеть. Криптография может использоваться для защиты от перехвата или повторного использования аутентификационной информации. Средства аутентификации иногда обеспечивается механизмом «запрос—ответ»;

c) криптографические функции могут быть самыми простыми/самыми легкими/самыми дешевыми для реализации, эксплуатации и/или использования;

d) криптографические функции могут использоваться как часть множества различных средств для защиты информации (что также известно, как концепция «усиление безопасности в глубину»). Например, если данные защищают от несанкционированного с использованием «традиционных» компьютерных средств управления доступом и/или физических средств безопасности, то для обеспечения дополнительного уровня защиты на случай сбоя этих механизмов, данные также зашифровывают. Таким образом, если злоумышленник способен преодолеть средства управления доступом, то он для получения данных также должен будет преодолеть криптографические механизмы защиты.

С.3.3 Использование криптографических стандартов

В более широком понимании, может потребоваться соответствие криптографических функций конкретному стандарту (международному, национальному, отраслевому или стандарту организации) по одной или нескольким из следующих причин:

a) стандарт может способствовать установлению общепризнанного приемлемого уровня безопасности;

b) стандарт может способствовать широкому взаимодействию;

c) стандарт может способствовать взаимному признанию;

d) стандарт может требоваться политикой безопасности конкретной организации;

e) стандарт может способствовать реализации необходимых функциональных возможностей.

С.4 Формирование требований безопасности

С.4.1 Покрытие

В разделе С.4 определяются связанные с криптографией аспекты, которые необходимо рассматривать при спецификации угроз, политик безопасности организаций и целей безопасности для ОО, содержащих криптографические функциональные возможности, а также при рассмотрении криптографических потребностей при формировании требований безопасности и предположений, которые должны быть определены в ПЗ или ЗБ. Настоящий раздел стандарта отражает только вопросы, необходимые при формировании требования безопасности для ОО, содержащих криптографические функциональные возможности, и может не охватывать сопутствующие некриптографические вопросы.

С.4.2 Угрозы

С.4.2.1 Спецификация угроз

Известные типовые или предполагаемые угрозы ИТ-активам в ОО, содержащем криптографические функциональные возможности, должны быть определены в ПЗ или ЗБ. Этим угрозам ОО может противостоять или может не противостоять.

Как указано в разделе 8 настоящего стандарта, четкая спецификация угрозы должна быть детализирована в терминах источника угрозы (или агента угрозы), ИТ-активов, подверженных атаке, а также — вида атаки (реализации угрозы). К тому же должны быть определены только те события, которые непосредственно ставят под угрозу (компрометируют) ИТ-активы, а не атаки, основанные на недостатках или слабостях в реализации ОО.

Это означает, что один из подходов к спецификации угроз состоит в том, чтобы излагать угрозы в виде кортежей из трех элементов, включающих в себя источник угрозы/агент угрозы, ИТ-активы, подверженные атакам со стороны источника угрозы, и вид атаки (реализации угрозы). Затем угрозы могут использоваться для определения целей безопасности, которые в свою очередь могут быть уточнены в требованиях безопасности ИТ.

С.4.2.2 Типовые источники угроз

Типовые источники угроз (или агенты угроз) для ОО, содержащих криптографические функциональные возможности, включают в себя (но не ограничиваются):

a) уполномоченных пользователей ОО;

b) неуполномоченных лиц.

Примечание — В данном контексте уполномоченным пользователем является тот, кто уполномочен (авторизован) иметь доступ к определенным активам ИТ.

С.4.2.3 Типовые ИТ-активы, связанные с криптографией

Типовые виды ИТ-активов в ОО, связанные с криптографией, требующие защиты, включают в себя (но не ограничиваются):

a) криптографические переменные (включая секретные ключи, частные ключи, публичные ключи, параметры публичных ключей, векторы инициализации и т.д.);

b) исходные данные и выходные данные криптографической функции (например, открытый и зашифрованный тексты);

c) реализация криптографического алгоритма в аппаратных средствах, программном обеспечении и/или программно-аппаратных средствах;

d) параметры вызовов (также известные как «другие критические параметры безопасности»).

С.4.2.4 Типовые виды атак (реализации угроз)

ИТ-активы, связанные с криптографией, обычно нуждаются в защите от нескольких видов атак. Они включают в себя (но не ограничиваются):

a) обнаружение электромагнитного излучения, исходящего от ОО;

b) маскировку под уполномоченных пользователей ОО;

c) внесение ошибок в ОО;

d) неправильное использование (то есть эксплуатацию или администрирование) ОО;

e) сбои (отказы) аппаратных, программно-аппаратных или программных средств, составляющих ОО;

f) физическое воздействие.

Примечание — Данные атаки не обязательно ограничиваются криптографическими активами.

С.4.2.5 Типовые угрозы

Используя типовые исходные данные для трехэлементных кортежей, идентифицированные в предыдущих подпунктах, существует не более 48 специфических угроз (то есть два источника угрозы на шесть видов атак на четыре ИТ-актива, связанных с криптографией). Примеры сформированных таким образом угроз приведены в таблице С.1.

Таблица С.1 — Типовые угрозы, относящиеся к криптографическим активам

Идентификатор угрозы	Типовая угроза
T.EMI	Связанные с криптографией активы ИТ могут быть раскрыты неуполномоченному лицу или пользователю через электромагнитные излучения ОО
N.IMPERSON	Нарушитель (внешний или внутренний) может выдавать себя за уполномоченного пользователя ОО
T.ERROR	Неуполномоченное лицо или пользователь ОО, инициируя ошибки в ОО, может добиться несанкционированного раскрытия или модификации связанных с криптографией активов ИТ
T.MODIFY	Целостность информации может быть поставлена под угрозу (скомпрометирована) из-за несанкционированной модификации или уничтожения информации нарушителем
T.ATTACK	Необнаруженная компрометация связанных с криптографией активов ИТ может произойти в результате попыток нарушителя (внутреннего или внешнего) выполнения действий, на выполнение которых нарушитель не уполномочен
T.ABUSE	Необнаруженная компрометация связанных с криптографией активов ИТ может произойти в результате преднамеренного или непреднамеренного выполнения любым уполномоченным пользователем ОО действий, на выполнение которых уполномочено конкретное лицо

Окончание таблицы С.1

Идентификатор угрозы	Типовая угроза
T.MAL	Связанные с криптографией активы ИТ могут быть модифицированы или раскрыты неуполномоченному лицу или пользователю ОО в результате сбоя (отказа) ОО
T.PHISICAL	Критичные с точки зрения безопасности части ОО могут быть подвержены физическим атакам, которые могут поставить под угрозу (скомпрометировать) безопасность

С.4.3 Политика безопасности организации

Правила ПБОр (если заданы), которыми должен руководствоваться ОО, также должны быть изложены в ПЗ или ЗБ. Следует документировать изложение ПБОр относительно криптографических функциональных возможностей ОО, которое не может быть включено или подразумеваться в описании угроз. Изложение ПБОр включает в себя (но не ограничивается) изложение:

a) политики идентификации и аутентификации;

b) политики управления доступом пользователей;

c) политики аудита и учета;

d) политики управления криптографическими ключами;

e) политики физической безопасности;

f) политики управления излучениями.

Разработчики ПЗ и ЗБ также могут применить изложение этих ПБОр к аспектам ОО, не связанным с криптографией.

Дополнительная информация различных составляющих политики безопасности для ОО, содержащего криптографические функциональные возможности, а также способ их представления в соответствии со стандартами серии ИСО/МЭК 15408 представлены в С.5.5.

С.4.4 Цели безопасности и обоснование

Типовые цели безопасности приведены в таблице С.2.

Таблица С.2 — Типовые цели безопасности для ОО

Идентификатор цели	Цель безопасности
O.I&A	ОО должен выполнять уникальную идентификацию всех пользователей и аутентификацию (проверку подлинности) идентификационной информации до предоставления пользователю доступа к сервисам ОО
O.DAC OO	ОО должен предоставлять своим 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 дискреционной политикой безопасности
O.PHP	ОО должен защищать себя и связанные с криптографией активы ИТ от несанкционированного физического доступа, модификации или использования
O.INTEGRITY	ОО должен иметь средства обнаружения нарушения целостности информации
O.FAILSAFE	В случае возникновения ошибки ОО должен сохранять безопасное состояние
O.ADMIN	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
OE.EMI	Должны быть предприняты процедурные и физические меры для предотвращения раскрытия связанных с криптографией активов ИТ неуполномоченным лицам или пользователям через электромагнитные излучения ОО

Окончание таблицы С.2

Идентификатор цели	Цель безопасности
OE.PHYSICAL	Ответственные за ОО должны обеспечить, чтобы части ОО, являющиеся критичными по отношению к реализации политики безопасности, были защищены от физического нападения, которое могло бы поставить под угрозу безопасность ИТ
Примечание — Цели безопасности OE.EMI и OE.PHYSICAL являются целями безопасности для среды. Остальные цели являются целями безопасности для ОО. Другие цели безопасности для среды могут быть связаны: a) с процедурами обработки и хранения связанных с криптографией активов ИТ, вводимых в и выводимых из ОО; b) с процедурами эксплуатации и поддержки ОО; c) с уровнем доверия к уполномоченным пользователям ОО; d) с обучением уполномоченных пользователей (например, держателей криптографических ключей, обслуживающего персонала, основных пользователей), которые должны каким-либо образом взаимодействовать с ОО; e) с физическими мерами, необходимыми для защиты ОО; f) с ограничениями, связанными со средой эксплуатации ОО (включая ограничения, связанные с электромагнитными излучениями); g) с ИТ-средой безопасности ОО (например, ограничениями по типу программного обеспечения, по использованию базовой доверенной операционной системы для реализации политики управления доступом к ОО).	

Обоснование целей безопасности для противостояния угрозам приведена в таблице С.3. Данная таблица не отражает уровень детализации, необходимый для обоснования целей безопасности в ЗБ или ПЗ.

Таблица С.3 — Обоснование целей безопасности

Идентификатор угрозы	Соответствующая цель безопасности и обоснование
T.EMI	OE.EMI — требование использования процедурных и физических мер (например, экранирование помещения, размещение на определенном расстоянии от общедоступной зоны) должно уменьшить риск раскрытия связанных с криптографией активов ИТ через излучения ОО
T.IMPERSON	O.I&A — требование надежной идентификации и аутентификации пользователя должно уменьшить риск маскировки под уполномоченного пользователя
T.ERROR	O.FAILSAFE — требование ОО сохранять безопасное состояние в случае возникновения ошибки должно уменьшить риск негативного воздействия из-за случайной модификации или раскрытия связанных с криптографией активов ИТ
T.ABUSE	O.DAC — требование о соответствии процедуры предоставления доступа к ОО установленной политике управления доступом должно уменьшить риск того, что пользователи будут, выполнять операции, доступ к которым им не требуется
T.MAL	O.INTEGRITY — требование к ОО по обнаружению нарушения целостности увеличивает возможности по обнаружению ошибок. O.FAILSAFE — требование ОО сохранять безопасное состояние в случае возникновения ошибки должно уменьшить риск негативного воздействия из-за случайной модификации или раскрытия связанных с криптографией активов ИТ
T.PHYSICAL	O.PHP — требование по защите от физических атак должно уменьшить риск физических атак. OE.PHYSICAL — требование по использованию процедурных и физических мер для ограничения физического доступа к ОО только пользователями, уполномоченными на физический доступ и которым это требуется, должно уменьшить риск физической атаки на ОО

Окончание таблицы С.3

Идентификатор угрозы	Соответствующая цель безопасности и обоснование
T.MODIFY	O.INTEGRITY — возможность обнаружения нарушения целостности должна уменьшить возможности нарушителя по модификации связанных с криптографией активов ИТ. O.ADMIN — надлежащая конфигурирование и администрирование ОО должны уменьшить риск модификации
T.ATTACK	O.I&A – требование надежной идентификации и аутентификации пользователя должно уменьшить риск несанкционированного доступа. O.DAC — требование о соответствии процедуры предоставления доступа к ОО установленной политике управления доступом должно уменьшить риск того, что пользователи будут выполнять операции, доступ к которым им не требуется

С.4.5 Требования безопасности

Цели безопасности могут быть уточнены в требованиях безопасности ИТ в соответствии с таблицей С.4.

Таблица С.4 — Формирование требований безопасности на основе целей безопасности

Идентификатор цели	Цель безопасности	Компонент в соответствии со стандартами серии ИСО/МЭК 15408
O.I&A	ОО должен выполнять уникальную идентификацию всех пользователей и аутентификацию (проверку подлинности) идентификационной информации до предоставления пользователю доступа к ОО и связанным с криптографией активам ИТ	FIA_UID.1-2, FIA_UAU.1-5
O.DAC	ОО должен предоставить своим пользователям средства управления и ограничения доступа к связанным с криптографией активам ИТ в соответствии с установленной политикой управления доступом	FDP_ACC.1-2, FDP_ACF.1
O.PHP	ОО должен защищать себя и связанные с криптографией активы ИТ от несанкционированного физического доступа, модификации или использования	FPT_PHP.1-3
O.INTEGRITY	ОО должен иметь средства обнаружения нарушения целостности информации	FPT_AMT.1, FPT_TST.1.
O.FAILSAFE	В случае возникновения ошибки ОО должен сохранять безопасное состояние	FPT_FLS.1-4
O.ADMIN	ОО должен предоставить функциональные возможности, которые позволят уполномоченному администратору управлять криптографическими ключами в соответствии с установленной политикой управления криптографическими ключами	FCS_CKM.1-4, FCS_COP.1
OE.EMI	Должны быть предприняты процедурные и физические меры для предотвращения раскрытия связанных с криптографией активов ИТ неуполномоченным лицам или пользователям через электромагнитные излучения ОО	AGD_ADM.1, AGD_USR.1, процедуры безопасной эксплуатации

Окончание таблицы С.4

Идентификатор цели	Цель безопасности	Компонент в соответствии со стандартами серии ИСО/МЭК 15408
OE.PHYSICAL	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	Процедуры безопасной эксплуатации

С.5 Изложение требований безопасности ИТ

С.5.1 Введение

В данном разделе объясняется, каким образом на основе стандартов серии ИСО/МЭК 15408 в ПЗ или ЗБ могут быть выражены требования безопасности ИТ, которые предъявляются к ОО, содержащему криптографические функциональные возможности.

