Руководящий документ
Руководство по разработке профилей защиты и заданий по безопасности

Гостехкомиссия России, 2003 год

1. Область применения

Настоящий документ (далее – Руководство) представляет собой руководство по разработке профилей защиты и заданий по безопасности продуктов и систем (изделий) ИТ в соответствии с Руководящим документом Гостехкомиссии России «Критерии оценки безопасности информационных технологий», далее по тексту – ОК.

Руководство предназначено для разработчиков и оценщиков ПЗ и ЗБ, а также может представлять интерес для пользователей ПЗ и ЗБ, позволяя им понять, чем руководствовались авторы ПЗ и/или ЗБ при их разработке, и на какие части ПЗ и/или ЗБ следует обратить особое внимание.

2. Нормативные ссылки

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 1: Введение и общая модель, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.

Руководящий документ – Безопасность информационных технологий – Критерии оценки безопасности информационных технологий – Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

3. Термины и определения

3.1 **Активы**: Информация или ресурсы, подлежащие защите с применением изделия ИТ

3.2 **Доверие**: Основание для уверенности в том, что изделие ИТ отвечает своим целям безопасности

3.3 **Задание по безопасности**: Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки безопасности конкретного изделия ИТ

3.4 **Изделие ИТ**: Обобщенный термин для продуктов и систем ИТ

3.5 **Информационная технология:** Приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации

3.6 **Объект оценки:** Подлежащие оценке продукт или система ИТ с руководствами администратора и пользователя (данный термин используется в ПЗ/ЗБ для обозначения соответствующего изделия ИТ)

3.7 **Пакет доверия:** Предназначенная для многократного использования совокупность компонентов доверия для удовлетворения совокупности определенных целей безопасности. Примером ПД является оценочный уровень доверия

3.8 **Политика безопасности организации:** Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности

3.9 **Предположения:** Условия, которые должны быть обеспечены в среде, чтобы изделие ИТ могло рассматриваться как безопасное.Условия, которые должны быть обеспечены в среде, при которых может рассматриваться как безопасное.

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

3.11 **Профиль защиты** (protection profile): Независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя

3.12 **Система ИТ:** Специфическое воплощение изделия ИТ с конкретным назначением и условиями эксплуатации

3.13 **Среда безопасности:** Область среды, в пределах которой предусматривается обеспечение необходимых условий для поддержания требуемого режима безопасности изделия ИТ

3.14 **Угроза:** Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу

3.15 **Функциональный пакет:** Предназначенная для многократного использования совокупность функциональных компонентов, объединенных для удовлетворения совокупности определенных целей безопасности

3.16 **Функция безопасности:** Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности

3.17 **Цель безопасности:** Сформулированное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям

4. Сокращения

ЗБ – задание по безопасности

ИТ – информационная технология

ИФБО – интерфейс ФБО

ОДФ – область действия ФБО

ОК – Общие критерии

ОО – объект оценки

ОУД – оценочный уровень доверия

ПБО – политика безопасности ОО

ПЗ – профиль защиты

ПФБ – политика функции безопасности

СФБ – стойкость функции безопасности

ФБ – функция безопасности

ФБО – функции безопасности ОО

ПБОр – политика безопасности организации;

СУБД – система управления базами данных;

ТДБ – требование доверия к безопасности;

ФТБ – функциональное требование безопасности.

5. Общие положения

5.1 Введение в профили защиты и задания по безопасности

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

Профиль защиты включает взаимосвязанную информацию, имеющую отношение к безопасности ИТ, в том числе:
- формулировку потребности в безопасности, соответствующую проблеме безопасности и выраженную в терминах, ориентированных на пользователей изделий ИТ;
- описание среды ОО, уточняющее формулировку потребности в безопасности с учетом порождаемых средой угроз, которым нужно противостоять, политики безопасности, которая должна выполняться, и сделанных предположений;
- 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;
- функциональные требования безопасности и требования доверия к безопасности, которые направлены 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;
- обоснование, показывающее, что функциональные требования и требования доверия к безопасности являются надлежащими для удовлетворения сформулированной потребности в безопасности. Посредством целей безопасности должно быть показано, что необходимо сделать в плане решения проблем безопасности, имеющихся в описании среды безопасности ОО. Функциональные требования безопасности и требования доверия к безопасности должны удовлетворять целям безопасности.

Задание по безопасности во многом похоже на ПЗ, но содержит дополнительную информацию, ориентированную на конкретную реализацию изделия ИТ и разъясняющую, каким образом требования ПЗ реализуются в конкретном продукте или системе. ЗБ содержит следующую дополнительную информацию, отсутствующую в ПЗ:
- краткую спецификацию ОО, которая представляет функции безопасности и меры доверия к безопасности для конкретного ОО;
- дополнительный раздел, который включается в ЗБ в тех случаях, когда утверждается о соответствии ЗБ одному или более ПЗ;
- дополнительные свидетельства в разделе «Обоснование», устанавливающие, что краткая спецификация ОО обеспечивает удовлетворение требований безопасности, а любые утверждения о соответствия ПЗ действительны.

Использование ПЗ и ЗБ. Профиль защиты может использоваться для определения типового набора требований безопасности, которым должны удовлетворять один или более продуктов или которым должны удовлетворять 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). Разработчики изделий ИТ в соответствии с потребностями безопасности, сформулированными в ПЗ, могут разработать ЗБ, которое будет демонстрировать то, как их изделие ИТ удовлетворяет 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 данными сторонами. Оценка конкретной системы ИТ на соответствие ЗБ, которое в свою очередь соответствует ПЗ, может являться частью процесса приемки системы ИТ.

5.2 Краткий обзор руководства

Рассматриваемый документ представляет собой детальное руководство по разработке различных частей ПЗ или ЗБ и дает исчерпывающее представление об их взаимосвязи. Наиболее важные аспекты Руководства представлены в Приложении 1 в виде памятки (или резюме), что в значительной степени облегчает знакомство и работу с документом.

В остальных приложениях приводятся примеры, иллюстрирующие применение Руководства.

Глава 5 посвящена целям и направленности Руководства.

Глава 6 содержит краткий обзор ПЗ и ЗБ, который включает примерные оглавления и отображает предполагаемое содержание, а также потенциальных пользователей различных частей ПЗ или ЗБ. В этой главе также комментируется соотношение между ПЗ и ЗБ и проблемы, связанные с процессом их разработки.

В главе 7 более глубоко рассматриваются описательные 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).

Следующие пять глав придерживаются той структуры ПЗ и ЗБ, которая установлена в ОК.

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

Глава 9 представляет собой руководство по определению и спецификации целей безопасности в ПЗ или ЗБ в соответствии со сформулированными ранее исходными «потребностями в безопасности». Обе эти главы представляют интерес не только для авторов ПЗ и ЗБ, но также и для других лиц – пользователей ПЗ и ЗБ.

Глава 10 представляет собой руководство по выбору и спецификации требований безопасности информационных технологий в ПЗ. В этой главе достаточно подробно описывается использование функциональных компонентов и компонентов доверия к безопасности в соответствии с ОК, а также компонентов, не предусмотренных ОК, для обеспечения более точного определения требований безопасности ИТ.

Глава 11 представляет собой руководство по разработке ЗБ в части спецификации требований безопасности ИТ (отличающейся от ПЗ) и краткой

спецификации ОО. Таким образом, главы 10 и 11 будут главным образом интересны авторам и оценщикам ПЗ/ЗБ.

Главы 12 и 13 представляют собой руководство по составлению и представлению разделов «Обоснование» в ПЗ и ЗБ. В главе 12 описывается формирование раздела ПЗ «Обоснование», а в главе 13 рассматриваются те аспекты раздела «Обоснование» в ЗБ, которые отличаются от раздела «Обоснование» в ПЗ.

Эти материалы также будут в первую очередь интересны авторам ПЗ и/или ЗБ и их оценщикам.

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

Глава 15 представляет собой руководство по формированию функциональных пакетов и пакетов доверия к безопасности, причем таким образом, чтобы их 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/или ЗБ.

Как упоминалось выше, Приложение 1 резюмирует руководство в виде памятки.

Приложение 2 представляет примеры угроз, политики безопасности организации, предположений и целей безопасности, а также устанавливает соответствие между общими функциональными требованиями и соответствующими функциональными компонентами из части 2 ОК. Предполагается, что эти примеры достаточно широкомасштабны, но никоим образом не исчерпывающи.

В Приложениях 2 и 3 иллюстрируются возможности применения Руководства при разработке ПЗ и ЗБ для различных типов ОО. Так, в Приложении 2 рассмотрена возможность использования Руководства при разработке ПЗ и/или ЗБ для межсетевых экранов, в Приложении 3 – для СУБД, в котором подчеркивается особая важность решения вопросов, связанных со ИТ-средой.

6. Краткий обзор профилей защиты и заданий безопасности

В данной главе приводится краткий обзор и содержание ПЗ и ЗБ. Рассматриваются взаимосвязи между ПЗ и ЗБ и процесс их разработки (см. также Приложения Б и В части 1 ОК).

6.1 Профиль защиты

Требуемое содержание ПЗ приведено в Приложении Б части 1 ОК. Пример оглавления ПЗ представлен в таблице 1.

Таблица 1

Пример оглавления профиля защиты
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. Логическое обоснование целей безопасности
7.2. Логическое обоснование требований безопасности

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

В раздел «Описание ОО» включается сопроводительная информация об ОО (или типе ОО), предназначенная для пояснения его назначения и требований безопасности.

В раздел ПЗ «Среда безопасности ОО» включается 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 политики безопасности организации (ПБОр), которой должен удовлетворять ОО. Этот раздел ПЗ более подробно рассмотрен в главе 8 настоящего Руководства.

В раздел ПЗ «Цели безопасности» включается 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 главе 9 настоящего руководства.

В раздел ПЗ «Требования безопасности ИТ» включаются 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 из частей 2 и 3 ОК. Раздел ПЗ «Требования безопасности ИТ» более подробно рассмотрен в главе 10 настоящего Руководства.

В раздел ПЗ «Замечания по применению ПЗ» может включаться любая дополнительная информация, 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 главе 7 настоящего руководства.

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

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. Практически, дополнительные разделы могут быть необходимы для предоставления полезной информации, например:
а) раздел «Введение ПЗ» может включать подраздел, описывающий организацию ПЗ, а также содержать ссылки на другие ПЗ и другие документы;
б) раздел «Среда безопасности ОО» может включать отдельные подразделы для различных доменов в ИТ-среде для ОО;

в) 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.

6.2 Задание по безопасности

Требуемое содержание ЗБ дано в Приложении В части 1 ОК. Пример оглавления ЗБ представлен в таблице 2.

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

В раздел ЗБ «Описание ОО» включается сопроводительная информация об ОО, предназначенная для пояснения его назначения и требований безопасности. Раздел ЗБ «Описание ОО» должен также включать описание конфигурации, в которой ОО подлежит оценке. Раздел ЗБ «Описание ОО» более подробно рассмотрен в главе 7 настоящего Руководства.

В раздел ЗБ «Среда безопасности ОО» включается 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 удовлетворять ОО. Раздел ЗБ «Среда безопасности ОО» более подробно рассмотрен в главе 8 настоящего Руководства.

Таблица 2

Пример оглавления задания по безопасности
1. Введение ЗБ
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. Логическое обоснование целей безопасности
8.2. Логическое обоснование требований безопасности
8.3. Логическое обоснование краткой спецификации ОО
8.4. Логическое обоснование утверждений о соответствии ПЗ

В раздел ЗБ «Цели безопасности» включается 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 ЗБ более подробно рассмотрен в главе 9 настоящего Руководства.

В раздел ЗБ «Требования безопасности ИТ» включаются 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 частей 2 и 3 ОК. Раздел ЗБ «Требования безопасности ИТ» более подробно рассмотрен в главе 10 настоящего Руководства.

В раздел «Краткая спецификация ОО» включается 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 главе 11 настоящего Руководства.

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 главе 13 настоящего Руководства.

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

Как и в случае ПЗ (см. п. 6.1), при разработке ЗБ можно 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 содержания таблиц 1 и 2 очевидна 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, чтобы ЗБ ссылалось на содержание ПЗ с добавлением, где необходимо, деталей, отличающих ЗБ от ПЗ.

Следующие разделы ЗБ не имеют аналогов в ПЗ и, таким образом, являются специфичными для ЗБ:
а) раздел «Краткая спецификация ОО» включает функции безопасности ИТ, механизмы и способы обеспечения безопасности, а также меры доверия к безопасности;
б) раздел «Утверждения о соответствии ПЗ» мотивирует и детализирует требования соответствия ПЗ;
в) подразделы раздела «Обоснование», которые 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 информационные потребности потенциальных пользователей этих документов:
- потребители изделий ИТ (дистрибуторы и покупатели) нуждаются в информации, дающей общее представление о том, каким образом 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 техническую правильность и эффективность ПЗ или ЗБ.

Структура ПЗ и ЗБ разработана таким образом, чтобы разные разделы содержали информацию, предназначенную для разных категорий пользователей.

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

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

В раздел «Обоснование» включается информация, предназначенная преимущественно для оценщиков. В то же время оценщикам целесообразно ознакомиться со всеми разделами ПЗ и ЗБ.

6.5 Процесс разработки ПЗ и ЗБ

Анализ приложений Б и В части 1 и глав 3 – 5 части 3 ОК показывает, что разработка ПЗ/ЗБ осуществляется в следующей (нисходящей) последовательности:
- идентификация аспектов среды безопасности;
- определение целей безопасности, учитывающих идентифицированные аспекты среды безопасности;

- формирование требований безопасности ИТ, направленных на удовлетворение целей безопасности.

В общем случае, хотя и с учетом данной последовательности действий, процесс разработки ПЗ/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/ЗБ. При этом только когда все проблемы формирования «Обоснования» ПЗ/ЗБ решены, процесс разработки ПЗ/ЗБ можно считать завершенным.

Процесс разработки ПЗ/ЗБ может также включать внесение изменений в документ с тем, чтобы отразить изменения условий применения, например:
- идентификацию новых угроз;
- изменение ПБОр;
- связанные со стоимостными и временными ограничениями изменения в разделении ответственности обеспечения безопасности, возлагаемой соответственно на ОО и среду ОО;
- 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/ЗБ имеют четкое представление относительно ФТБ, которым удовлетворяет ОО (даже если эти требования не были выражены в стиле ОК). В таких случаях определение аспектов среды безопасности и целей безопасности будет осуществляться, исходя из этих ФТБ. Процесс разработки ПЗ/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:
- 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 все требования безопасности ИТ, специфицированные в последнем);

- разработка совокупности ПЗ, каждый из которых относится к различным компонентам системы ИТ, например, семейство «смарт-карты» могло бы включать 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 главу 14 настоящего Руководства, в которой рассматриваются вопросы разработки ПЗ для компонентов системы ИТ).

7. Описательные разделы профилей защиты и заданий по безопасности

Настоящая глава содержит рекомендации по формированию следующих описательных разделов ПЗ и ЗБ:
а) «Введение ПЗ/ЗБ»;
б) «Описание ОО» в ПЗ/ЗБ;
в) «Замечания по применению» в ПЗ.

7.1 Описательные части профиля защиты

7.1.1 Раздел «Введение ПЗ»

Подраздел «Идентификация ПЗ»

Назначение данного подраздела состоит в предоставлении информации для идентификации ПЗ, например, в целях последующей регистрации ПЗ. Идентификация, как минимум, должна включать название ПЗ и идентификатор, который является уникальным для данной версии ПЗ. В подраздел «Идентификация ПЗ» также целесообразно включить следующую информацию:
а) ключевые слова;
б) оценочный уровень доверия (ОУД), если он применяется в ПЗ;

в) утверждение о соответствии версии ОК;
г) состояние оценки ПЗ.

Аннотация ПЗ

Согласно ОК подраздел «Аннотация ПЗ» должен иметь форму 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, каким образом ПЗ способствует решению проблемы безопасности. При этом необходимо обеспечить соответствие 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 таким образом, чтобы его можно было перенести в реестр.