Детальное рассмотрение содержания частей ПЗ и ЗБ, связанных со средой безопасности ОО (угрозы, ПБОр и предположения безопасности) и целями безопасности.

Разработчикам необходимо помнить, что данный стандарт применяется только к разработке ПЗ и ЗБ для тех ОО, которые включают в себя криптографические функциональные возможности. В настоящем стандарте рассматриваются только те компоненты и семейства, которые могли бы быть использованы при формировании требований к таким ОО, и в которых могут не учитываться функциональные возможности, связанные с некриптографическими вопросами. В настоящем стандарте не учитывается потребность в расширенных требованиях или требованиях каких-либо предопределенных функциональных пакетов или пакетов доверия (таких как заявленный оценочный уровень доверия). Также не принимаются во внимание взаимозависимости всех дополнительных компонентов.

С.5.2 Традиционные вопросы проектирования и реализации криптографии

Разработчики криптографического оборудования заинтересованы некоторыми уязвимостями, установленными на основе опыта эксплуатации и разработки и связанными преимущественно с аппаратными криптографическими средствами. Традиционные уязвимости и связанные с ними традиционные решения представлены в таблице С.5.

Таблица С.5 — Традиционные уязвимости и связанные с ними традиционные решения

Уязвимость	Традиционное решение в терминах ИСО/МЭК 15408
Смешивание (неразделение) данных и ключей	Отдельные физические точки доступа
Использование служебных точек доступа	Установление служебных ролей
Смешивание (неразделение) открытого и зашифрованного текста	Отдельные каналы ввода и вывода. Разделение открытых/закрытых данных
Утечка чувствительной информации вследствие криптографического сбоя	Два внутренних, независимых действия для передачи чувствительной информации. Отключение каналов вывода данных от системы генерации ключей, ввода ключей и обнуления ключей
Несанкционированный доступ	Идентификация и аутентификация. Управление доступом к функциям, сервисам и данным
Ошибки в проекте	Проектирование конечных автоматов
Физическая атака	Меры физической безопасности
Сбои аппаратных средств	Самотестирование
Электромагнитные излучения	Стандарты управления электромагнитными излучениями

Представление традиционных решений, связанных с традиционными уязвимостями, в терминах стандартов серии ИСО/МЭК 15408 рассматривается в таблице С.6.

Таблица С.6 — Представление традиционных решений в терминах стандартов серии ИСО/МЭК 15408

Уязвимость	Представление решения в терминах ИСО/МЭК 15408
Смешивание (неразделение) данных и ключей	Модульность (ADV_INT)
Использование служебных точек доступа	Поддержка ПФБ управления доступом (FDP_ACC, FDP_ACF)
Смешивание (неразделение) открытого и зашифрованного текста	Модульность и сокрытие информации (ADV_INT)
Утечка чувствительной информации вследствие криптографического сбоя	Безопасность при отказе (FPT_FLS). Модульность и сокрытие информации (ADV_INT)
Несанкционированный доступ	Идентификация и аутентификация (FIA_UID, FIA_UAU, FIA_ATD). ПФБ управления доступом пользователей (FDP_ACC, FDP_ACF)
Ошибки в проекте	Полуформальный и формальный проект (ADV_HLD, ADV_LLD)
Физическая атака	Физическая безопасность (FPT_PHP)
Сбои аппаратных средств	Безопасность при отказе (FPT_FLS). Самотестирование (FPT_AMT, FPT_TST)
Электромагнитные излучения	Предположения, связанные с политикой управления излучениями

Для упрощения пояснений по представлению решений на основе стандартов серии ИСО/МЭК 15408, а также типовых представлений в соответствии с таблицей С.4, выражение типовых требований безопасности ОО, содержащих криптографические функциональные возможности, рассматривается под следующими шестью заголовками:

1) «Определение ОО»;
2) «Проект и реализация ОО»;
3) «Политика безопасности ОО»;
4) «Функциональные возможности безопасности ОО»;
5) «Тестирование ОО»;
6) «Эксплуатация ОО».

С.5.3 Определение объекта оценки

С.5.3.1 Руководство

Объект оценки, его компоненты, функции и интерфейсы должны быть полностью определены в ПЗ и ЗБ, то есть должна быть функциональная спецификация ОО, что должно гарантировать, что все функциональные требования, определенные в ПЗ и ЗБ, учтены и ПБО реализована в ФБО. Должна быть определена также политика безопасности ОО, согласованная с функциональной спецификацией (см. также 5.5).

Примечание — Определение ОО отличается от проекта ОО тем, что оно связано с определением функциональных возможностей ОО и физических/логических границ ОО. Проект ОО связан с уточнением функциональной спецификации, которое может быть осуществлено.

С.5.3.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Компонент(ы) из семейства ADV_FSP (функциональная спецификация) следует использовать для выражения требований для высокоуровневого описания видимых пользователю интерфейсов и режима выполнения ФБО.

При наличии требования к полуформальному проекту (например, проект конечного автомата) следует использовать компонент ADV_FSP.3 (полуформальная функциональная спецификация). Если есть требование по

модели политики безопасности, то должно использоваться семейство ADV_SPM (моделирование политики безопасности).

С.5.4 Проект и реализация объекта оценки

С.5.4.1 Общее доверие

С.5.4.1.1 Руководство

Необходимо уделить внимание тому, чтобы минимизировать и (где возможно) устранить ошибки проектирования и реализации. В ПЗ и ЗБ должно быть продемонстрировано, что, по крайней мере, высокоуровневая архитектура ОО является надлежащей для реализации установленных функциональных требований.

Если требуется большая уверенность в проекте и его реализации, то может потребоваться демонстрация того, что более низкие уровни проекта (потенциально до самого нижнего уровня) также отражают требуемые функциональные возможности и были корректно уточнены по отношению к более высоким уровням проекта.

С.5.4.1.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для обеспечения необходимой уверенности в правильности проекта и реализации ОО следует выбрать соответствующие компоненты следующих семейств:

a) ADV_HLD (проект верхнего уровня);

b) ADV_LLD (проект нижнего уровня);

c) ADV_RCR (соответствие представлений);

d) ALC_TAT (инструментальные средства и методы).

Компоненты из семейства ADV_HLD должны использоваться для выражения требований к описанию ФБО в терминах основных структурных частей (то есть подсистем) и связи этих частей с функциями, которые они выполняют. Компонент ADV_HLD.2 (детализация вопросов безопасности в проекте верхнего уровня) следует использовать, если есть требование по отделению криптографических границ ОО от границ ОО в целом.

Компоненты из семейства ADV_LLD следует использовать для выражения требований к описанию внутреннего содержания ФБО в терминах модулей, их взаимосвязей и зависимостей.

Компоненты из семейства ADV_RCR следует использовать при наличии требований к демонстрации соответствия между различными представлениями проекта.

Компонент ALC_TAT.2 следует использовать при наличии требования к выполнению разработки в соответствии с конкретным стандартом реализации (например, стандарт кодирования).

С.5.4.2 Модульный проект

С.5.4.2.1 Руководство

Как уже отмечалось, разработчики криптографии обычно озабочены тем, что ошибка в одной части ОО может повлиять на другие части ОО, и информация из одной части ОО может стать доступной для других частей ОО, которым она не требуется. Эта озабоченность привела к следующим типам традиционных требований:

a) все входные данные, поступающие в ОО через интерфейс ввода данных, должны пройти только через маршрут ввода данных;

b) все выходные данные, выходящие из ОО через интерфейс вывода данных, должны пройти только через маршрут вывода данных;

c) маршрут вывода данных должен быть логически отделен от системы и процессов генерации ключей, ручного ввода ключей или обнуления ключей;

d) ОО должен поддерживать отдельные маршруты для открытых и закрытых данных.

Предназначение этих требований заключается в том, чтобы обеспечить техническое руководство, связанное с модульным проектированием, уменьшением сложности и минимизации негативных последствий ошибок в какой-либо части системы.

С.5.4.2.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для выражения требований к модульному проекту ОО в ПЗ и ЗБ следует выбрать компонент(ы) из следующих семейств:

a) ADV_FSP (функциональная спецификация);

b) ADV_HLD (проект верхнего уровня);

c) ADV_INT (внутренняя структура ФБО);

d) ADV_LLD (проект нижнего уровня).

Например, проект нижнего уровня показывает все потоки данных и может быть использован для обеспечения уверенности в том, что входные, выходные данные, открытый и зашифрованный тексты доступны только компонентам ОО, которым они необходимы. Требования модульности и иерархичности помогают обеспечить уверенность в том, что ОО разрабатывается с использованием надлежащих принципов проектирования, и, следовательно, доступ к данным могут получить только те компоненты ОО, которым они необходимы.

В этом направлении существуют следующие элементы компонента ADV_INT.3 (минимизация сложности) из семейства ADV_INT (внутренняя структура ФБО):

a) ADV_INT.3.3C — описание архитектуры должно содержать изложение, каким образом проект ФБО обеспечивает большую независимость модулей, чтобы избежать ненужного взаимодействия;

b) ADV_INT.3.5C — описание архитектуры должно показать, что взаимные связи были минимизированы, и содержать строгое обоснование оставшихся связей;

c) ADV_INT.3.6C — описание архитектуры должно показывать, каким образом все ФБО структурированы для минимизации сложности.

С.5.5 Политика безопасности объекта оценки

С.5.5.1 Введение

В ПЗ и ЗБ должна быть описана политика безопасности ОО. Политика безопасности ОО, содержащего криптографические функциональные возможности, должна включать в себя следующие аспекты (но может ими не ограничиваться):

a) политика идентификации и аутентификации;

b) политика управления доступом пользователей;

c) политика аудита и учета;

d) политика управления криптографическими ключами;

e) политика физической безопасности;

f) политика управления электромагнитными излучениями.

Выражение этих политик безопасности обычно достигается сочетанием формулировок политики безопасности организации (например, ссылка на стандарты электромагнитных излучений, спецификацию политики управления доступом пользователей), предположений (например, ссылка на физические и процедурные меры защиты ОО) и функциональных ИТ-требований безопасности к ОО (например, определение функциональных механизмов, которые реализуют политику управления доступом пользователей).

С.5.5.2 Политика идентификации и аутентификации

С.5.5.2.1 Руководство

В ПЗ и ЗБ следует определить типы пользователей и/или ролей, а также способов/средств их аутентификации.

Типовые роли, связанные с криптографией, включают в себя:

a) ответственного за криптографию;

b) ответственного за сопровождение системы;

c) аудитора системы;

d) ответственного за безопасность системы;

e) пользователя/оператора.

С.5.5.2.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для выражения требований к установлению и верификации предъявленного пользователем идентификатора следует выбирать соответствующие компоненты из класса FIA. Как правило, следует выбирать компонент(ы) из следующих семейств:

a) FIA_UID (идентификация пользователя);

b) FIA_UAU (аутентификация пользователя);

c) FIA_ATD (определение атрибутов пользователя).

Компонент(ы) из семейства FIA_UID следует использовать для определения условия, при которых от пользователей должна требоваться собственная идентификация до выполнения при посредничестве ФБО каких-либо других действий, требующих идентификации пользователя.

Компонент(ы) из семейства FIA_UAU должен(ы) быть использован(ы) для определения механизмов аутентификации пользователя, предоставляемые ФБО.

Компонент(ы) из семейства FIA_ATD следует использовать для определения атрибутов безопасности пользователей. Компонент(ы) из семейства FIA_ATD следует использовать для определения информации о криптографическом ключе как атрибуте пользователя.

Защита аутентификационной информации от перехвата и повторного использования может быть достигнута с использования компонентов из семейства FTP_TRP (доверенный маршрут) и/или FIA_UAU (FIA_UAU.3 — аутентификация, защищенная от подделок и FIA_UAU.4 — механизмы одноразовой аутентификации).

С.5.5.3 Политика управления доступом пользователей

С.5.5.3.1 Руководство

ОО должен реализовывать управление доступом пользователей к криптографическим активам ИТ в соответствии с установленной политикой управления доступом пользователей. В контексте ОО, содержащего криптографические функциональные возможности, элементами политики управления доступом пользователей являются:

a) роли пользователей;

b) сервисы, к которые может осуществляться доступ;

c) критичные параметры безопасности, например, криптографические ключи (как незашифрованные, так и зашифрованные), другие критичные параметры безопасности (такие, например, как аутентификационные данные);

d) виды доступа (например, чтение, запись, выполнение, удаление и т.д.) к сервисам и критичным параметрам безопасности.

Управление доступом пользователей к ОО может быть основано на ролевой политике управления доступом (RBAC), политике управления доступом, основанной на идентификаторе (IBAC), или на сочетании этих двух политик.

В некоторых проектах персонал, ответственный за сопровождение, может обойти механизмы управления доступом ОО, содержащего криптографические функциональные возможности. Таким образом, может также потребоваться реализация политики управления доступом при сопровождении. Эта политика должна регламентировать, каким образом информация пользователей должна быть защищена от доступа со стороны персонала, ответственного за сопровождение, что может быть достигнуто процедурными и/или техническими мерами. Примером может служить следующая политика:

До того, как персоналу, ответственному за сопровождение, будет разрешен доступ к ОО:

a) вся открытыя информация должна быть зашифрована с использованием мастер-ключа;

b) мастер-ключ должен быть изъят, а его копия внутри ОО должна быть обнулена.