Профили защиты, с которыми связан рассматриваемый профиль, и другие документы, на которые ссылается (необязательный подраздел)

Если ПЗ связан (или такая связь предполагается) с одним или несколькими другими ПЗ, рекомендуется, чтобы эти профили были идентифицированы в разделе «Введение ПЗ». При этом для пользователя ПЗ представляет особый интерес характер данной связи. При наличии тесной связи оцениваемого ПЗ с существующим оцененным ПЗ результаты оценки последнего могут быть использованы для оценки рассматриваемого ПЗ. Таким образом, основные усилия при оценке ПЗ необходимо будет сконцентрировать на отличиях двух ПЗ.

Необходимо отметить, что в данный подраздел включается информация, которая представляет интерес для пользователя ПЗ и уже известна разработчику ПЗ. При этом от разработчика ПЗ никакой более подробной информации о существующих ПЗ не требуется.

Профиль защиты для большой распределенной системы может ссылаться на ряд других документов (предварительное изучение угроз; документы, содержащие высокоуровневое описание ОО; документы, содержащие описание различных компонентов ИТ-среды). Такие документы могут разрабатываться различными организациями в разное время и противоречить друг другу в терминологии, концепции, в описании среды и целей безопасности. В таких случаях в ПЗ необходимо пояснить, что именно взято из документов, на которые ссылается ПЗ.

Структура и организация профиля защиты (необязательный подраздел)

Данный подраздел предназначен для объяснения структуры и организации ПЗ пользователям, не знакомым с типовой структурой ПЗ. Ниже приведен шаблон рассматриваемого подраздела (текст, зависящий от структуры и содержания ПЗ/ЗБ, обрамлен квадратными скобками и выделен курсивом).

Профиль защиты включает следующие основные разделы: «Описание ОО», «Среда безопасности ОО», «Требования безопасности ИТ» и «Обоснование». *[Если в ПЗ включаются требования безопасности для не-ИТ-среды, то целесообразно раздел ПЗ «Требования безопасности ИТ» озаглавить – «Требования безопасности».]*

В раздел ПЗ «Описание ОО» включается общая информация об ОО, предназначенная для пояснения требований безопасности, предъявляемых к ОО, и необходимая для оценки ПЗ.

В раздел «Среда безопасности ОО» включается описание аспектов среды безопасности, в которой предполагается использование ОО, а также способ использования ОО. *[Если в среде ОО выделены несколько отдельных доменов, целесообразно дополнительно включить в ПЗ следующий текст: «Аспекты среды безопасности рассматриваются отдельно для каждого домена среды безопасности ОО».]* Раздел «Среда безопасности ОО» содержит описание:
а) предположений о предназначении ОО и о его среде эксплуатации;
б) угроз безопасному функционированию ОО;
в) ПБОр, которой должен удовлетворять ОО.

[При необходимости пункты б) и/или в) можно опустить]

Цели безопасности отражают сформулированное предназначение ПЗ. Они раскрывают, каким образом ОО должен противостоять идентифицированным угрозам и учитывать предположения и ПБОр. Цели безопасности делятся на цели безопасности для ОО и цели безопасности для среды *[иногда целесообразно дополнительно включить в ПЗ следующий текст: одна и та же цель безопасности может быть классифицирована как цель безопасности и для ОО, и для среды]*. *[Первое предложение, связанное с требованиями безопасности, может быть выбрано разработчиками из следующего списка, исходя из того, какие требования включаются в ПЗ/ЗБ:*

1. «Все требования безопасности в настоящем ПЗ имеют отношение к самому ОО» (если задаются требования безопасности только для ОО).

2. «Раздел «Требования безопасности ИТ» содержит в отдельных подразделах требования для ОО и требования для среды ОО» (если задаются требования безопасности для ОО и для среды ОО).

3. «Раздел «Требования безопасности» содержит в отдельных подразделах требования для ОО и требования для среды ОО» (если среда включает не-ИТ-среду)].

Требования безопасности ИТ делятся на: (а) функциональные требования безопасности ОО [если в состав требований доверия к безопасности включен компонент AVA_SOF.1, то необходимо включить следующий текст: «включая требования к стойкости функций безопасности ОО, реализуемым вероятностными или перестановочными механизмами»] и (б) требования доверия к безопасности.

Раздел «Обоснование» содержит свидетельство того, что ПЗ представляет собой полный набор взаимосвязанных требований безопасности ИТ, и что соответствующий данному ПЗ объект оценки надлежащим образом учитывает все аспекты среды безопасности.

Раздел «Обоснование» состоит из двух основных частей. Первая – «Логическое обоснование целей безопасности» – демонстрирует, что цели безопасности надлежащим образом учитывают все аспекты среды безопасности ОО. Вторая – «Логическое обоснование требований безопасности» – демонстрирует, что требования безопасности надлежащим образом учитывают все цели безопасности.

7.1.2 Раздел «Описание ОО»

В раздел «Описание ОО» включается информация следующих видов (первые два вида информации – предписаны ОК, два последних – являются необязательными):
а) тип продукта ИТ;
б) основные функциональные возможности ОО;
в) границы ОО (необязательная информация);
г) среда функционирования ОО (необязательная информация).

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

Описание «границ ОО» (необязательное) – это описание того, что включает и что не включает в себя ОО. При этом ПЗ может оставлять

некоторую 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 максимально стремиться к тому, чтобы исключить возможность неправильного понимания пользователями ПЗ/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).

7.1.3 Раздел «Замечания по применению»

Раздел ПЗ «Замечания по применению» является необязательным. Замечания по применению могут быть либо оформлены отдельным разделом 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 «замечаний по применению» – пояснить, каким образом 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» разнесены по тексту ПЗ, то в этих случаях необходимо их однозначно идентифицировать. Это нужно для того, чтобы пользователь ПЗ интерпретировал их именно как «замечания по применению», а не как, например, уточнения для ФТБ и ТДБ.

7.2 Описательные части задания по безопасности

7.2.1 Раздел «Введение ЗБ»

При формировании раздела «Введение ЗБ» целесообразно руководствоваться рекомендациями по формированию раздела «Введение ПЗ» (см. п. 7.1), за исключением следующего:
а) утверждение о соответствии ОК является необязательным для ЗБ;

б) к ЗБ неприменимы процедуры регистрации ПЗ;
в) может потребоваться идентификация ЗБ, связанных с рассматриваемым ЗБ, если ОО представляет собой составной ОО, либо является частью составного ОО.

7.2.2 Раздел «Описание ОО»

При формировании раздела «Описание ОО» целесообразно руководствоваться рекомендациями по формированию раздела «Введение ПЗ» (см. п. 7.1), 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.

8. Среда безопасности ОО

В данной главе представлены рекомендации по спецификации раздела ПЗ/ЗБ «Среда безопасности ОО». Требования к содержанию этого раздела ПЗ/ЗБ определены в п. Б.2.4 и п. В.2.4 части 1 ОК.

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

Цель раздела «Среда безопасности ОО» состоит в том, чтобы определить аспекты безопасности среды ОО (см. рисунок 1).

Рисунок 1–Определение аспектов среды безопасности ОО

Поэтому в данном разделе предметом рассмотрения становятся следующие аспекты:
а) предположения относительно среды безопасности ОО;
б) 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;
в) ПБОр или правила, которым должен соответствовать ОО.

Последующие 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 это возможно, описания того, каким образом ОО учитывает аспекты безопасности среды. Такой подход позволяет акцентировать внимание пользователя ПЗ/ЗБ на наиболее важных аспектах безопасности среды ОО.

8.1 Идентификация и спецификация предположений безопасности

В соответствии с ОК в раздел «Среда безопасности ОО» ПЗ/ЗБ необходимо включать перечень предположений относительно среды безопасности ОО или предполагаемого использования ОО.

Для формирования такого перечня необходимо определиться с характером предположений относительно среды безопасности ОО и ее границами. Например, может потребоваться формулирование предположений, связанных с тем, что потенциальные угрозы практически не оказывают влияния на безопасность активов среды ОО.

В ПЗ/ЗБ целесообразно включать следующие группы предположений:
а) предположения относительно предопределенного использования ОО;
б) предположения, связанные с защитой любой части ОО со стороны среды (например, физическая защита);
в) предположения связности (например, межсетевой экран должен быть единственным сетевым соединением между частной (защищаемой) и внешней (потенциально враждебной) сетью);
г) предположения, имеющие отношение к персоналу (например, предполагаемые пользовательские роли, основные обязанности (ответственность) пользователей и степень доверия этим пользователям).

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

Чаще всего невозможно полностью идентифицировать все предположения с первого раза. Поэтому предположения могут быть дополнительно идентифицированы на протяжении всего периода разработки ПЗ или ЗБ. В частности, при формировании раздела ПЗ/ЗБ «Обоснование» (например, при

демонстрации пригодности целей безопасности для противостояния идентифицированным угрозам) необходимо установить, были ли сделаны предположения, не нашедшие своего отображения в ПЗ/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/ЗБ в виде требований безопасности для не-ИТ-среды (смотри п.10.5.2).

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

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

Примеры предположений даны в Приложении 3 настоящего Руководства.

8.2 Идентификация и спецификация угроз

Согласно п. Б.2.4 части 1 ОК необходимо в ПЗ/ЗБ включать описание всех угроз активам, подлежащим 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 все же рекомендуется, чтобы формулировка угроз была включена в ПЗ/ЗБ, поскольку она обеспечивает лучшее понимание аспектов среды безопасности ОО, чем соответствующая 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, в результате чего активы организации могут остаться подверженными соответствующему риску. Следует отметить, что подробные рекомендации по организации процесса идентификации угроз активам (являющегося одним из самых трудоемких этапов анализа риска организации) в настоящее Руководство не включены. Тем не менее, далее излагаются общие принципы идентификации угроз.

8.2.1 Идентификация угроз

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 следующие вопросы:
а) какие активы требуют защиты;
б) кто или что является источником угрозы;
в) от каких методов нападения или нежелательных событий активы должны быть защищены.

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 стремиться, вопреки желаниям и интересам владельцев активов, скомпрометировать их, например, путем нарушения конфиденциальности, целостности и доступности данных активов.

Активы, которые надлежит учесть разработчику ПЗ/ЗБ, могут быть представлены в виде первичных активов организации (например, денежные активы, персонал и репутация организации). Под владельцем активов понимаются 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/ЗБ целесообразно при описании активов идентифицировать владельцев первичных активов.

В примере ПЗ для доверенного центра (ДЦ) инфраструктуры открытых ключей (см. Приложение 5) различные криптографические ключи будут иметь разных владельцев: подписчиков доверенного центра и владельца самого ДЦ. Другой пример – медицинские системы ИТ. Хранимая и обрабатываемая в них информация не имеет какого-либо одного владельца, а предназначена для использования всеми заинтересованными сторонами в соответствии с заданным набором правил ее использования и контроля такого использования.

Активы обычно включают 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/ЗБ идентифицировать как «активы» информацию и ресурсы, которые связаны с представлением самого ОО, и которые только косвенно связаны с первичными активами. Такая детализация может привести к:
а) нечеткому пониманию основного предназначения ОО (обеспечение защиты первичных активов или их представлений в пределах ИТ-среды);
б) слишком раннему (еще до описания угроз и целей безопасности) ознакомлению пользователя ПЗ/ЗБ с деталями реализации.

Идентификация источников угроз

Источником угроз могут быть люди либо иные факторы. При этом основное внимание обычно уделяется тем угрозам, которые связанны со злонамеренной или другой деятельностью человека.

При идентификации источников угроз необходимо рассмотреть следующие аспекты:
а) кто может быть по каким-либо причинам заинтересован в компрометации идентифицированных активов;
б) 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;

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

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.

Идентификация методов нападения

Следующим шагом 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:
а) потенциальные уязвимости активов, которые могут быть использованы источниками угроз;
б) возможности нарушителей, имеющих доступ к среде безопасности ОО.

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

Влияние результатов анализа рисков на идентификацию угроз

Проведение анализа рисков целесообразно на этапе идентификации угроз. Соответствующие методы в настоящем Руководстве не рассматриваются. Процесс анализа рисков также необходим и на этапе идентификации целей безопасности для ОО и его среды (см. главу 8), и требуемого уровня доверия к контрмерах, направленных на противостояние возможным угрозам (см. главу 9). Методы анализа риска должны учитывать следующие аспекты:
а) вероятность и последствия компрометации активов с учетом:
- возможности реализации идентифицированных методов нападения;
- вероятности успешной реализации нападения;
- возможного ущерба (включая величину материального ущерба, явившегося результатом успешного нападения);

б) другие ограничения, например, правовые нормы и стоимость.

8.2.2 Спецификация угроз

Следующим шагом после идентификации угроз, которые должен учитывать ОО и его среда, является спецификация данных угроз в ПЗ/ЗБ. Как отмечалось выше, раздел «Среда безопасности ОО» должен иметь четкую и краткую формулировку аспектов среды безопасности ОО и, в частности, – краткую и четкую спецификацию угроз.

Чтобы обеспечить четкую спецификацию угроз, необходимо учесть следующие аспекты (идентифицированные в соответствии с п.8.2.1):
а) источники угроз (например, уполномоченный пользователь ОО);
б) активы, подверженные нападению (например, конфиденциальные данные);
в) используемый метод нападения (например, маскировка под уполномоченного пользователя ОО).

Далее приводятся 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/ЗБ сущности угрозы. Так, в примерах угроз, изложенных выше, целесообразно дать пояснение, 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 перекрытие описаний угроз. Это поможет избежать потенциальных недоразумений при использовании ПЗ/ЗБ, а также ненужных повторений, обеспечив тем самым более простое обоснование ПЗ/ЗБ.

Перекрытия формулировок при описании 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 данный 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). Маркировка угроз может осуществляться одним из перечисленных ниже способов:
а) последовательная нумерация угроз (например, У1, У2, У3 и т.д.);
б) присвоение уникальной метки, обеспечивающей краткое, но значащее «имя» (см. примеры в Приложении 3).

Преимущество второго подхода перед первым заключается в том, что уникальная метка является более информативной, так как несет в себе более значимую информацию, чем просто число. Неудобство этого подхода заключается в том, что не всегда удается назначить метку с однозначным смыслом (из-за практических ограничений, связанных с ограничением числа символов в метке); так, в некоторых случаях метка может ввести в заблуждение или ей можно дать различное толкование.

Описание угроз должно затрагивать только те потенциальные события, которые непосредственно могут привести к компрометации активов, требующих защиты. Поэтому не рекомендуется включать угрозы, например, следующего вида: «В ОО могут существовать недостатки обеспечения безопасности ОО». Такая формулировка угрозы не способствует пониманию пользователем ПЗ/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/ЗБ такого рода угроз необходимо стремиться к тому, чтобы:
а) в результате их включения в раздел «Среда безопасности ОО» преждевременно не рассматривались детали реализации ОО, нарушающие системный подход к решению проблем безопасности;
б) 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 ОК) в свою очередь предъявляются требования взаимной поддержки, существует необходимость рассмотрения атак (таких как 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 представлены в Приложении 2 данного руководства.

8.2.3 Окончательное формулирование угроз

В раздел «Среда безопасности ОО» необходимо включать описание всех 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/ЗБ могут включаться угрозы, непосредственно которым ОО не противостоит.

Далее приводятся примеры угроз, которые оказывают влияние на безопасное функционирование ОО, но которым ОО может не противостоять:
а) физическое нападение на ОО;
б) злоупотребление правами со стороны привилегированных пользователей;
в) 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/ЗБ имеется некоторая свобода действий в принятии решения, 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 и предположения, и угрозы в дальнейшем отображаются на целях безопасности. При выборе между двумя возможными решениями необходимо стремиться к тому, чтобы обеспечить наилучшее понимание пользователем ПЗ/ЗБ аспектов среды безопасности ОО. Как правило, конкретные нападения должны трактоваться как угрозы, в то время как более общие формы нападений – учитываться при формулировке предположений.

При этом важно, чтобы каждый аспект среды безопасности был сформулирован только один раз: либо в виде предположения безопасности, либо в виде угрозы.

8.3 Идентификация и спецификация политики безопасности организации

Раздел «Среда безопасности ОО» должен содержать описание всех правил ПБОр, которым должен следовать ОО. В тоже время, формулировка ПБОр может быть опущена, если цели безопасности формулируются исключительно на основе угроз: другими словами, в том случае, когда «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 либо ОО, либо его средой, либо некоторой их комбинацией.

Если ПЗ/ЗБ специфицирует и ПБОр, и угрозы, то следует придерживаться краткости изложения в разделе «Среда безопасности ОО» аспектов среды безопасности ОО. Так, например, нецелесообразно включать в ПЗ/ЗБ правило ПБОр, являющееся простой переформулировкой угрозы.