После того, как персонал, ответственный за сопровождение, выполнит свои задачи по сопровождению, мастер-ключ должен быть загружен в ОО, чтобы расшифровать предварительно зашифрованную информацию.

С.5.5.3.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Следует выбирать компонент(ы) из следующих семейств:

a) FDP_ACC (политика управления доступом);

b) FDP_ACF (функции управления доступом);

c) FDP_IFC (политика управления информационными потоками).

Криптографические ключи должны храниться и защищаться в ОО. Ключи пользователей могут быть защищены в соответствии с политикой управления доступом с использованием компонента из семейства FDP_ACC. Системные ключи могут быть защищены в соответствии с семейством FMT_MTD.

Как минимум, следует использовать компонент FDP_ACC.1. С использованием этого компонента следует определять ПФБ для управления доступом всех субъектов к активам ИТ, связанным с криптографией. В зависимости от других функций и ПФБ для ОО в целом компонент FDP_ACC.2 может оказаться более подходящим.

FDP_ACF.1 следует использовать для определения требования по реализации ПФБ управления доступом пользователей:

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять политику управления доступом пользователей к объектам, основываясь на [назначение: атрибуты безопасности, именованные группы атрибутов безопасности].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте: субъекту разрешено выполнение криптографических операций, используя [назначение: объекты].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах: [назначение: правила, основанные на атрибутах безопасности, которые явно разрешают доступ субъектов к объектам].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах: [назначение: правила, основанные на атрибутах безопасности, которые явно запрещают доступ субъектов к объектам].

Субъектами в приведенном примере являются пользователи или активные абстрактные сущности (например, процессы), действующие от имени пользователя.

Каждый субъект имеет атрибут-идентификатор пользователя, текущую роль(и) и текущее время (если применимо).

Объектами в приведенном выше примере являются открытые данные и незашифрованные криптографические ключи. В качестве объекты могут также рассматриваться зашифрованные данные и зашифрованные криптографические ключи.

Примерами атрибутов объектов являются криптографическая функция объекта, связанная с объектом роль, пользователи, связанные с объектом, идентификатор объекта и срок действия (если применимо) для объекта.

Данная политика безопасности не регламентирует защиту открытого текста или защищенных (например, зашифрованных) критичных параметров безопасности, таких как аутентификационная информация. Для защиты аутентификационной информации (даже если используется шифрование) должны использоваться соответствующие семейства и компоненты из класса FMT (например, должно использоваться семейство FMT_MSA для определения политики управления защитой аутентификационных данных).

Если атрибуты субъекта, запрашиваемая криптографическая функция и атрибуты объекта удовлетворяют правилу(ам), определенному FDP_ACF.1, тогда разрешается выполнение данной функции.

Криптографический ключ также должен быть защищен в соответствии с политикой управления информационными потоками. Политика управления информационными потоками должна быть определена при использовании компонента из семейства FDP_IFC.

С.5.5.4 Политка аудита и учета

С.5.5.4.1 Руководство

Требования к ОО, связанные с аудитом и учетом (если предъявляются), следует определить в ПЗ и ЗБ.

Процедурные требования могут включать в себя:

a) определение того, когда необходимо осуществлять инспекцию ОО для физического вмешательства или ошибок (примерами могут служить: установленный минимальный период; случай возникновения подозрения о вмешательстве или неожиданной ошибке; возможное нарушение пользователем предположений о среде; при возможном нарушении пользователем обязанностей по физической защите ОО);

b) способ обнаружения и отчета о физическом вмешательстве или ошибках.

Если ОО осуществляет функциональные возможности аудита и учета, то разработчики должны обеспечить, чтобы чувствительная информация (например, секретные или частные криптографические ключи) не содержались бы в какой-либо форме в записях аудита.

С.5.5.4.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для выражения процедурных требований к аудиту и учету в ПЗ и ЗБ следует использовать предположения безопасности.

Минимальный и базовый уровни аудита определены как для для семейства FCS_CKM, так и для семейства FCS_COP. Подробная информация по использованию компонентов аудита, а также требований аудита для других поддерживающих функциональных требований представлена в ИСО/МЭК 15408-2. События и действия, подвергаемые аудиту, должны быть тщательно отобраны так, чтобы важные события аудита регистрировались и могли быть проанализированы, не затерявшись в чрезмерных данных аудита.

С.5.5.5 Политика управления криптографическими ключами

С.5.5.5.1 Руководство

Криптографические ключи должны использоваться и управляться безопасным способом на протяжении всего их жизненного цикла. Жизненный цикл включает в себя генерацию криптографического ключа, распределение криптографического ключа, доступ к криптографическому ключу (включая резервное копирование, архивирование, восстановление) и уничтожение криптографического ключа.

С.5.5.5.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для спецификации требований политики управления криптографическими ключами в ПЗ и ЗБ следует выбирать компонент(ы) из семейства FCS_CKM (управление криптографическими ключами).

Семейство FCS_CKM определяет требования для различных функций управления криптографическими ключами. Если ОО выполняет одну или более из этих функций управления криптографическими ключами, то следует выбрать соответствующий(ие) компонент(ы) из семейства FCS_CKM.

С.5.5.6 Политика физической безопасности

С.5.5.6.1 Руководство

Требования политики физической безопасности, относящиеся к аппаратным и программно-аппаратным средствам, составляющим ОО и среду, в пределах которой расположен ОО, должны быть описаны в ПЗ и ЗБ.

Политика физической безопасности должна учитывать следующие аспекты:

a) предположения относительно среды (они должны быть теми же, что и общие предположения относительно среды для любых ПЗ и ЗБ независимо от того, включают ли они криптографию или нет). Эти предположения должны быть выражены типовым способом (см. раздел 8). Однако, если они относятся непосредственно к требованиям к программным средствам, программно-аппаратным средствам и/или аппаратным средствам среды ИТ, то они должны быть оформлены как требования безопасности для среды ИТ;

b) обязанности разных типов пользователей и администраторов по физической защите ОО (данная информация также должна быть задокументирована в руководствах пользователя и администратора).

С.5.5.6.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Физические, процедурные меры и меры, связанные с персоналом, внешние по отношению к ОО, следует обычно выражать в виде предположений. Кроме того, должны быть выбраны компоненты из следующих двух семейств доверия:

a) AGD_USR (руководство пользователя);

b) AGD_ADM (руководство администратора).

Компонент(ы) из семейства AGD_ADM следует использовать для выражения требования по документированию физических ограничений и ограничений относительно среды, в соответствии с которыми ФБО должны находиться под управлением администратора.

Компонент(ы) из семейства AGD_USR следует использовать для выражения требования по документированию физических ограничений и ограничений относительно среды, в соответствии с которыми ФБО должны находиться под управлением пользователя.

Если сам ОО реализует требования по физической безопасности, то для включения в ПЗ и ЗБ следует выбрать компонент(ы) из семейства FPT_PHP (физическая защита ФБО). Эти компоненты могут использоваться для выражения требований к физической безопасности, которые будут реализованы в ФБО для предотвращения физического вмешательства, а также реагирования на такие нападения.

В приведенном ниже примере компонент FPT_PHP.2 выражает требования к физической безопасности для защиты аппаратных и программно-аппаратных средств ОО. Компонент FPT_PHP.3 определяет действия, предпринимаемые для защиты связанных с криптографией активов ИТ при обнаружении вмешательства:

FPT_PHP.2 Оповещение о физическом нападении

FPT_PHP.2.1 ФБО должны обеспечить однозначное обнаружение физического воздействия, которое может угрожать выполнению ФБО. Реализация ФБО должна быть полностью внутри оболочки, позволяющей обнаруживать вмешательства путем сверления, дробления или измельчение содержимого ОО или его покрытия.

FPT_PHP.2.2 ФБО должны предоставить возможность определить, произошло ли физическое воздействие на устройства или элементы, реализующие ФБО.

FPT_PHP.2.3 Для устройств/элементов, реализующих ФБО, ФБО должны постоянно контролировать устройства, элементы и оповещать пользователя ОО о том, что произошло физическое воздействие на устройства или элементы, реализующие ФБО.

FPT_PHP.3 Противодействие физическому нападению

FPT_PHP.3.1 ФБО должны противодействовать следующим сценариям физического воздействия на устройства и элементы, реализующие ФБО, автоматически реагируя так, чтобы предотвратить нарушение ПБО:

a) ОО должен содержаться в пределах крепкого несъемного корпуса. Корпус должен быть спроектирован таким образом, чтобы попытки удалить его или проникнуть через него приводили с высокой вероятностью к серьезному повреждению ОО (то есть ОО станет неработоспособным);

b) если покрытие ОО или корпус содержат какие-нибудь вентиляционные отверстия или щели, то они должны быть маленькими и выполнены таким образом, чтобы предотвратить необнаруженное физическое вмешательство внутрь корпуса;

c) после обнаружения вмешательства все открытые криптографические ключи и другие незащищенные критические параметры безопасности должны быть немедленно обнулены.

С.5.5.7 Политика управления электромагнитными излучениями

С.5.5.7.1 Руководство

Уровень электромагнитных излучений ОО должен быть ограничен с тем, чтобы предотвратить раскрытие связанных с криптографией активов ИТ неуполномоченными лицами или пользователями. Кроме того, также должны быть приняты процедурные и физические меры для предотвращения обнаружения электромагнитных излучений неуполномоченными лицами или пользователями. Также могут быть заданы требования по физической защите, касающейся предотвращения побочных электромагнитных излучений (ЭМИ)/ радиочастотных излучений от нежелательных источников, по причине обеспечения их целостности или доступности.

Оценка технических физических аспектов безопасности ИТ, например таких, как управление электромагнитными излучениями, не рассматривается в стандартах серии ИСО/МЭК 15408 (см. ИСО/МЭК 15408-1), хотя многие из этих понятий будут применимы и в этой области. В частности, в стандартах серии ИСО/МЭК 15408 рассматриваются некоторые аспекты физической защиты ОО.

С.5.5.7.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Правила политики безопасности организации (см. С.4.3) должны использоваться для определения способов управления электромагнитными излучениями ОО.

Учитывая то, что требования к оценке электромагнитных излучений исключены из стандартов серии ИСО/МЭК 15408, должен быть использован механизм предположений безопасности для четкого формулирования требований к ОО по реализации этой политики безопасности. Предположения должны также использоваться для спецификации процедурных и физических мер, которые должны быть приняты для предотвращения обнаружения электромагнитных излучений неуполномоченными лицами или пользователями, или предотвращения нежелательных излучений ЭМИ или в радиочастотном диапазоне.

С.5.6 Функциональные возможности безопасности объекта оценки

С.5.6.1 Введение

Функциональные возможности безопасности, требуемые для осуществления аспектов политики безопасности ОО, рассмотрены в предыдущем разделе. В данном разделе настоящего стандарта рассматриваются оставшиеся функциональных возможности безопасности, которые обычно находятся в пределах ОО, содержащем криптографические функциональные возможности.

Для обеспечения эффективности и безопасности ОО, содержащего криптографические функциональные возможности, обычно необходимо рассмотреть два вида требований безопасности:

1) криптографические функциональные требования безопасности;

2) другие некриптографические функциональные требования и требования доверия безопасности, которые поддерживают эти криптографические функциональные возможности и политику безопасности ОО.

Способы выражения политики безопасности ОО на базе стандартов серии ИСО/МЭК 15408 изложены в С.5.5.

С.5.6.2 Криптографические функциональные возможности

С.5.6.2.1 Руководство

Криптографическими ключами необходимо управлять на протяжении всего их жизненного цикла. Типовые события в жизненном цикле криптографического ключа включают в себя (но не ограничиваются): генерацию, распределение, ввод, хранение, доступ (например, резервное копирование, архивирование, восстановление) и уничтожение.

Как минимум, криптографические ключи должны пройти следующие стадии: генерацию, хранение и уничтожение. Наличие других стадий зависит от осуществляемой стратегии управления ключами, поскольку ОО не дол-

жен быть связан со всем жизненным циклом ключа (например, ОО может только генерировать и распределять криптографические ключи).

Фактически криптографические функциональные требования безопасности могут быть разделены на два подвида:

a) функциональные требования безопасности по выполнению аспектов управления криптографическими ключами, например:

- генерация криптографического ключа,
- распределение криптографического ключа,
- доступ к криптографическому ключу,
- уничтожение криптографического ключа;

b) функциональные требования безопасности по выполнению криптографических операций, например:

- генерация и/или верификация цифровой подписи,
- генерация криптографической контрольной суммы для контроля целостности и/или для верификации контрольной суммы,
- вычисление хэш-функции (дайджеста сообщение или файла),
- шифрование и/или расшифровывание данных,
- шифрование и/или расшифровывание криптографического ключа,
- согласование криптографического ключа.

Как отмечалось во вводной части настоящего приложения, область применения данного руководства не включает в себя стойкость криптографии, включая длину ключа и стойкость алгоритма. Ни одно функциональное семейство или семейство требований доверия из стандартов серии ИСО/МЭК 15408 (включая AVA_SOF) не должно использоваться для оценки стойкости криптографических функций или длины используемых ключей. Это связано с тем, что стандарты серии ИСО/МЭК 15408 не предназначены для оценки криптографических алгоритмов и связанных с ними технических средств. Требуется независимая оценка математических свойств криптографии, включенной в ОО. Система, которая применяется в стандартах серии ИСО/МЭК 15408, должна создать условия для такой оценки (см. ИСО/МЭК 15408-1). Предполагается, что эта система может требовать соответствия дополнительным стандартам или критериям, регламентирующие область криптографии.

Реализация генератора псевдослучайных чисел также является критичной по безопасности криптографических ключей и криптографических операций. Должны быть выбраны алгоритм и параметры, связанные с генератором псевдослучайных чисел, позволяющие оптимизировать степень непредсказуемости и область значений случайного числа. Для реализации генератора псевдослучайных чисел следует обеспечить требуемую стойкость функции безопасности ОО (AVA_SOF). См. также [9].