Например, если идентифицирована следующая угроза:

«Неуполномоченный субъект может получить логический доступ к ОО»,

то не имеет смысла включать в ПЗ/ЗБ следующее правило ПБОр:

«Пользователи должны быть идентифицированы до предоставления им доступа».

Это 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 тех случаях, если ОО предполагается использовать в конкретных организациях, а также в тех случаях, когда существует необходимость, чтобы ОО следовал ряду правил, которые не являются очевидными из описания угроз. Далее приведены примеры:

а) идентификация применяемых правил управления информационными потоками;

б) идентификация применяемых правил управления доступом;
в) определение правил ПБОр для аудита безопасности;
г) решения, предписанные организацией, например, использование определенных криптографических алгоритмов или следование определенным стандартам.

Каждое правило ПБОр должно иметь уникальную метку.

Примеры правил ПБОр представлены в Приложении 2 настоящего Руководства.

9. Цели безопасности

Данная глава 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/ЗБ отследить взаимосвязь между аспектами среды безопасности ОО и соответствующими требованиями безопасности (рисунок 2).

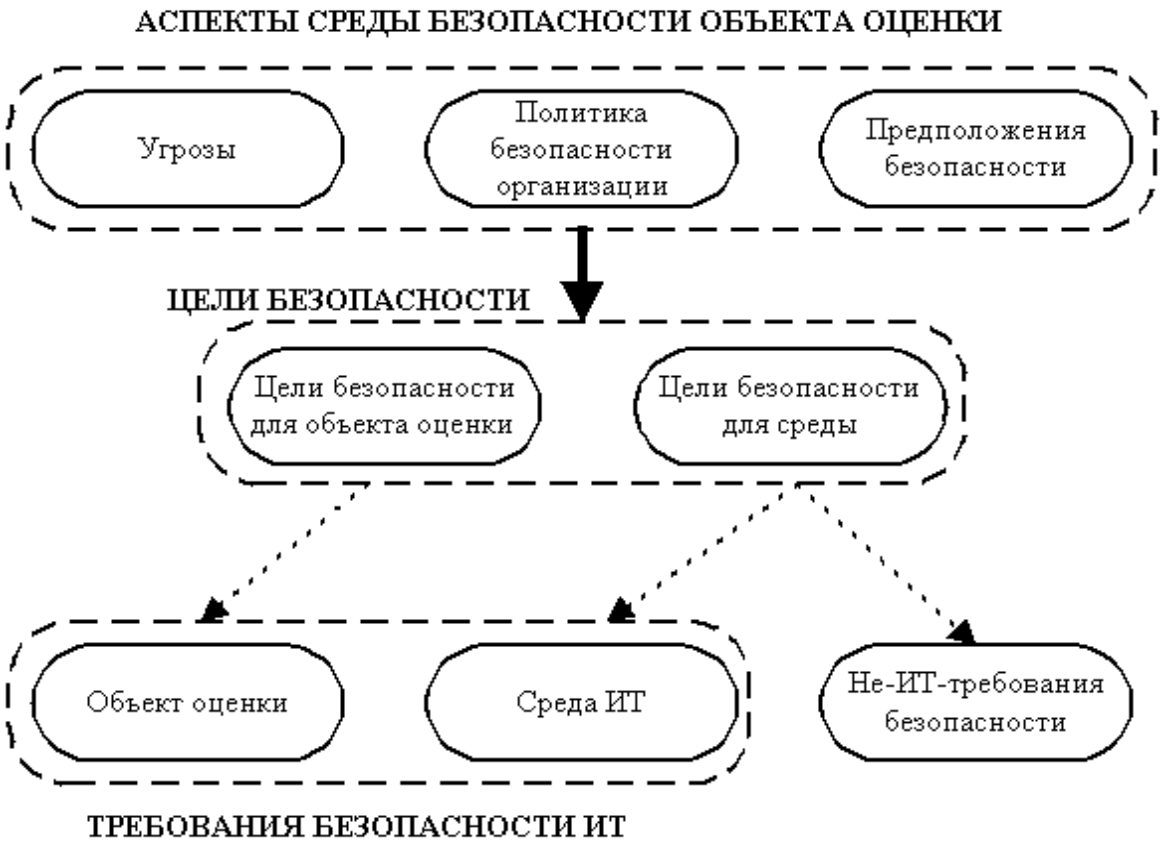

Рисунок 2–Роль и место целей безопасности в структуре ПЗ/ЗБ

Как следует из рисунка 2, в ПЗ/ЗБ необходимо различать два типа целей безопасности:
а) цели безопасности для ОО, которые должны достигаться путем применения контрмер, реализуемых ОО;
б) цели безопасности для среды ОО, которые должны достигаться путем применения 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 то, решение каких аспектов проблемы безопасности возлагается на ОО. Разделение 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 для ОО влияют как на выбор необходимых функциональных требований безопасности ОО, так и на определение уровня доверия к обеспечению безопасности ОО.

9.1 Спецификация целей безопасности для ОО

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

Учитывая ту центральную роль, которую играют цели безопасности в ПЗ/ЗБ, важным является вопрос о наиболее приемлемом уровне детализации при их (целей безопасности) изложении. Требование краткого изложения целей безопасности предполагает достижение определенного равновесия между двумя следующими аспектами:
а) с одной стороны, цели безопасности должны помочь пользователю ПЗ/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 как это решение достигается.
б) в то же время необходимо, чтобы формулировка целей безопасности не являлась бы простым повторением, хотя и в несколько другой форме, информации, содержащейся в описании угроз и ПБОр.

Окончательная проверка правильности выбора уровня детализации формулировки целей безопасности осуществляется 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 либо 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. п. 10.1.1; в части ТДБ см. п. 10.2.1), что, в свою очередь, служит основой для минимизации стоимости и времени, затрачиваемых на оценку ОО.

С точки зрения противостояния идентифицированным угрозам, существует три типа целей безопасности для ОО:
а) цели предупредительного характера, направленные либо на

предотвращение реализации угроз, либо на перекрытие возможных путей реализации данных угроз;
б) цели обнаружения, определяющие способы обнаружения и постоянного мониторинга событий, оказывающих влияние на безопасное функционирование ОО;
в) 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 попадают в категорию целей предупредительного характера. Если ОО должен реализовывать более одной политики управления доступом и информационными потоками, то рекомендуется для каждой политики идентифицировать отдельные цели безопасности. Такой подход способствует упрощению процесса обоснования требований безопасности.

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

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

Примером 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 минимальное значения некоторых частных показателей эффективности обеспечения безопасности, в основном снимая, таким образом, неопределенность относительно уровня эффективности, который должен быть обоснован в разделе ПЗ/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/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/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 данной главе требованиям и рекомендациям по их формулированию. В частности, необходимо убедиться в том, что цели безопасности не содержат излишние детали реализации.

Примеры формулировок целей безопасности приведены в Приложении 2 настоящего Руководства.

Соответствие целей безопасности для ОО угрозам и ПБОр достигается за счет следующего:
а) учета каждой идентифицированной угрозы, направленной против ОО, по крайней мере, одной целью безопасности для ОО;
б) учета каждого правила идентифицированной ПБОр, которому должен удовлетворять 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 виде таблицы. Несмотря на то, что демонстрация соответствия целей безопасности угрозам и ПБОр будет приведена в разделе «Обоснование» (см. главы 12 и 13), для пользователя ПЗ/ЗБ отображение такого соответствия было бы полезно уже в разделе «Цели безопасности». В случае, когда 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 2).

Цели безопасности для ОО должны быть уникально маркированы. Маркировка может быть основана либо на последовательной нумерации (например, Ц1, Ц2, Ц3 и т.д.), либо на использовании значащих меток (см. примеры, представленные в Приложении 2).

9.2 Спецификация целей безопасности для среды ОО

Цели безопасности для среды ОО включают 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:
а) противостояние угрозам (или отдельным аспектам угроз), которым ОО не противостоит;
б) поддержку реализации правил ПБОр, которые не удовлетворены или не полностью удовлетворены ОО;
в) поддержку идентифицированных целей безопасности для ОО в плане противостояния угрозам и реализации соответствующих правил ПБОр;
г) 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:
а) сформулировать новую цель безопасности для учета рассматриваемого аспекта среды безопасности ОО;
б) 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 логического 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).

Формулирование целей безопасности для среды ОО целесообразно осуществлять 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:
а) цели безопасности для ОО должны быть сформулированы таким образом, чтобы соответствующие им требования ИТ не требовали чрезмерно больших затрат на оценку их выполнения;
б) цели безопасности для среды ОО должны быть сформулированы таким образом, чтобы соответствующие им требования к организационным мерам и не-ИТ-средствам были практически реализуемы, а также не накладывались чрезмерные ограничения на действия пользователей ОО.

Типовые не-ИТ-цели безопасности для среды могут предусматривать:
а) разработку и применение организационных мер (методик, процедур, приемов), обеспечивающих эксплуатацию ОО таким образом, что его безопасность не нарушается (в частности, соблюдаются все предположения о среде);
б) 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 п. 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. п. 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. п. 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 тех случаях, когда 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. п.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 бы четко различало 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 представлены в Приложении 2 настоящего Руководства.

10. Требования безопасности ИТ

Данная глава содержит рекомендации по формированию в ПЗ/ЗБ требований безопасности ИТ как для ОО, так и для ИТ-среды. Кроме того, в данной главе кратко излагаются вопросы формирования требований

безопасности для не-ИТ-среды (требования для не-ИТ-среды не являются обязательными для ПЗ/ЗБ).

В ПЗ/ЗБ формулируются следующие типы требований безопасности ИТ.
а) Функциональные требования безопасности ОО. Функциональные требования безопасности определяют требования для функций безопасности, обеспечивающих достижение целей безопасности для ОО.
б) Требования доверия к безопасности ОО. Требования доверия к безопасности определяют требуемый уровень уверенности в надлежащей реализации ФТБ.
в) 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).

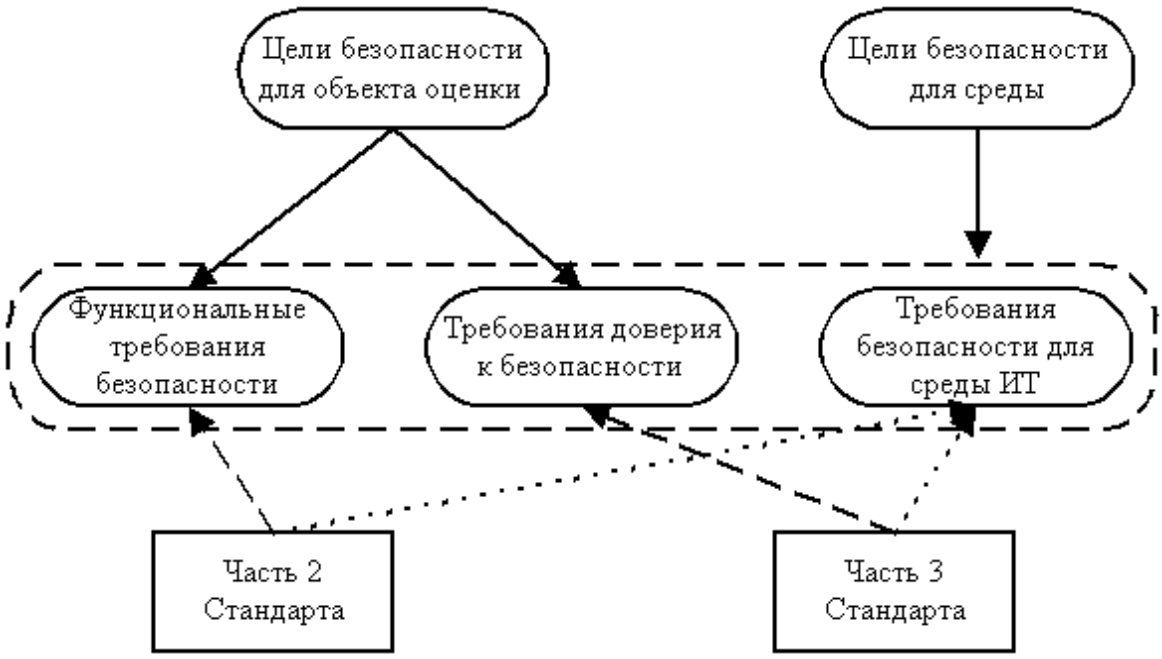

Рисунок 3–Формирование требований безопасности ИТ

Как следует из рисунка 3, требования безопасности ИТ могут быть сформированы, где это возможно, с использованием каталога функциональных компонентов, определенных в части 2 ОК, и каталога компонентов доверия к безопасности, определенных в части 3 ОК.

Использование каталогов требований, определенных в ОК, позволяет достичь определенного уровня стандартизации в области представления

требований безопасности, что значительно облегчает сравнение ПЗ и ЗБ между собой.

Если в частях 2 и 3 ОК отсутствуют соответствующие функциональные компоненты или компоненты доверия к безопасности, требования безопасности ИТ могут быть сформулированы в явном виде. При этом сформулированные в явном виде требования безопасности ИТ должны быть однозначными, подлежать оценке и излагаться в стиле, подобном стилю изложения существующих компонентов ОК.

В пп. 10.1.5 и 10.2.3 даны рекомендации по спецификации соответственно ФТБ и ТДБ в тех случаях, когда в частях 2 или 3 ОК нет подходящих компонентов требований для формулирования рассматриваемых ФТБ и ТДБ.

ОК обеспечивают определенную степень гибкости формирования ФТБ и ТДБ на основе компонентов требований, определяя набор разрешенных операций над компонентами. Разрешенными операциями являются следующие: назначение, итерация, выбор и уточнение.

Рекомендации по выполнению операций над функциональными компонентами, определенными в ОК, включены в п.10.1.2; над компонентами доверия к безопасности – в п. 10.2.2.

При этом отметим, что в ОК каждому компоненту требований безопасности назначается основанная на определенной классификации уникальная метка. Например, для FAU_GEN.1.2 компонента FAU_GEN.1 метка имеет следующий вид:
а) 'F' указывает на то, что это – функциональное требование;
б) 'AU' указывает на то, что ФТБ принадлежит классу ФТБ «Аудит безопасности»;
в) 'GEN' указывает на то, что ФТБ принадлежит семейству «Генерация данных аудита безопасности» класса FAU;
г) '1' указывает на то, что ФТБ принадлежит компоненту «Генерация данных аудита» семейства FAU_GEN;
д) '2' указывает на то, что ФТБ является вторым элементом компонента FAU_GEN.1.

Требования ФТБ и ТДБ выбираются на уровне компонентов: все элементы, входящие в компонент, должны быть включены в ПЗ/ЗБ, если в ПЗ/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. Отношение иерархии предполагает, что один компонент включает 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 разрабатываемый ПЗ/ЗБ обоих этих компонентов.

2. Компоненты могут иметь зависимости 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/ЗБ все зависимости компонентов требований безопасности ИТ должны быть, как правило, удовлетворены. Это достигается включением в ПЗ/ЗБ всех компонентов, от которых зависят уже включенные в ПЗ/ЗБ компоненты. Зависимости могут не удовлетворяться в тех случаях, когда в ПЗ/ЗБ показано, что зависимости не соответствуют целям безопасности и угрозам.

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

10.1 Спецификация функциональных требований безопасности в профиле защиты

10.1.1 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. главу 15).

В процессе формирования ФТБ выделяются несколько этапов. Исходя из них, различают следующие два типа ФТБ:
а) основные ФТБ, непосредственно удовлетворяющие конкретные цели безопасности для ОО;
б) поддерживающие ФТБ, не предназначенные для непосредственного удовлетворения целей безопасности для ОО, но способствующие

выполнению основных ФТБ и, тем самым, косвенным образом способствующие удовлетворению целей безопасности для ОО.

Хотя в 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, соответствующим конкретным целям безопасности для ОО, является идентификация основных ФТБ, непосредственно удовлетворяющих данным целям безопасности. После формирования полной совокупности основных ФТБ начинается итерационный процесс формирования полной совокупности поддерживающих ФТБ. Как упоминалось выше, все ФТБ (и основные, и поддерживающие) целесообразно, где это возможно, формировать на основе функциональных компонентов, определенных в части 2 ОК. При выборе функциональных компонентов, определенных в ОК, целесообразно учитывать рекомендации, содержащиеся в приложениях к части 2 ОК и связанные с интерпретацией данных компонентов.