С.5.6.2.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

В зависимости от криптографических функций, которые выполняет ОО, для включения их в ПЗ и ЗБ следует выбрать компонент(ы) из следующих семейств:

a) FCS_CKM (управление криптографическими ключами);

b) FMT_MSA (управление атрибутами безопасности);

c) FCS_COP (криптографические операции).

Необходимо отметить, что класс FCS включает в себя два семейства: FCS_CKM (управление криптографическими ключами) и FCS_COP (криптографические операции). Семейство FCS_CKM включает в себя аспекты управления криптографическими ключами, а семейство FCS_COP связано с использованием этих криптографических ключей. См. также [6].

Компонент(ы) из семейства FCS_CKM может (могут) использоваться для определения функциональных требований, связанные с различными аспектами политики управления криптографическими ключами. Семейство предназначено для поддержки жизненного цикла криптографических ключей и, следовательно, определяет требования к генерации, распределению, доступу и уничтожению криптографических ключей. Данное семейство должно быть использовано при наличии функциональных требований по управлению или администрированию криптографических ключей.

При этом разработчики ПЗ и ЗБ должны учитывать, что:

a) семейство FCS_CKM не включает в себя компонент для защиты криптографических ключей при хранении. Рекомендуется для регламентации защиты криптографических ключей пользователей, сохраненных в ФБО (то есть, сохраненных как данные пользователя), использовать компоненты из семейств FDP_ACC (политика управления доступом) и FDP_ACF (функции управления доступом). Защита криптографических ключей ФБО (то есть, сохраненных как данные ФБО) должна быть регламентирована путем использования компонентов из семейства FPT_SEP (разделение домена) или семейства FMT_MTD (управление данными ФБО). Необходимо отметить, что классы FDP или FPT могут использоваться для обеспечения конфиденциальности и/или целостности криптографических ключей;

b) семейство FCS_CKM не содержит компонентов для защиты ввода криптографического ключа. Криптографические ключи могут вводиться в незашифрованной, зашифрованной или разделенной форме. Для спецификации этого требования следует использовать компонент из семейства FDP_ITC (импорт данных из-за пределов действия ФБО). Если компонент из семейства FDP_ITC используется, то для определения необходимости шиф-

рования или разделения криптографических ключей должно быть выполнено назначение «дополнительные правила управления импортом»;

c) на основе компонентов из семейства FCS_CKM должны быть выражены аспекты безопасности криптографических протоколов, в особенности те, которые касаются распределения криптографических ключей (FCS_CKM.2);

d) если необходимо предусмотреть возможность отзыва публичных криптографических ключей, то следует использовать компонент FCS_CKM.2 для регламентации отзыва публичного криптографического ключа. Аргументом использования компонента FCS_CKM.2 является то, что этот компонент определяет схему распределения криптографических ключей, а распространение информации об отзыве и аннулировании ключей рассматривается как неотъемлемая часть распределения криптографических ключей (например, это следует из стандарта X.509 для списков аннулированных и отозванных сертификатов).

Компонент(ы) из семейства FMT_MSA (управление атрибутами безопасности) следует использовать для определения атрибутов криптографических ключей. Примерами атрибутов ключей являются: пользователь, тип ключа (например, публичный, частный, секретный), срок действия и область использования (например, цифровая подпись, шифрование ключа, согласование ключей, шифрование данных).

Компонент(ы) из семейства FCS_COP может (могут) использоваться для определения функциональных требований по выполнению криптографических операций. Криптографические операции могут использоваться для поддержки одного или более сервисов безопасности ОО. Компонент FCS_COP может использоваться более чем один раз, в зависимости от:

a) пользовательских приложений, для которых используется сервис безопасности;

b) использования различных криптографических алгоритмов и/или длин криптографических ключей;

c) использования различных типов и/или чувствительности обрабатываемых данных.

Если ОО не осуществляется управление или осуществляется управление только частью жизненного цикла криптографических ключей, то любые требования, не относящиеся к ОО (то есть, к среде ОО), должны быть выражены в виде предположений безопасности.

С.5.6.3 Импорт, экспорт и передача между функциями безопасности объекта оценки связанных с криптографией активов информационных технологий

С.5.6.3.1 Руководство

Политика управления доступом пользователей подразумевает обеспечение безопасности связанных с криптографией активов ИТ (таких, например, как незашифрованные криптографические ключи, данные аутентификации открытого текста и другие критичные параметры безопасности), которые передаются через недоверенные компоненты или напрямую к (от) человеку(а)-пользователю(я).

Важно, чтобы пользователи знали о чувствительности этой информации и случайно не смешали ее с другой. Первоначально разработчики криптографии достигали этого реализацией отдельных физических каналов для ввода и вывода этой информации; таким образом, пользователи и ОО знали о чувствительности информации. Альтернативный подход может заключаться в использовании меток безопасности данных.

С.5.6.3.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Следует выбирать компонент(ы) из следующих семейств:

a) FDP_ITC (импорт данных из-за пределов действия ФБО);

b) FDP_ETC (экспорт данных за пределы действия ФБО);

c) FTP_ITC (доверенный канал передачи между ФБО), или FTP_TRP (доверенный маршрут).

Элемент(ы) компонента FDP_ITC.2 следует использовать для выражения требований безопасности по введению информации в ОО, что должно реализовываться использованием ПФБ Управления доступом пользователями.

Элемент(ы) компонента FDP_ETC.2 следует использовать для определения правил экспорта данных из ОО, что должно реализовываться использованием ПФБ Управления доступом пользователями.

Компонент(ы) из семейства FTP_ITC следует использовать для выражения требований безопасности по передаче криптографических активов между ФБО и ФБО другого ОО. В качестве альтернативы, для выражения требований для ввода и вывода криптографических активов от(к) человека(у)-пользователя(ю) может (могут) использоваться компонент(ы) из семейства FTP_TRP . Однако разработчики ПЗ и ЗБ должны учитывать, что использование семейств FTP_TRP и FTP_ITC является взаимоисключающим.

В представленном ниже примере использован компонент из FPT_TRP:

FTP_TRP.1 Доверенный маршрут

FTP_TRP.1.1 ФБО должны предоставлять маршрут связи между собой и локальными пользователями, который логически отличим от других маршрутов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту передаваемых данных от модификации или раскрытия.

FTP_TRP.1.2 ФБО должны позволить ФБО и локальным пользователям инициировать связь через доверенный маршрут.

FTP_TRP.1.3 ФБО должны требовать использования доверенного маршрута для начальной аутентификации пользователей, ввода и вывода компонентов незашифрованных криптографических ключей, открытых аутентификационных данных и других незащищенных критичных по безопасности параметров.

С.5.6.4 Поддержка безопасного состояния

С.5.6.4.1 Руководство

Первоначально озабоченность по поводу проектных ошибок или сбоев в ОО, содержащем криптографические функциональные возможности, приводят к следующим типам предъявляемых требований:

a) для предотвращения неумышленного вывода чувствительной криптографической информации, требуется два независимых внутренних действия для вывода данных через любой интерфейс вывода, через который незашифрованные криптографические ключи или другие критичные параметры безопасности или чувствительные данные могли быть выведены (выданы);

b) когда обнаруживается ошибка в ОО, то ОО должен перейти в аварийный режим и запретить любой вывод (выдачу) информации.

Предназначение типа по перечислению a) заключается в том, чтобы удостовериться, что ошибка в проекте или функционировании ОО не приведет к случайной выдаче чувствительной криптографической информации (он также предусматривает, что ОО может обнаружить выдачу чувствительной криптографической информации). Предназначение типа по перечислению b) заключается в том, что когда ОО обнаруживает ошибку, он не должен допустить выдачу чувствительной криптографической информации. Таким образом, в случае появления ошибки ОО всегда должен стремиться сохранять безопасное состояние.

С.5.6.4.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для выражения требований к ОО по сохранению безопасного состояния при возникновении ошибок следует выбирать компонент(ы) из семейства FPT_FLS (безопасность при сбое). Например:

FPT_FLS.1 Сбой с сохранением безопасного состояния

FPT_FLS.1.1 ФБО должны сохранить безопасное состояние при следующих типах сбоев:

a) ОО некорректно попытается выдать незашифрованные криптографические ключи, чувствительные открытые данные или других незащищенные критичные параметры безопасности;

b) сбой криптографической функции;

c) сбой в тестировании абстрактной машины ОО (при запуске, по запросу и/или по условию);

d) обнаружение физического вмешательства в ОО (включая нарушение среды).

Безопасное состояние должно означать, что выдача подавляется, и никакие другие функции не выполняются, пока не будет выполнено надежное восстановление.

Разработчики ПЗ и ЗБ должны учесть, что этот компонент зависит от компонента ADV_SPM.1 (неформальная модель политики безопасности ОО). Кроме того, разработчики ПЗ и ЗБ должны будут также включить в ПЗ и ЗБ компоненты для спецификации функциональных возможностей, которые могут породить ошибку (например, функциональные возможности по самотестированию ОО).

Компонент(ы) из семейства FPT_RCV может (могут) использоваться для спецификации требований по возврату ОО к безопасному состоянию и/или предотвращения перехода к небезопасному состоянию.

С.5.6.5 Самотестирование криптографических функций

С.5.6.5.1 Руководство

Из потребности в обнаружении ошибок в ОО следует потребность для любого ОО сохранять безопасное состояние при возникновении этих ошибок.

Как правило при разработке ОО предусматривается возможность проведения самотестирования в части криптографических функциональных возможностях для обеспечения корректной работы. Самотестирование обычно включает в себя:

a) самотестирование при запуске (при включении электропитания или загрузке):

- тестирование ожидаемого отклика,
- тестирование целостности программного обеспечения/программно-аппаратных средств,
- тестирование генератора случайных чисел;

b) тестирование по запросу:

- тестирование ожидаемого отклика,
- тестирование целостности программного обеспечения/программно-аппаратных средств,
- тестирование генератора случайных чисел;

c) тестирование при выполнении определенных условий:

- генерация пары (секретный/открытый) ключей, тестирование соответствия ключевой пары,
- загрузка программного обеспечения/ программно-аппаратных средств проверка целостности программного обеспечения/программно-аппаратных средств,
- ввод ключа, тестирование целостности ключа,
- генерация случайного числа, тестирование случайного числа.

С.5.6.5.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для спецификации требований по самотестированию ОО должен(ы) быть выбран(ы) компонент(ы) из одного или нескольких следующих семейств:

a) FDP_SDI (целостность хранимых данных);

b) FPT_AMT (тестирование базовой абстрактной машины);

c) FPT_TST (самотестирование ФБО).

Компонент(ы) из семейства FDP_SDI следует использовать для выражения требования по обнаружению нарушений целостности данных и (при необходимости) принятию корректирующих действий.

Компонент(ы) из семейства FPT_AMT следует использовать для спецификации тестов базовой абстрактной машины (например, при запуске, по запросу и условию).

Компонент (ы) из семейства FPT_TST следует использовать для выражения следующих требований: обнаружение искажения криптографического кода в результате различных сбоев, которые не обязательно приводят к нарушению работоспособности ОО; проверка, что ФБО работает корректно (например, при запуске, по запросу и условию).

С.5.6.6 Внешние зависимости

С.5.6.6.1 Руководство

При определенных обстоятельствах ОО может зависеть от других программных, программно-аппаратных или аппаратных средств (например, от функциональных возможностей безопасности базовой операционной системы).

С.5.6.6.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

В соответствии с разделом 10, ФТБ, которые должны быть удовлетворены применением других программных, программно-аппаратных или аппаратных средств, внешних по отношению к ОО, должны быть определены в подразделе ПЗ или ЗБ, относящемся к требованиям безопасности для среды ИТ.

С.5.7 Тестирование объекта оценки

С.5.7.1 Руководство

Функциональные возможности ОО должны быть протестированы для обеспечения доверия, что ФБО удовлетворяет, по крайней мере, установленным ФТБ. Следовательно должны быть выбраны требования к тестированию с учетом чувствительности приложений и потребности в доверии. Необходимо обратить внимание на то, должно ли тестирование проводиться независимой третьей стороной, на строгость тестирования и покрытие тестами, уровень абстракции ОО, связанный со строгостью тестирования (например, функциональная спецификация, проект верхнего уровня, проект нижнего уровня).

С.5.7.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Обычно следует выбирать компонент(ы) из следующих семейств:

a) ATE_COV (покрытие);

b) ATE_DPT (глубина);

c) ATE_FUN (функциональное тестирование);

d) ATE_IND (независимое тестирование);

e) AVA_VLA (анализ уязвимостей).

Компонент(ы) из семейства ATE_COV может (могут) использоваться для спецификации требований к полноте тестирования ОО.

Компонент(ы) из семейства ATE_DPT может (могут) использоваться для спецификации требований к уровню детализации тестирования ОО.

Компонент(ы) из семейства ATE_FUN может (могут) использоваться для спецификации требований по установлению того, что ФБО обладает свойствами, необходимыми для удовлетворения функциональных требований, идентифицированных в ПЗ и ЗБ.

Компонент(ы) из семейства ATE_IND может (могут) использоваться для спецификации требований к демонстрации того, что ФБО выполняются так, как специфицировано.

Компонент(ы) из семейства AVA_VLA может (могут) использоваться для спецификации требований к тестированию недостатков среды ОО, включающего в себя криптографические функциональные возможности.

С.5.8 Эксплуатация объекта оценки

С.5.8.1 Руководство

Должно быть предоставлено руководство по безопасной установке, администрированию и эксплуатации ОО со стороны уполномоченных пользователей ОО.

С.5.8.2 Представление в соответствии со стандартами серии ИСО/МЭК 15408

Для выражения этого требования в ПЗ и ЗБ следует выбрать компонент(ы) из следующих семейств:

a) AGD_ADM (руководство администратора);

b) AGD_USR (руководство пользователя).

Компонент(ы) из семейства AGD_ADM следует использовать для выражения требований документированию того, каким образом администратором должен правильно устанавливаться (инсталлироваться) и администрироваться ОО.

Компонент(ы) из семейства AGD_USR следует использовать для выражения требований документированию того, каким образом пользователем должен правильно эксплуатироваться ОО.

С.6 Руководство по применению требований доверия

Как упоминалось выше, вопросы стойкости криптографии, выбора размера ключа или стойкости какого-либо алгоритма не входят в область применения настоящего стандарта. Тем не менее, хотя вопросы выбора или пригодности криптографического алгоритма (и выбора размера ключа) находятся вне области применения стандартов серии ИСО/МЭК 15408, реализация алгоритма в ОО входит в его область применения.

Заявитель оценки ОО отвечает за выбор алгоритма(ов), способа(ов) и размера(ов) ключей, которые используются в ОО. Заявитель может использовать один или несколько из описанных ниже подходов для обеспечения корректности реализации:

a) предоставить соответствующую реализацию;

b) гарантировать соответствие реализации стандарту;

c) отказаться от требований по тестированию соответствия;

d) выполнить тестирование на соответствие;

e) потребовать проведения тестов на соответствие оценщиками. Эти тесты должны проводиться с использованием установленных в стандартах тестов на соответствие. Если в стандартах не установлены тесты на соответствие, заявитель может их предоставить или указать другой источник для получения тестов;

f) проанализировать реализацию (например, провести детальный анализ кода) в соответствии с компонентом ADV_RCR;

g) требовать, чтобы оценщики проанализировали реализацию (например, провели детальный анализ кода) в соответствии с компонентом ADV_RCR.

Примечание — Заявитель может отказаться от анализа реализации независимо от уровня доверия согласно стандартам серии ИСО/МЭК 15408, поскольку исходный код может быть недоступен для оценщиков вследствие чувствительности алгоритма. От тестирования соответствия алгоритма, вероятно, также может быть придется отказаться вследствие отсутствия пригодных тестов для оценки соответствия (это, в частности, может иметь место для новых алгоритмов).

Приложение D
(рекомендуемое)

Рабочий пример: профиль защиты и задание по безопасности для межсетевого экрана

D.1 Введение

В настоящем приложении проиллюстрировано применение руководства, содержащегося в разделах 7—13, посредством рабочего примера применительно к межсетевому экрану.

D.2 Описание объекта оценки

В ПЗ представлено общее описание области применения ОО и его функциональных возможностей по обеспечению безопасности (так как единственное назначение ОО — обеспечение безопасности). Более детальное описание области применения ОО и его функциональных возможностей по обеспечению безопасности представлено в ЗБ, в частности:

a) идентификация операционной системы, под управлением которой работает межсетевой экран, и аппаратной платформы;

b) краткое описание среды функционирования, например, в части необходимости физической защиты ОО и различий между администратором межсетевого экрана и пользователями (которые не получают непосредственного доступа к межсетевому экрану).

D.3 Среда безопасности объекта оценки

D.3.1 Предположения безопасности

Для межсетевого экрана может быть определен ряд предположений, связанных с обеспечением эффективности функционирования межсетевого экрана. Например:

a) межсетевой экран должен быть универсальным посредником, так как существует возможность обойти его (межсетевой экран);

b) только администраторы могут получить доступ к межсетевому экрану: данное предположение необходимо в целях ограничения возможностей, доступных нарушителям.

Предположения, относящиеся к использованию свойств безопасности (например, управление и анализ журнала аудита), следует трактовать как цели безопасности для среды либо как требования безопасности, не относящиеся к ИТ.

D.3.2 Угрозы

Предполагается, что среда для межсетевого экрана включает в себя, с одной стороны, частную сеть и, с другой стороны, предположительно враждебную сеть. Поэтому активы ИТ, подлежащие защите, — это предоставляемые частной (приватной) сетью сервисы и информация, хранимая в частной сети. Источники угрозы в основном — это нарушители из враждебной (внешней) сети.

Ниже приведен пример угрозы, которой должен противостоять межсетевой экран:

Нарушитель из враждебной (внешней) сети может использовать недостатки реализации сервисов для того, чтобы получить доступ к хостам (узлам частной сети) или другим сервисам.

Формулировка угрозы оперирует следующими понятиями:

a) источник угрозы — нарушитель из потенциально враждебной (внешней) сети;

b) активы ИТ, подверженные нападению, — это хосты (узлы) или другие сервисы частной сети;

c) форма нападения — использование недостатков реализации сервисов.

Хотя большинство угроз, с которыми сталкивается межсетевой экран, связано с нарушителями из враждебной сети, существуют угрозы, когда нарушитель может находиться как во враждебной, так и в частной сети:

нарушитель может получить доступ к межсетевому экрану, выдавая себя за администратора.

Идентифицированные угрозы, которым ОО не противостоит, отражают практические ограничения в отношении межсетевого экрана. Например:

a) определенные способы атак, применяемые нарушителями из враждебной сети, которым ОО не противостоит, такие как перехват сеанса и поиск (сниффинг) данных;

b) частная сеть может стать уязвимой для атак в результате действий злоумышленников из частной сети;

c) уязвимость частной сети со стороны вирусов, которые могут содержаться во входящем трафике — это также угроза, для противостояния которой межсетевой экран не предназначен;

d) частная сеть может стать уязвимой для атак в результате действия или бездействия администратора межсетевого экрана;

e) частная сеть может стать уязвимой для атак в результате непосредственной физической атаки на межсетевой экран.

Ниже приведена возможная (заслуживающая особого внимания) угроза для межсетевого экрана, выполняющего роль шлюза прикладного уровня (далее — МЭ прикладного уровня):

нарушители из враждебной сети используют новые, ранее неизвестные, методы атак, например, используя прежде заслуживающие доверия сервисы.

Из этого следует, что угроза со стороны нарушителей из враждебной сети является динамической (то есть непрерывно изменяющейся), а значит, сам ОО должен изменяться, например, определяя полномочия для новых прикладных программ.

D.3.3 Политика безопасности организации

Обычно должна существовать возможность настройки межсетевого экрана для реализации ряда различных правил ПБОр.

В этом случае можно сформулировать в общем виде политику управления доступом, которая должна осуществляться межсетевым экраном.

D.4 Цели безопасности

D.4.1 Цели безопасности для объекта оценки

Цели безопасности для межсетевого экрана можно сформулировать следующим образом:

a) Цель O1 — основная цель безопасности должна определить требования к функциональным возможностям управления доступом, обеспечиваемым межсетевым экраном, например, в виде ограничений допустимого диапазона адресов, списка хостов (узлов) и портов, к которым разрешен доступ.

b) Цель O2 — к межсетевому экрану прикладного уровня может быть предъявлено требование организовать серверы полномочий (сервер полномочий перехватывает попытки соединений с серверами и затем сам посылает запросы на нужные серверы от имени пользователей; когда сервер возвращает информацию, сервер полномочий пересылает ее пользователю) в целях противостояния атакам, основанным на недостатках реализации прикладных сервисов.

c) Цель O3 — аналогично может существовать требование аутентификации полномочий приложений.

d) Цель O4 — требование к функциональным возможностям аудита, обеспечивающим средства регистрации событий, относящихся к безопасности.

e) Цель O5 — требование к функциональным возможностям управления безопасностью в части функций, которые должны быть доступны администраторам, а также в части управления доступом к этим функциональным возможностям.

Пример цели безопасности для ОО:

межсетевой экран должен, для определенных сервисов частной сети, выполнять необходимую аутентификацию конечного пользователя до установления соединения.

Таким образом, в ОО должны быть реализованы функциональные возможности по идентификации и аутентификации. Следует отметить, что так как в ПЗ не определяются сервисы, которые необходимо обеспечить, то в цели безопасности не определяется подмножество сервисов, требующих аутентификации. Данное утверждение оставляется на рассмотрение автору ЗБ, который (в обосновании ЗБ) должен обосновать список сервисов, требующих (или которые могут быть соответствующим образом настроены так, чтобы требовать) аутентификации конечного пользователя.

D.4.2 Цели безопасности для среды

Ниже приведен пример цели безопасности для среды, являющейся требованием к использованию функциональных возможностей аудита:

администраторы межсетевого экрана должны обеспечить эффективное использование и управление средствами аудита. В частности, должны быть выполнены соответствующие действия в целях обеспечения непрерывного ведения аудита, например, путем регулярного архивирования файлов журналов аудита с тем, чтобы обеспечить достаточное свободное пространство (на диске). Кроме того, файлы журналов аудита должны регулярно просматриваться, и должны быть предприняты соответствующие действия по обнаружению нарушений безопасности или событий, которые могут привести к нарушению безопасности в будущем.

Данная цель безопасности близко связана с целью безопасности для межсетевого экрана по обеспечению функциональных возможностей аудита.

D.5 Требования безопасности информационных технологий

D.5.1 Функциональные требования безопасности

Для непосредственного удовлетворения целей безопасности для ОО, описанных в предыдущем разделе, могут быть выбраны следующие ФТБ:

a) цель безопасности O1 может быть удовлетворена соответствующим использованием FDP_ACF.1 (управление доступом, основанное на атрибутах безопасности) и FDP_ACC.2 (полное управление доступом) либо FTA_TSE.1 (открытие сеанса с ОО);

b) цель безопасности O2 может быть удовлетворена FIA_UAU.2 (аутентификация до любых действий пользователя) и FIA_UID.2 (идентификация до любых действий пользователя). Другие подходящие ФТБ: FIA_UAU.3 (аутентификация, защищенная от подделок), FIA_UAU.4 (механизмы одноразовой аутентификации) и FIA_UAU.5 (сочетание механизмов аутентификации), поскольку они учитывают спецификацию более сильных опознавательных механизмов;

c) цель безопасности O4 может быть удовлетворена FAU_GEN.1 (генерация данных аудита) и FAU_ARP.1 (сигналы нарушения безопасности) с тем, чтобы обеспечить анализ информации аудита в реальном масштабе времени;

d) цель безопасности O5 может быть удовлетворена FMT_SMR.1 (роли безопасности) вместе с FIA_UAU.2 и FIA_UID.2, использующими аутентификацию администратора межсетевого экрана.

После формирования начального набора остальные ФТБ выбирают главным образом, для того, чтобы удовлетворить зависимости. Дополнительные ФТБ могут быть включены, потому что они обеспечивают полезную (но не существенную) поддержку полномочий и, например, могут включать в себя FIA_AFL.1 (обработка отказов аутентификации), FPT_RVM.1 (невозможность обхода ПБО) и FPT_SEP.3 (полный монитор обращений).

Далее необходимо выбрать соответствующий уровень аудита (то есть «неопределенный», «минимальный», «базовый» или «детализированный»). Этот уровень должен соответствовать целям безопасности для ОО.

Далее необходимо (если требуется) использовать операцию назначения.

D.5.2 Требования доверия к безопасности объекта оценки

Выбор требований доверия должен быть относительно простым. Если авторы ПЗ и ЗБ не считают необходимым расширение или усиление требований доверия, то выбор последних сводится к выбору соответствующего оценочного уровня доверия к безопасности. Например, анализируя характер угроз (включая относительно сложные атаки) и ценность активов ИТ, можно выбрать ОУД4 как наиболее подходящий.

D.5.3 Требования безопасности для ИТ-среды

Необязательно, чтобы межсетевой экран обеспечивал все функциональные возможности, необходимые для удовлетворения целей безопасности для ОО. Например, на операционную систему, под управлением которой работает межсетевой экран, можно возложить хранение журнала аудита межсетевого экрана. Авторы ПЗ поэтому должны решить, какие функциональные возможности должны выполняться межсетевым экраном, а какие могут обеспечиваться операционной системой, под управлением которой работает межсетевой экран.

Выбор требований доверия в рассматриваемом случае соответствует выбору требований доверия для ИТ, например, ОУД4.

D.6 Краткая спецификация объекта оценки

D.6.1 Функции безопасности объекта оценки

При построении функций безопасности ИТ авторы ЗБ могут начинать с ФТБ и получать функции безопасности ИТ из них следующим образом:

a) следует добавить (если необходимо) определенные детали ОО для того, чтобы конкретизировать функциональные возможности, особенно для функций межсетевого экрана по управлению доступом (главное назначение ОО);

b) поддерживающие функции (особенно функции управления безопасностью) целесообразно специфицировать в краткой форме, но без потери существенных деталей; в некоторых случаях это приводит к комбинации нескольких функциональных требований в одной функции безопасности.

Пример первых функций безопасности ОО: ОО должен управлять доступом на основе:

- явного IP- адреса или имени хоста источника;
- явного номера порта источника;
- IP- адреса или имени хоста получателя;
- номера порта получателя.

Пример вторых функций безопасности ОО: администратор межсетевого экрана и только он может выполнять следующие функции:

- отображать и изменять параметры межсетевого экрана по управлению доступом;
- инициализировать и изменять данные аутентификации пользователей;
- отображать и изменять атрибуты пользователей;
- выбирать события, которые нужно контролировать;
- выделять подмножество контролируемых событий, предположительно отображающих возможное или предстоящее нарушение безопасности;
- сопоставлять отдельные механизмы аутентификации с определенными событиями аутентификации;
- проверять целостность межсетевого экрана.

Таким образом, можно интегрировать требования нескольких ФТБ в одной функции безопасности ИТ (ФТБ необходимо определить, используя FMT_MSA.1.1, FMT_MOF.1.1, FMT_MTD.1.1 и FPT_TST.1.3).

D.7 Утверждения о соответствии профиля защиты

В этом разделе ЗБ для межсетевого экрана следует идентифицировать в профили защиты для межсетевых экранов, на которых основано данное ЗБ, и продемонстрировать согласованность ЗБ с этими ПЗ.