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

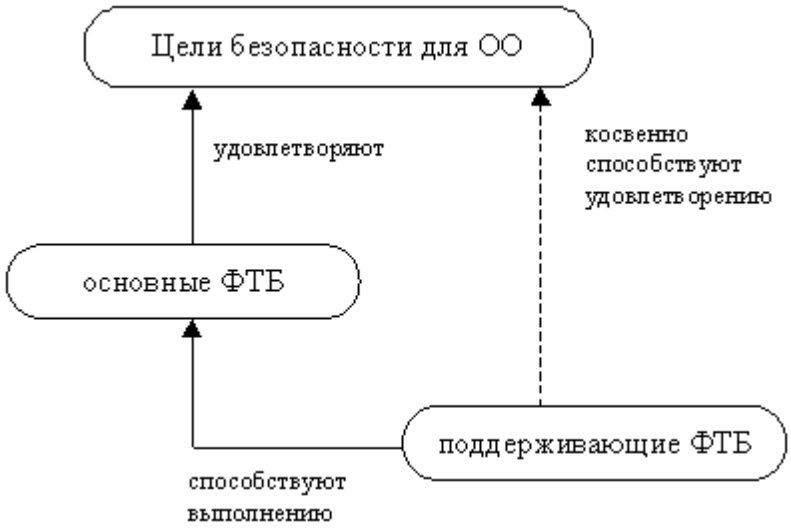

Рисунок 4–Взаимосвязь основных и дополнительных ФТБ

Формирование полной совокупности поддерживающих ФТБ включает следующие стадии:
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.

Идентификация поддерживающих ФТБ представляет собой итерационный процесс, например:
а) предположим, что ПЗ включает 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»;
б) 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;
в) компонент FAU_SAA.1 имеет зависимость от FAU_GEN.1 «Генерация данных аудита»;
г) компонент FAU_GEN.1 имеет зависимость от FPT_STM.1 «Надежные метки времени»;
д) компонент FPT_STM.1 не требует ввода дополнительных функциональных компонентов.

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

При удовлетворении зависимостей необходимо обеспечить согласованность соответствующих компонент. 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 (т.е. тех, которые не требуются для удовлетворения зависимостей) включает 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 следующие:

а) ФТБ, основанные на соответствующих компонентах из того же самого 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 другое изделие ИТ.

б) 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».

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

Выбор поддерживающих ФТБ должен всегда осуществляться в соответствии с целями безопасности, чтобы сформировать целостный набор взаимно поддерживающих ФТБ. Таким образом, на выбор поддерживающих ФТБ существенное влияние может оказывать процесс построения раздела ПЗ «Обоснование». Необходимо избегать включения в ПЗ поддерживающих ФТБ, которые не направлены на достижение целей безопасности, так как включение подобных ФТБ приведет к ограничению сферы применения ПЗ вследствие следующих обстоятельств:
а) некоторые ОО могут быть не способны удовлетворить избыточные поддерживающие ФТБ;
б) увеличение числа ФТБ увеличивает стоимость оценки.

Если ПЗ создается на основе другого (базового) ПЗ, то процесс выбора ФТБ значительно упрощается. Однако в новый ПЗ должны быть включены (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.

10.1.2 Выполнение операций над функциональными требованиями безопасности

Как излагалось выше, над функциональными компонентами могут выполняться разрешенные операции. Выполняя операции над функциональными компонентами, разработчик ПЗ может сформировать соответствующее данному ПЗ требование безопасности. Допустимыми операциями являются:
а) назначение – позволяет специфицировать идентифицированный параметр (результат спецификации может быть, в том числе, и «пустым» значением);
б) итерация – позволяет несколько раз использовать функциональный компонент с различным выполнением операций для определения различных требований;
в) выбор – позволяет специфицировать один или несколько элементов из списка;
г) уточнение – позволяет добавить детали к требованиям безопасности, ограничивая, таким образом, возможную совокупность приемлемых решений без необходимости введения новых зависимостей от других ФТБ.

Операция «итерация» часто используется для определения ФТБ на основе компонентов класса FMT («Управление безопасности»), которые включаются в ПЗ для удовлетворения зависимостей многих других функциональных компонентов. Для того чтобы удовлетворить такие зависимости, обычно необходимо использовать компоненты класса FMT, над которыми операции «назначение» и «выбор» выполняют по-разному.

Например, компонент FMT_MSA.1 может быть использован многократно для определения отдельных ФТБ, соответствующих управлению различными типами атрибутов безопасности. Аналогично, может потребоваться неоднократное использование компонентов семейств FDP_ACC и FDP_ACF в тех случаях, когда требуется, чтобы ОО реализовывал различные политики управления доступом, например, дискреционную и ролевую.

Целесообразно использовать операцию «итерация» для улучшения читабельности ПЗ, например, для того, чтобы разбить сложное и громоздкое ФТБ на отдельные понятные ФТБ. Использование операции «итерация», тем не менее, может породить другие потенциальные проблемы при представлении ФТБ в ПЗ/ЗБ (см. п. 10.1.6).

Для каждого ФТБ, включаемого в ПЗ, необходимо принять решение:
а) выполнить операции «назначение» и «выбор», предусмотренные функциональным компонентом для изложения ФТБ;
б) специфицировать операцию «уточнение» для ФТБ.

Операции «назначение» и «выбор»

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

При принятии решения о необходимости выполнения операций «назначение» и «выбор» в каждом конкретном случае необходимо учитывать следующие факторы:
а) 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.
б) 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 «Логического 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 оставить разработчику ЗБ максимальную свободу действий и, вместе с тем, предотвратить такое выполнение операций «назначение» и «выбор», которое несовместимо с целями безопасности для ОО.

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

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

Другой 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, чтобы в ЗБ для соответствующего ОО была специфицирована защита 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. Аналогично, частичное выполнение операции «назначение» является надлежащим, если допустимые значения выполнения операции «назначение» над ФТБ являются допустимыми и для исходного функционального компонента. Если по какой-либо причине эти условия не выполняются, то необходимо использовать расширенный функциональный компонент с другими операциями «назначение» и «выбор».

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

При выполнении операций «назначение» и/или «выбор» в ПЗ целесообразно выделить другим шрифтом специфицированный текст в целях большей наглядности для пользователей ПЗ (и особенно для оценщика ПЗ при проверке соответствия ПЗ требованиям ОК). Например, требование на основе элемента FMT_SAE.1.1 могло быть представлено следующим образом:

«ФБО должны ограничить возможность назначать срок действия для паролей пользователя 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 содержания ресурсов при распределении ресурса для следующих объектов: [назначение: список специфицируемых разработчиком ЗБ объектов]».

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

Операция «уточнение»

Операция «уточнение» может быть выполнена над любым элементом 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 эти термины подвергаются операции «уточнение». Дополнительные детали 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. Использование операции «уточнение» целесообразно в следующих случаях:
а) если ПЗ разрабатывается организацией, выдвигающей такие требования безопасности, которых нет в функциональных компонентах ОК и которые не могут быть специфицированы путем выполнения над функциональными компонентами разрешенных операций «назначение» и «выбор»;
б) если выбранный функциональный компонент допускает ненадлежащую для рассматриваемого типа ОО реализацию требования безопасности;
в) если читабельность ФТБ может быть улучшена.

В целях содействия пользователю ПЗ (и, особенно, – оценщику ПЗ) целесообразно (как и в случаях с операциями «назначение» и «выбор») выделять специфицированный с помощью операции «уточнение» текст.

Далее приводится пример выполнения операции «уточнение» применительно к требованию на основе элемента FMT_MTD.3.1:

«ФБО должны обеспечить присвоение данным ФБО только безопасных значений.

Уточнение: ФБО должны обеспечить, чтобы минимальная длина пароля, требуемого ОО, была, по крайней мере, 6 символов».

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

10.1.3 Спецификация требований аудита

Если в ПЗ включены требования аудита (основанные на компоненте FAU_GEN.1), то при формировании всех 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:
а) определенные в ПБОр требования к аудиту безопасности;
б) значимость аудита безопасности для достижения целей безопасности;
в) значимость некоторых событий и их характеристик для целей безопасности;
г) анализ «стоимость-эффективность».