D.8 Обоснование профиля защиты

D.8.1 Обоснование целей безопасности

Демонстрация пригодности целей безопасности для того, чтобы противостоять угрозам, может быть осуществлена:

a) с использованием таблицы, показывающей, какие цели безопасности каким угрозам соответствуют (например, O.ACCESS (O1), которая определяет потребность в политике управления доступом межсетевого экрана, может соответствовать угрозам, относящимся к нарушителям из враждебной сети, типа IP-спуфинга (подмена IP-адреса) или атаки на уязвимые сервисы), обеспечивая отображение каждой цели безопасности, по крайней мере, на одну угрозу;

b) путем аргументации для каждой угрозы, а именно: почему идентифицированные цели безопасности являются соответствующими данной угрозе.

Ниже приведен пример объяснения пригодности:

Угроза T.PROTOCOL. Нарушитель из враждебной сети может применить ненадлежащее использование протоколов сервисов (например, использование «известного» номера порта для протокола, отличного от протокола, определенного для использования этого порта).

Цель O.ACCESS ограничивает хосты и порты сервисов, к которым можно обращаться, соответственно, из враждебных (внешних) сетей и частной сети.

Цель O.AUDIT контролирует возможные атаки, предоставляя администратору межсетевого экрана средства их обнаружения и принятия соответствующих мер.

Цель O.ADMIN обеспечивает необходимую поддержку, обеспечивая безопасное административное управление межсетевым экраном, поддерживаемое O.INSTALL и O.TRAIN.

D.8.2 Обоснование функциональных требований безопасности

Демонстрацию пригодности ФТБ для удовлетворения целей безопасности для ОО можно представить следующим образом:

a) показ посредством таблицы, какие ФТБ и каким целям безопасности соответствуют (например, FDP_ACF.1 и FDP_ACC.2 соответствует цели безопасности O.ACCESS (O1)), гарантируя, что каждое ФТБ отображается по крайней мере на одну цель безопасности;

b) обеспечение для каждой цели безопасности для ОО аргументации относительно того, почему идентифицированные ФТБ подходят для удовлетворения цели.

Ниже приведен пример обоснования пригодности:

цель O.ADDRESS. Межсетевой экран должен ограничить диапазон допустимых адресов частной и враждебной (внешней) сети (то есть внешний хост не может подменить внутренний хост).

FDP_ACF.1 вместе с FDP_ACC.2 обеспечивают возможность ограничения доступа, как это требует O.ADDRESS, а FPT_RVM.1 обеспечивает, чтобы эти функции вызывались всегда, когда требуется.

Демонстрация взаимной поддержки и внутренней согласованности может быть обеспечена, во-первых, посредством анализа зависимостей. Во-вторых, она может быть дополнена таблицей, демонстрирующей поддержку ФТБ со стороны других ФТБ для защиты от обхода, вмешательства и блокирования соответствующих ФБО. Демонстрация взаимной поддержки и внутренней согласованности может сопровождаться пояснением данных таблицы. Вместо рассмотрения каждого требования по порядку (что ведет к повторам) можно выделить общие вопросы, необходимые для понимания данных таблицы. Например, атаки вмешательства предотвращаются:

- FPT_SEP.3, который поддерживает разделение на домены и, в частности, предотвращает вмешательство нарушителя в функции безопасности;

- функциями безопасности, которые ограничивают возможности модификации атрибутов или данных настройки уполномоченным администратором (например, основанные на FMT_MSA.1);

- функциями безопасности, которые предотвращают несанкционированную модификацию других данных, целостность которых является критичной для функции безопасности (то есть основанные на FMT_MTD.1).

D.8.3 Обоснование требований доверия к безопасности

Формирование этого раздела ПЗ не должно вызвать особых трудностей, если ПЗ ссылается на ОУД4 и в нем отсутствуют другие, более сильные требования доверия к безопасности. В этом случае можно утверждать, что ОУД4 содержит известный набор взаимно поддерживающих и внутренне непротиворечивых компонентов доверия, для которых все зависимости удовлетворены.

D.9 Обоснование задания по безопасности

В ЗБ, разработанного в соответствии с ПЗ для межсетевого экрана в разделе «Обоснование ЗБ», могут широко использоваться материалы раздела ПЗ «Обоснование ПЗ», в частности:

a) если угрозы, политика безопасности организации, предположения и цели безопасности идентичны, тогда обоснование целей безопасности в ЗБ будет идентично соответствующему обоснованию в ПЗ; следовательно, в данной части обоснования ЗБ можно просто сослаться на соответствующий подраздел обоснования ПЗ;

b) если в ЗБ добавлено небольшое число ФТБ по отношению к ФТБ, определенных в ПЗ, в обосновании ЗБ может быть ссылка на соответствующую часть обоснования ПЗ, а также продемонстрировано:

- что дополнительные требования являются надлежащими для удовлетворения целей безопасности,

- что дополнительные требования не приводят к каким-либо конфликтам, а поддерживают другие требования,

- что дополнительные зависимости были удовлетворены или не должны были быть удовлетворены;

c) если идентичные ПЗ требования доверия к безопасности были определены в ЗБ, то в подразделе ЗБ «Обоснование требований безопасности» можно просто сослаться на соответствующую часть обоснования ПЗ.

Остаются следующие положения, которые должны быть охвачены обоснованием ЗБ:

a) логическое обоснование соответствия ПЗ; оно может быть выполнено посредством использования таблицы для демонстрации покрытия всех ФТБ из ПЗ, а также — таблицы, показывающей выполнение в ЗБ операций, предусмотренных в ПЗ;

b) обоснование функций безопасности ИТ; оно может быть выполнено посредством явного сопоставления специфицированных функций безопасности ИТ с ФТБ. Если никаких новых функциональных возможностей на этом уровне не вводится, то демонстрация взаимной поддержки может считаться представленной в обосновании требований безопасности.

Приложение Е
(рекомендуемое)

Рабочий пример: профиль защиты для системы управления базой данных

Е.1 Введение

В настоящем приложении поясняется применение руководства, содержащегося в разделах 7—13, посредством рабочего примера применительно к системе управления базами данных (СУБД). В данном примере предполагается использование СУБД в коммерческих условиях, когда существует потребность в защите конфиденциальности, целостности и доступности информации, содержащейся в базе данных, на основе дискреционного принципа управления доступом.

Е.2 Среда безопасности объекта оценки

Е.2.1 Предположения безопасности

Для базы данных важно, чтобы формулировка предположений относительно среды безопасности ясно устанавливала возможности и границы ОО.

Например, могут быть сделаны следующие предположения:

Предположение А1. Объект оценки (СУБД) работает под управлением операционной системы, которая установлена и функционирует в безопасном режиме, то есть в соответствии с эксплуатационной документацией данного продукта ИТ.

Предположение А2. Ресурсы ОО и операционной системы, под управлением которой он работает, защищены от несанкционированного физического доступа.

Предположение А3. Все относящиеся к базе данных файлы и каталоги защищены от несанкционированного доступа операционной системой, под управлением которой работает ОО.

Главная задача разработчика ПЗ заключается в том, чтобы определить границы среды безопасности как непосредственно ОО, так и операционной системы, под управлением которой работает ОО. В дальнейшем в ПЗ определяются цели и требования к операционной системе (как части ИТ-среды).

Предположения, относящиеся к особенностям обеспечения безопасности (например, особенности накопления в журнале аудита и анализа информации, обеспечивающей контроль функционирования системы безопасности), могут формулироваться как цели безопасности для среды.

Е.2.2 Угрозы

Для базы данных защищаемые активы — это объекты базы данных (например, собственно данные). Объекты могут входить в состав данных, содержащихся в других объектах. Конфиденциальность, целостность и доступность информации, хранимой в этих объектах, должны быть обеспечены в соответствии с требованиями владельцев объектов.

Субъектами угрозы являются уполномоченные и неуполномоченные пользователи базы данных. Последняя категория включает в себя как уполномоченных, так и неуполномоченных пользователей операционной системы, под управлением которой работает СУБД.

Дополнительными потенциальными источниками угроз целостности и доступности информации, содержащейся в базе данных, являются внешние события, такие как прерывания операций в результате сбоя в работе аппаратных средств, источников питания, носителей данных и т.д.

Две основные угрозы несанкционированного доступа к информации, содержащейся в базе данных, могут быть представлены следующим образом:

Угроза Т1. Нарушитель получает доступ к базе данных в результате маскировки под уполномоченного пользователя или в результате анонимного доступа.

Угроза Т2. Уполномоченный пользователь базы данных обращается к информации, содержащейся в этой базе данных, без разрешения пользователя, являющегося владельцем или ответственным за защиту данных.

В формулировке угроз определены источник угрозы, активы ИТ, подверженные нападению, и форма нападения.

Источник угрозы — это уполномоченный пользователь базы данных в Т2, но мог бы быть и неуполномоченный или уполномоченный пользователь базы данных в Т1.

Активы ИТ, подверженные нападению (в формулировке обеих угроз), — это информация, содержащаяся в объектах базы данных, к которым осуществляется доступ.

Форма нападения выражена в виде маскировки под законного пользователя или «анонимного доступа» в Т1 и «обращается к информации» в Т2.

Угроза доступности информации, содержащейся в СУБД, может быть сформулирована следующим образом.

Угроза Т3. Уполномоченный пользователь базы данных использует общие ресурсы базы данных так, чтобы поставить под угрозу доступность базы данных для других уполномоченных пользователей.

Следует отметить, что в угрозе Т3, как и в угрозах Т1 и Т2, актив ИТ, подверженный риску, — это информация, содержащаяся в базе данных.

«Общие ресурсы базы данных» представляют собой простое средство реализации атаки на доступность информации, содержащейся в базе данных.

Наличие угроз, которым не противостоит ОО, обуславливает необходимость введения ограничений на функционирование СУБД. Рассмотрим пример такой угрозы.

Угроза ТЕ1. База данных не может быть надежно защищена объектом оценки от пользователей с большими полномочиями, которые злоупотребляют предоставленными им привилегиями.

Обычно контрмерой угрозе злоупотребления привилегиями уполномоченным пользователем является аудит безопасности. Но существуют некоторые доверенные пользователи, которые имеют право удалять контрольные записи в журнале аудита и таким образом скрывать свои действия. В связи с этим необходимы соответствующие процедурные меры, обеспечивающие, чтобы пользователи с большими полномочиями являлись действительно заслуживающими доверия личностями. С учетом таких процедурных мер должна быть сформулирована цель безопасности, соответствующая угрозе ТЕ1.

Е.2.3 Политика безопасности организации

В качестве ПБОр для СУБД может быть, например, выбрана:

Политика безопасности Р1. Права доступа к определенным объектам базы данных определяются:

a) владельцем объекта;

b) результатом проверки подлинности субъекта, осуществляющего доступ;

c) правами доступа к объекту, предоставленными субъекту;

d) привилегиями, которыми обладает субъект.

Е.3 Цели безопасности

Е.3.1 Цели безопасности для объекта оценки

С учетом сформулированных угроз цели безопасности для СУБД могут быть определены следующим образом.

Цель О1. Объект оценки должен обеспечивать идентификацию пользователей ОО.

Цель О2. Объект оценки должен обеспечить конечным пользователям возможности управления и ограничения доступа путем определения владельцев объектов БД и ответственных за эти объекты в соответствии с выбранной политикой безопасности Р1.

Цель О3. Объект оценки должен иметь функции управления использованием общих ресурсов пользователями ОО, в том числе — функции ограничения числа параллельных сеансов.

Цель О1 основана на предположении о том, что требуемая проверка подлинности пользователя осуществляется операционной системой, под управлением которой работает ОО и которая является частью ИТ-среды. Необходимость осуществления операционной системой идентификации и аутентификации можно выразить в виде целей безопасности для среды.

Е.3.2 Цели безопасности для среды

Анализ угрозы ТЕ1 показывает необходимость формулировки цели безопасности для среды, связанной с проблемой привилегированных пользователей.

Данную цель безопасности можно сформулировать следующим образом:

Цель ОЕ1. Лица, ответственные за эксплуатацию ОО, должны обеспечить проведение соответствующих процедурных и кадровых мероприятий, гарантирующих то, что только доверенным лицам назначены привилегии, позволяющие им:

a) модифицировать данные журнала аудита и настройки аудита;

b) модифицировать атрибуты безопасности пользователей (включая разрешения на использование привилегий пользователя).

Далее приводится пример цели безопасности для среды, которая (цель) является требованием по использованию операционной системы, под управлением которой работает ОО:

Цель ОЕ2. Лица, ответственные за эксплуатацию ОО, должны обеспечить, чтобы данные аутентификации для каждой учетной записи пользователя операционной системы содержались в тайне и были недоступны лицам, не уполномоченным использовать данную учетную запись.

Цель ОЕ2 определяет потребность (выраженную в предположениях безопасности А1, А2, А3) в том, чтобы файлы базы данных были соответствующим образом защищены операционной системой. Если данные проверки подлинности (учетные записи) не защищены надлежащим образом, то нарушитель сможет обойти функции управления доступом.

Е.4 Требования безопасности информационных технологий

Е.4.1 Функциональные требования безопасности

Можно выбрать следующие функциональные требования безопасности, непосредственно удовлетворяющие описанные выше цели безопасности для ОО:

a) цель О1, требующая идентификации пользователей объектом оценки (аутентификация предписана операционной системе), может быть удовлетворена ФТБ, определенными в компонентах FIA_UIE.1 «Выбор момента времени идентификации» и FIA_USB.1 «Связи пользователь-субъект»;

b) цель безопасности О2, требующая управления доступом к объектам базы данных, может быть удовлетворена ФТБ, определенными в компонентах FDP_ACC.1 «Ограниченное управление доступом» и FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности»;

c) цель безопасности О3, требующая ограничений на использование общих ресурсов, может быть удовлетворена ФТБ, определенными в компонентах FRU_RSA.1 «Максимальные квоты» и FTA_MCS.1 «Базовое ограничение на параллельные сеансы».

Аналогично (путем выбора соответствующих компонентов из ИСО/МЭК 15408-2 для определения требуемых ФТБ) следует удовлетворять и другие цели безопасности, включенные в ПЗ (например, для определения требований аудита следует выбрать компонент FAU_GEN.1 «Генерация данных аудита»).

Сформировав начальный набор ФТБ, оставшиеся ФТБ следует выбирать так, чтобы удовлетворить зависимости, установленные в ИСО/МЭК 15408-2, или определить другие сопутствующие функциональные возможности.

Например:

a) компонент FMT_MSA.3 «Инициализация статичных атрибутов» необходим (как зависимость для компонента FDP_ACF.1) для спецификации функции управления доступа по умолчанию для вновь созданного объекта базы данных;

b) компонент FMT_MSA.1 «Управление атрибутами безопасности» необходим для определения функций контроля за модификацией объектов или назначением атрибутов безопасности пользователей и атрибутов безопасности объектов. Может потребоваться операция итерации для определения контроля за атрибутами пользователей и атрибутами объектов отдельно, так как последние могут быть изменены владельцами объектов, а первые — только администратором;

c) компонент FDP_RIP.1 «Ограниченная защита остаточной информации» нужен, чтобы определить функциональные возможности повторного использования объекта в поддержку политики контроля доступа к базе данных;

d) компонент FAU_SAR.1 «Просмотр аудита» может быть выбран для того, чтобы определить, кто может просматривать данные аудита (например, уполномоченные пользователи могут иметь возможность читать записи аудита, касающиеся объектов, по отношению к которым пользователи являются владельцами, в то время как только уполномоченный администратор может иметь возможность просматривать весь журнал аудита).

Далее необходимо принять решение об уровне аудита событий: минимальный, базовый или детализированный.

Подходящий уровень выбирается, исходя из целей безопасности для ОО. При этом требование аудита не должно быть необоснованно завышено.

Е.4.2 Требования доверия к безопасности объекта оценки

Требования доверия должны быть сформулированы на основе рассмотрения характера (природы) угроз. Для СУБД, предназначенной для хранения и обработки информации определенного уровня ценности, следует использовать требования доверия не ниже соответствующего ОУД.

Е.4.3 Требования безопасности для ИТ-среды

Разработку данного раздела ПЗ для СУБД необходимо вести с учетом функций ОС по обеспечению контроля доступа, идентификации и аутентификации. При этом некоторые требования могут быть определены в результате удовлетворения зависимостей ФТБ ОО. Требования доверия для ОС должны, по меньшей мере, соответствовать ОО, то есть в данном случае быть не ниже выбранного ОУД.

Е.5 Обоснование профиля защиты

Е.5.1 Обоснование целей безопасности

Демонстрация соответствия целей безопасности идентифицированным угрозам может быть выполнена:

a) в виде таблицы, показывающей, какие цели безопасности каким угрозам соответствуют (например, угрозе Т3 соответствует цель О3), при этом необходимо обеспечить соответствие каждой цели безопасности, по крайней мере, одной угрозе;

b) в виде обоснования того, что цели безопасности противостоят угрозам.

Ниже приведен пример обоснования целей безопасности.

Угрозе Т3 (чрезмерное потребление ресурсов) непосредственно противостоит цель О3, которая гарантирует, что ОО имеет функции ограничения использования общих ресурсов, включая установку ограничений на число параллельных сеансов отдельных пользователей.

Е.5.2 Обоснование функциональных требований безопасности

Демонстрацию соответствия ФТБ целям безопасности для ОО можно представить:

a) в виде таблицы, показывающей, какие ФТБ какие цели безопасности удовлетворяют (например, компоненты FRU_RSA.1 и FTP_MCS.1 соответствуют цели безопасности О3), при этом необходимо обеспечить соответствие каждого ФТБ, по крайней мере, одной цели безопасности;

b) в виде обоснования соответствия ФТБ целям безопасности.

Ниже приведен пример обоснования ФТБ.

Достижение цели О3 обеспечивается компонентом FRU_RSA.1, который предусматривает функции контроля использования общих ресурсов отдельными пользователями, и компонентом FTA_MCS.1, который предусматривает функции контроля числа параллельных сеансов пользователя.

Анализ зависимостей компонентов ФТБ также можно представить в виде таблицы.

Демонстрацию взаимной поддержки и внутренней последовательности требований безопасности можно обеспечивать, выделяя и комментируя дополнительные вспомогательные зависимости между идентифицированными ФТБ (включая, где необходимо, требования к операционной системе), не выделенные в анализе зависимостей. Это следует делать, рассматривая для каждого ФТБ, в свою очередь, потенциальную необходимость другого ФТБ с целью предотвращения обхода или вмешательства в работу соответствующих ФБО.

Ниже приведен пример демонстрации взаимной поддержки требований безопасности:

a) компонент FDP_RIP.1 поддерживает компоненты FDP_ACC.1 и FDP_ACF.1, предотвращая обход ФБО, соответствующих данным компонентам, при многократном использовании объектов хранения данных и доступе к этим объектам различных субъектов;

b) компонент FMT_MSA.1 поддерживает компоненты FRU_RSA.1 и FTA_MCS.1, ограничивая возможности уполномоченного администратора изменять квоты пользователей по использованию ресурсов ОО;

c) компонент FAU_STG.1 «Защищенное хранение журнала аудита» поддерживает компонент FAU_GEN.1, защищая целостность журнала аудита.

Е.5.3 Обоснование требований доверия к безопасности

Формирование настоящего подраздела ПЗ не должно вызвать особых трудностей, если ПЗ ссылается на ОУД и в нем отсутствуют другие, более сильные требования доверия к безопасности. В этом случае можно утверждать, что ОУД содержит известный набор взаимно поддерживающих и внутренне непротиворечивых компонентов доверия, для которых все зависимости удовлетворены.

Приложение F
(рекомендуемое)

Рабочий пример: профиль защиты третьей доверенной стороны

F.1 Введение

В настоящем приложении поясняется применение руководства, содержащегося в разделах 7—13, посредством рабочего примера применительно к третьей доверенной стороне (ТДС). Рассматриваемый пример учитывает гибкость набора ФТБ, который зависит от типов сервисов, предоставляемых ТДС, например:

a) ТДС может обеспечивать или не обеспечивать сервисы конфиденциальности;

b) ТДС может предоставлять сервисы генерации ключей или предполагать, что подписчики ТДС выполняют действия по генерации ключей самостоятельно.

Исходя из вышеперечисленного, необходимо определить набор основных и дополнительных сервисов, предоставляемых ТДС.

Основные сервисы представляют собой минимум сервисов, обеспечиваемых ТДС, и относятся к регистрации подписчика, а также к выпуску, распределению, аннулированию и хранению в архиве сертификатов открытых ключей аутентификации.

Дополнительные сервисы ТДС включают в себя генерацию ключей, верификацию (проверку подлинности) сертификатов, управление сертификатами, восстановление ключей и создание резервных копий.

При делении сервисов на основные и дополнительные исходят из того, что подписчики ТДС могут иметь собственные прикладные программы для выполнения таких функций, как генерация ключей, генерация и верификация цифровой подписи и т.д.

Разработка ПЗ ТДС с учетом основных и дополнительных сервисов создает проблему совместимости со стандартами серии ИСО/МЭК 15408, так как последние не позволяют задавать спецификацию необязательных требований безопасности в ПЗ.

Альтернативный подход разработки ПЗ для каждой возможной комбинации услуг ТДС, учитывая множество возможных перестановок, представляется непрактичным.

Разрешение данной проблемы заключается в том, чтобы определить основной набор ФТБ в ПЗ, соответствующий основным сервисам ТДС.

Кроме того, для каждого дополнительного сервиса может быть определен функциональный пакет для идентификации дополнительных ФТБ, необходимых для поддержки этого сервиса.

Сформированный таким образом ПЗ ТДС может быть использован:

a) при разработке задания по безопасности, совместно с одним или более определенным функциональным пакетом в зависимости от услуг, предоставляемых ТДС;

b) как основа для подготовки других ПЗ, с учетом конкретного набора услуг ТДС; такой ПЗ следует формировать на основе комбинации основного набора ФТБ соответственно с одним или более определенным функциональным пакетом. Данный подход приводит к созданию «семейства» ПЗ ТДС.

F.2 Среда безопасности объекта оценки

F.2.1 Предположения безопасности

Для ТДС важно, чтобы формулировка предположений относительно безопасности ясно устанавливала возможности и границы ОО.

Желательно, чтобы прикладные программы подписчика ТДС, используемые для генерации цифровой подписи или для зашифровывания/расшифровывания информации, рассматривались как находящиеся вне рамок ОО.

Исходя из вышеизложенного, целесообразно выделить следующие два предположения.

Предположение А1. ТДС не будет сертифицировать (предоставлять поручительство за) открытый ключ, если не удовлетворяется требование к целостности алгоритма, по которому генерируется пара ключей.

Предположение А2. Подписчики имеют доступные технические средства, посредством которых они могут (при необходимости) генерировать собственные открытые/секретные ключи, генерировать и верифицировать цифровые подписи и верифицировать сертификаты открытых ключей.

Предположение А1 необходимо, так как сертификат, выпущенный ТДС, был бы девальвирован, если отсутствует доверие к выполнению подписчиком соответствующего алгоритма.

Предположение А2 необходимо для полноты предположений безопасности (хотя ТДС может поддерживать это предположение, предоставляя соответствующие дополнительные услуги). Таким образом, предположение А2 заключается в том, что описанные функциональные возможности обеспечиваются прикладными программами подписчика, не включенными в возможности ОО «ТДС».

F.2.2 Угрозы

Для ТДС защищаемые активы ИТ — это сертификаты открытых ключей, сгенерированные или сохраненные (например, архивированные) ТДС вместе с ключами, используемыми или сгенерированными ТДС.

Открытые ключи и сертификаты по своей природе не требуют защиты их конфиденциальности, однако требуют обеспечения их целостности и доступности. С другой стороны, секретные ключи требуют защиты от рас-

крытия. Такими ключами могут быть ключи, используемые ТДС для подписи сертификатов, или ключи подписчика, сгенерированные и сохраненные (для восстановления или создания резервных копий). Эти активы в конечном счете формируются на основе информации, которой обмениваются подписчики, чьи ключи и сертификаты используются для защиты. Сама информация находится вне управления ТДС, но ключи и сертификаты находятся в его пределах.

Менее поддающийся оценке актив — это репутация организации, непосредственно использующей ТДС; этот актив также может быть скомпрометирован реализацией угроз по отношению к ключам и сертификатам.

Источниками угроз могут быть как злоумышленники, так и подписчики ТДС, а также уполномоченные пользователи ОО.

В качестве примера можно привести следующие угрозы, имеющие отношение к основным сервисам ТДС:

Угроза Т1. Секретный ключ аутентификации подписчика раскрыт лицу, которое не имеет права его знать.

В формулировке угрозы определены источник угрозы, активы ИТ, подверженные нападению, и форма нападения.

Источник угрозы — лицо, которое не имеет права знать секретный ключ подписчика ТДС.

Актив ИТ, подверженный нападению, — это секретный ключ подписчика ТДС.

Форма нападения выражена термином «раскрыт», это указывает на то, что имеет место пассивное либо активное нападение (данный аспект следует более подробно изложить в сопровождающем угрозу объяснении).

Угроза Т2. Один (или более) сертификат открытых ключей аутентификации не может быть распространен надлежащим образом или предоставлен уполномоченному подписчику ТДС.

Пример угрозы Т2 касается доступности сертификатов открытых ключей аутентификации.

В формулировке угрозы Т2 активами, подверженными нападению, являются сертификаты открытых ключей аутентификации.

В этом случае необходимо до сопровождающего угрозу объяснения идентифицировать возможные источники угроз (например, отказ самого ОО или маршрута связи подписчика ТДС) и любые формы нападения (например, преднамеренные попытки блокирования обслуживания или, наоборот, отсутствие явного нападения, если источник угрозы — операционная ошибка в ОО).

Приведем примеры угроз, имеющих отношение к дополнительным сервисам ТДС.

Угроза Т3. Один или более секретных ключей подписчика не могут быть распределены или переданы лицу, имеющему на то законное право.

Эта угроза относится к дополнительному сервису, связанному с восстановлением ключей.

Данная угроза может иметь место, если ТДС предоставляются дополнительные сервисы по созданию резервных копий ключей или генерации секретных ключей.

F.2.3 Политика безопасности организации

В качестве ПБОр для ТДС может быть выбрана следующая политика:

Политика безопасности Р1. Требуется, чтобы ТДС соответствовал действующему законодательству и нормативным документам в области информационной безопасности.

F.3 Цели безопасности

F.3.1 Цели безопасности для объекта оценки

Цели безопасности для ТДС делятся на цели безопасности основных и дополнительных сервисов. Цели безопасности для ТДС могут быть определены следующим образом:

Цель О1. Объект оценки должен обеспечить сервисы своевременной генерации, распределения и аннулирования сертификатов открытых ключей.

Цель О2. Объект оценки должен обеспечить сервисы верификации сертификатов открытых ключей, которая включает проверку цепочки сертификатов для доверенного субъекта (объекта).

Цель О3. Объект оценки должен обеспечить сервисы генерации цифровых подписей для подтверждения аутентичности.

Цели безопасности О1 и О2 имеют непосредственное отношение к основным сервисам ТДС, предоставляемым подписчикам ТДС.

Цель безопасности О3 напрямую не относится к основным сервисам ТДС, но, тем не менее, должна быть удовлетворена для поддержки основного сервиса — генерации ключей. То есть ТДС должен быть способен подписывать сертификаты открытых ключей, которые он генерирует.

Другие цели безопасности определяются в целях обеспечения надлежащей защиты активов ТДС. Эти цели относятся к целям «стандартной операционной системы» по идентификации и аутентификации пользователей ТДС, контролю доступа и аудиту событий, относящихся к безопасности.

В дополнение к «основному» набору целей безопасности для ОО определяются цели безопасности дополнительных сервисов, например:

Цель О4. Объект оценки должен иметь сервисы хранения ключевой информации, допускающие расшифрование сообщений от имени подписчика, являющегося владельцем ключа.

Цель безопасности О4 относится к дополнительному сервису по восстановлению ключей.

F.3.2 Цели безопасности для среды

Цели безопасности для среды определяют в случае наличия требований для процедур поддержания целостности функционирования ТДС.

Цель ОЕ1. Лица, ответственные за эксплуатацию ТДС, должны обеспечить использование следующих сервисов проверки процедур:

a) генерации сертификатов (с тем, чтобы гарантировать то, что неправильные данные не помещены в сертификат);

b) верификации сертификата (если необходимо обеспечить информирование подписчиков ТДС о положительном результате верификации сертификата).

Цель ОЕ2. Лица, ответственные за эксплуатацию ТДС, должны обеспечить наличие надлежащих процедур аутентификации подписчиков ТДС и (при необходимости) третьих лиц.

Цель ОЕ1 необходима для предотвращения компрометации ТДС в результате выпуска ненадлежащих (недостоверных) сертификатов.

Цель ОЕ2 необходима для того, чтобы, например, заархивированные секретные ключи (в целях восстановления ключей или создания резервных копий ключей) не были бы раскрыты лицам, которые не имеют на это права.

F.4 Требования безопасности информационных технологий

F.4.1 Функциональные требования безопасности объекта оценки

Первоначально выбирают ФТБ, непосредственно удовлетворяющие целям безопасности для ОО. Например, цель О1 требует, в том числе, возможности генерации сертификатов открытых ключей. Это требование может быть сформулировано на основе элемента FDP_DAU.2.1 компонента FDP_DAU.2 (аутентификация данных с идентификацией гаранта) следующим образом:

ФТБ1. ФБО должны предоставить возможность генерировать сертификаты открытых ключей, которые могут быть использованы как гарантия проверки правильности [увязки определенного имени (идентификационных признаков) с определенным открытым ключом и владением связанным с ним секретным ключом].

Примечание — Сертификаты открытых ключей должны быть сгенерированы в соответствии с определенным стандартом (например, X.509).

Другой элемент в компоненте FDP_DAU.2 — FDP_DAU.2.2 используется для определения требования возможности проверки сертификатов открытых ключей с тем, чтобы удовлетворить цель безопасности О2:

ФТБ2. ФБО должны предоставить [ТДС] возможность верифицировать сертификаты открытых ключей и идентификатор того ТДС, который сгенерировал сертификат.

Примечание — Верификация сертификата должна включать, как минимум:

a) проверку цифровой подписи;

b) проверку срока действия;

c) проверку параметров аннулирования.

Цель безопасности О3 требует возможности генерации цифровых подписей как доказательство происхождения. Это обстоятельство ведет к использованию следующих ФТБ, определенных при помощи компонента FCO_NRO.1 (избирательное доказательство отправления):

ФТБ3. ФБО должны быть способны генерировать цифровые подписи [для передаваемой информации] при запросе [ТДС].

ФТБ4. ФБО должны быть способны связать [идентификационные признаки] отправителя информации и информации, к которой прилагается цифровая подпись.

ФТБ5. ФБО должны предоставить возможность проверки цифровых подписей ТДС при [назначение: ограничения на цифровую подпись].

После того как сформирован начальный набор ФТБ, остальные ФТБ выбирают так, чтобы удовлетворить зависимости или идентифицировать другие (поддерживающие) функциональные возможности. Например, следующее ФТБ, определенное на основе компонента FCS_CKM.1, необходимо для поддержки цели О1 и должно предусматривать генерацию ключей ТДС для подписи сгенерированных сертификатов:

ФТБ6. ФБО должны генерировать пары ключей (открытый/секретный) ТДС в соответствии с определенным алгоритмом [назначение: алгоритм генерации криптографических ключей] и длиной [назначение: длины криптографических ключей], которые отвечают следующему: [назначение: список стандартов].

Так же на основе FCS_COP.1 определено ФТБ7 для поддержки ФТБ3 — ФТБ5 с тем, чтобы определить алгоритмы, используемые для генерации и верификации цифровых подписей:

ФТБ 7. ФБО должны выполнять [генерацию цифровых подписей и их верификацию] в соответствии с определенными алгоритмами [назначение: криптографические алгоритмы] и длиной [назначение: длины криптографических ключей], которые отвечают следующему: [назначение: список стандартов].

Далее необходимо принять решение об уровне аудита событий (минимальный, базовый или детализированный).

Подходящий уровень выбирают, исходя из целей безопасности для ОО. При этом требование аудита не должно быть необоснованно завышено.

Профиль защиты ТДС также включает в себя набор функциональных пакетов, определяющих ФТБ, необходимые для поддержания безопасности дополнительных сервисов ТДС, например:

ФТБ8. ФБО должны выполнять [восстановление ключей] в соответствии с определенным методом доступа [назначение: метод доступа к криптографическим ключам], который [должен обеспечить защиту секретной ключевой информации от несанкционированного раскрытия и модификации в процессе распределения].

ФТБ8 сформулировано на основе элемента FCS_CKM.3.1 компонента FCS_CKM.3 «Доступ к криптографическим ключам» путем выполнения соответствующих операций назначения:

- тип доступа к криптографическим ключам — восстановление ключей;
- список стандартов — должен обеспечить защиту секретной ключевой информации от несанкционированного раскрытия и модификации в процессе распределения.

Элемент FDP_DAU.2.2 в компоненте FDP_DAU.2 «Аутентификация данных с идентификацией гаранта» используется для определения требования возможности проверки сертификатов открытых ключей подписчиками ТДС. При этом имеет место операция итерации, то есть повторное включение в ПЗ компонента FDP_DAU.2 (см. ФТБ1, ФТБ2) с другим выполнением операции назначения.

ФТБ9. ФБО должны предоставить [подписчикам ТДС] возможность верифицировать сертификаты открытых ключей и идентификатор того ТДС, который сгенерировал сертификат.

Примечание — Верификация сертификата должна включать в себя как минимум:

a) проверку цифровой подписи;

b) проверку срока действия;

c) проверку параметров аннулирования сертификата.

Незначительная модификация ФТБ9 может расширить возможности подписчиков ТДС по проверке сертификатов подобно тому, как это выполняется ТДС.

F.4.2 Требования доверия к безопасности объекта оценки

Требования доверия к безопасности ОО должны быть сформулированы на основе анализа характера угроз, ценности активов и технической выполнимости требований доверия. Учитывая то, что ценность защищаемой информации может быть существенной, необходим относительно высокий уровень доверия. Однако с учетом ограничений технической реализуемости можно выбрать уровень доверия ОУД4. В соответствии со стандартами серии ИСО/МЭК 15408 ОУД4 обеспечивает умеренно высокий уровень доверия безопасности проектирования.

F.4.3 Требования безопасности для ИТ-среды

Для ТДС нет требований безопасности для ИТ-среды: все требования безопасности должны быть удовлетворены ОО. Однако считается, что соответствующий ОО должен работать под управлением операционной системы, которая обеспечивает идентификацию и аутентификацию, управление доступом и функциональные возможности аудита, требуемые для защиты активов ТДС, хранимых и обрабатываемых ОО.

F.5 Обоснование профиля защиты

F.5.1 Обоснование целей безопасности

Демонстрация соответствия целей безопасности угрозам может быть выполнена:

a) в виде таблицы, показывающей, какие цели безопасности каким угрозам противостоят (например, угрозе Т2 противостоят цели О1 и О3), при этом необходимо обеспечить соответствие каждой цели безопасности, по крайней мере, одной угрозе;

b) обоснованием того, что цели безопасности противостоят угрозам.

Ниже приведен пример обоснования целей безопасности.

Угрозе Т2 противостоит цель безопасности О1, обеспечивающая сервисы безопасной генерации и распределения сертификатов открытых ключей. Цель О3 обеспечивает возможность генерации цифровых подписей в дополнение к генерации сертификатов.

F.5.2 Обоснование функциональных требований безопасности

Демонстрацию соответствия ФТБ целям безопасности для ОО можно представить:

a) в виде таблицы, показывающей, какие ФТБ каким целям безопасности удовлетворяют (например, ФТБ3—4 и ФТБ7 соответствуют цели безопасности О3), при этом необходимо обеспечить соответствие каждого ФТБ, по крайней мере, одной цели безопасности;

b) в виде обоснования соответствия ФТБ целям безопасности.

Ниже приведен пример обоснования ФТБ.

Цель О3 удовлетворяет ФТБ3—4 и ФТБ7, обеспечивающим функциональные возможности генерации цифровой подписи.

Так как для каждого дополнительного сервиса ТДС имеется соответствующая цель безопасности, необходимо отдельное обоснование для каждого сервиса.

Анализ зависимостей компонентов ФТБ можно представить в виде таблицы.

Демонстрацию взаимной поддержки и внутренней последовательности требований безопасности можно обеспечивать, выделяя и комментируя дополнительные зависимости между идентифицированными ФТБ (включая, где необходимо, требования к операционной системе), не выделенные в анализе зависимостей. При этом следует рассматривать для каждого ФТБ, в свою очередь, потенциальную необходимость другого ФТБ с целью предотвращения обхода или вмешательства в работу соответствующих ФБО.

Ниже приведены примеры демонстрации взаимной поддержки требований безопасности:

a) ФТБ 6 обеспечивает безопасную генерацию ключей ТДС и поэтому поддерживает те ФТБ, которые полагаются на использование этих ключей: ФТБ1, ФТБ2;

b) ФТБ3—4,7 обеспечивают сервис цифровой подписи и поэтому поддерживают те ФТБ, которые полагаются на генерацию цифровых подписей: ФТБ1;

c) ФТБ4—5,7 обеспечивают сервис проверки цифровой подписи и поэтому поддерживают те ФТБ, которые относятся к проверке цифровой подписи: ФТБ2.

F.5.3 Обоснование требований доверия к безопасности

Формирование настоящего подраздела ПЗ не должно вызвать особых трудностей, если ПЗ ссылается на ОУД4 и в нем отсутствуют иные требования доверия к безопасности. Оценочный уровень доверия ОУД4 содержит известный набор взаимно поддерживающих и внутренне непротиворечивых компонентов доверия, для которых все зависимости между компонентами удовлетворены.

Приложение G
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица G.1

Обозначение ссылочного международного стандарта	Обозначение и наименования соответствующего национального стандарта
ИСО/МЭК 15408-1:1999	ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ИСО/МЭК 15408-2:1999	ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ИСО/МЭК 15408-3:1999	ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
ИСО 2382-8:1998 Информационные технологии — Словарь — Часть 8: Безопасность	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать русскую версию или аутентичный перевод на русский язык данного международного стандарта. Переводы международных стандартов (при их наличии) находятся в Федеральном информационном фонде технических регламентов и стандартов.

Библиография

[1] ИСО/МЭК 15292:2001 (ISO/IEC 15292:2001) Информационная технология. Методы и средства обеспечения безопасности. Процедуры регистрации профилей защиты (Protection Profile registration procedures)

[2] ИСО/МЭК 13335:2004 (ISO/IEC 13335:2004) Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной и телекоммуникационной безопасности (Information technology — Security Techniques — Management of information and communications technology security)

[3] ИСО/МЭК 14516:2002 (ISO/IEC 14516:2002) Информационная технология. Методы и средства обеспечения безопасности. Рекомендации по использованию услуг доверенных третьих сторон и управлению ими (Information technology — Security Techniques — Guidelines on the use and management of Trusted Third Parties services)

[4] ИСО/МЭК 9798-1:1997 (ISO/IEC 14516:1997) Информационная технология. Методы и средства обеспечения безопасности. Аутентификация логического объекта. Часть 1. Общие положения (Information technology — Security Techniques — Entity authentication — Part 1: General)

[5] ИСО/МЭК 10118-1:1994 (ISO/IEC 10118-1:1994) Информационная технология. Методы и средства обеспечения безопасности. Хэш-функции. Часть 1. Общие положения (Information technology — Security Techniques — Hash functions — Part 1: General)

[6] ИСО/МЭК 11770-1:1996 (ISO/IEC 11770-1:1996) Информационная технология. Методы и средства обеспечения безопасности. Распределение ключей. Часть 1. Основные положения (Information technology — Security Techniques — Key management — Part 1: Framework)

[7] ИСО/МЭК 13888-1:1997 (ISO/IEC 13888-1:1997) Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость. Часть 1. Общие положения (Information technology — Security Techniques — Non-repudiation — Part 1: General)

[8] ИСО/МЭК 14888-1:1998 (ISO/IEC 14888-1:1998) Информационная технология. Методы и средства обеспечения безопасности. Электронная цифровая подпись с приложением. Часть 1. Общие положения (Information technology — Security Techniques — Digital signature with appendix — Part 1: General)

[9] ИСО/МЭК 18031:2005 (ISO/IEC 18031:2005) Информационная технология. Методы и средства обеспечения безопасности. Генерация случайных чисел (Information technology — Security Techniques — Random number generation)

[10] ИСО/МЭК 18032:2005 (ISO/IEC 18032:2005) Информационная технология. Методы и средства обеспечения безопасности. Генерация простых чисел (Information technology — Security Techniques — Prime number generation)

УДК 351.864.1:004:006.354 ОКС 35.040 Т00

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

Редактор *В. Н. Колысов*
Технический редактор *В. Н. Прусакова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 06.11.2009. Подписано в печать 25.02.2010. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 12,09. Уч.-изд. л. 12,70. Тираж 223 экз. Зак. 2294

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256