Например, если ОО предназначен для защиты от 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:
а) является ли регистрируемая информация полезной для ее последующего анализа;
б) имеет ли администратор необходимые ресурсы (например, инструментальные средства поддержки) для эффективного анализа собранной информации;
в) каковы предполагаемые затраты на хранение и обработку собираемых данных.

В ОК введены три предопределенных уровня аудита: минимальный, базовый и детализированный. Для каждого предопределенного уровня в части 2 ОК 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:
а) минимальный уровень аудита требует, чтобы аудиту подвергалось только определенное подмножество действий или событий, связанных с данным функциональным компонентом (подвергаемые аудиту события – это обычно наиболее значимые события, представляющие наибольший интерес);
б) базовый уровень аудита требует, чтобы аудиту подвергались все действия или события, связанные с данным функциональным компонентом (например, успешные и неудачные попытки доступа к ОО);
в) 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, можно принять за основу минимальный уровень аудита, но в ряде случаев отклоняться от минимальных требований вследствие того, что какое-либо подмножество действий или событий является более значимым для достижения целей безопасности. Например, если компонент FDP_ACF.1 включен в ПЗ, то может потребоваться более детальный аудит неудачных попыток доступа по сравнению с успешными.

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

10.1.4 Спецификация требований управления

В подразделе «Управление» для каждого семейства компонент (см. часть 2 ОК) 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 ОК 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 тогда, когда 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. пп.12.1.1 и 12.1.4).

10.1.5 Спецификация в ПЗ функциональных требований, не изложенных в части 2 ОК

Если при разработке ПЗ требуется включить в документ функциональное требование, для которого в ОК отсутствует соответствующий функциональный компонент, то в качестве формы представления рассматриваемого ФТБ необходимо использовать форму представления функциональных компонентов в ОК.

Принятие решения о наличии либо отсутствии соответствующего функционального компонента в части 2 ОК может оказаться сложным, т. к. предполагает хорошее знание ОК. С учетом этого рекомендуется использовать приложение 2 настоящего Руководства, идентифицирующее функциональные компоненты, 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, несоответствующие 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 ОК.

Спецификация ФТБ в явном виде включает:
а) определение ФТБ на том же уровне абстракции, что и функциональные компоненты ОК;
б) использование стиля и фразеологии (языка) функциональных компонентов ОК.

Подобие нового ФТБ другим ФТБ, которые уже имеются в составе существующего в ОК класса или семейства, способствует ограничению его новизны и использованию специфических для данного класса или семейства формулировок и понятий.

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

б) использование устоявшихся терминов, таких как «атрибуты безопасности» и «уполномоченный пользователь»;
в) каждый элемент требований должен быть самостоятельным и понятным без каких-либо ссылок на другие элементы требований;
г) каждое требование безопасности должно быть оцениваемо, т. е. должна существовать возможность дать заключение о том, удовлетворяет ли ОО рассматриваемому требованию.

При формировании ФТБ в явном виде необходимо решить:
а) будут ли над ФТБ совершаться операции «выбор» и «назначение», подлежащие выполнению разработчиком ЗБ;
б) предполагает ли ФТБ какие-либо зависимости от других ФТБ, которые должны быть удовлетворены в ПЗ;
в) будет ли ФТБ требовать аудита каких-либо событий и, если будет, то какая информация о событиях подлежит регистрации;
г) будет ли ФТБ включать параметры безопасности, подлежащие управлению, например, зависеть от атрибутов безопасности, которые подлежат управлению.

Именование ФТБ, не основанных на компонентах ОК, должно показывать, что это – дополнительное по отношению к ОК требование безопасности.

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

10.1.6 Представление функциональных требований безопасности

При формировании перечня ФТБ разработчик ПЗ должен представить их таким образом, чтобы обеспечить наилучшее понимание требований безопасности пользователями и согласование ФТБ с требованиями ОК.

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 части 2 ОК.

Во-вторых, для маркировки ФТБ в ПЗ совсем не обязательно использовать систему маркировки элементов, принятую в части 2 ОК. Для этих целей разработчик ПЗ может использовать свою собственную систему маркировки ФТБ (например, на основе более информативных меток). При использовании собственной системы маркировки ФТБ разработчик ПЗ должен представить (например, в приложении к ПЗ) отображение представленных в ПЗ ФТБ на соответствующие функциональные компоненты, определенные в части 2 ОК. Подход к маркировке ФТБ на основе собственной системы маркировки разработчика ПЗ является предпочтительным, в частности, тогда, когда в ПЗ имеются неоднократные ссылки на одни и те же функциональные компоненты. В этих случаях использование системы маркировки, принятой в части 2 ОК, могло бы привести к серьезным затруднениям при формировании подраздела ПЗ «Логическое обоснование требований безопасности».

В-третьих, 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.

Далее приведен пример выполнения операции «уточнение» над элементом FMT_MSA.3.1 функционального компонента FMT_MSA.3

«Инициализация статических атрибутов».

Элемент FMT_MSA.3.1 в части 2 ОК 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» использовалась 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.

Результат выполнения операции «уточнение» в формулировке ФТБ должен быть выделен курсивом (или другим способом). 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 5 настоящего Руководства.

10.2 Спецификация в ПЗ требований доверия к безопасности

10.2.1 Выбор требований доверия к безопасности

Выбор требований доверия к безопасности зависит от следующих факторов:
а) ценности активов, подлежащих защите, и осознаваемого риска их компрометации;
б) технической реализуемости;
в) стоимости разработки и оценки;
г) требуемого времени для разработки и оценки ОО;
д) требований рынка (для продуктов ИТ);
е) зависимостей функциональных компонентов и компонентов доверия к безопасности.

Чем выше ценность активов, подлежащих защите, и чем больше риск компрометации этих активов, тем выше требуется уровень доверия к безопасности для функций безопасности, используемых для защиты рассматриваемых активов. Эти моменты следует отразить при формировании целей безопасности. Организации могут устанавливать свои собственные правила определения уровня доверия к безопасности, который требуется для снижения риска для этих активов до приемлемого уровня. Это, в свою очередь, определяет требуемый уровень доверия к безопасности продуктов ИТ, которые предполагается использовать в этой организации.

Остальные факторы, такие как стоимость и затраты времени, целесообразно рассматривать как ограничения на уровень доверия к безопасности, который является практически достижимым. Техническая реализуемость рассматривается в том случае, когда считается практически

нецелесообразной подготовка свидетельства, требуемого конкретными компонентами доверия к безопасности. Данная ситуация актуальна для наследуемых систем (в случаях, когда конструкторская документация недоступна), а также в тех случаях, когда в идеале требуется высокий уровень доверия к безопасности, но технически невозможно за приемлемое время подготовить требуемое формальное либо полуформальное свидетельство. В тех случаях, когда имеются ограничения на практически достижимый уровень доверия к безопасности, целесообразно согласиться с тем, что максимально достижимый уровень доверия к безопасности меньше, чем теоретически возможный. Такое восприятие риска должно быть отражено и при изложении целей безопасности.

Изложение целей безопасности может также указывать на то, какие конкретные требования доверия к безопасности должны быть включены в набор ТДБ. Например:
а) цели безопасности для ОО могут устанавливать, что ОО должен быть стойким к нарушителям с высоким потенциалом нападения;
б) цели безопасности могут требовать анализа скрытых каналов, что однозначно определяет включение в ПЗ/ЗБ компонента из семейства AVA_CCA «Анализ скрытых каналов», требующего проведения анализа скрытых каналов;
в) при формулировке целей безопасности может быть отмечено, что безопасность ОО серьезно зависит от безопасности среды разработки. В этом случае настоятельно рекомендуется включить в набор ТДБ компонент из семейства ALC_DVS «Безопасность разработки», содержащий требование анализа безопасности среды разработки.

Выбор ТДБ относительно несложен, если требуется просто выбрать подходящий пакет доверия к безопасности (см. главу 15), например, ОУД, определенный в ОК. Для того чтобы выбрать подходящий с точки зрения сформулированных целей безопасности пакет доверия к безопасности, необходимо изучить его описание (например, при выборе ОУД см. главу 6 части 3 ОК).

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».

10.2.2 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:
а) «итерация», допускающая многократное использование одного и того же компонента доверия к безопасности;
б) «уточнение», позволяющее добавить детали к требованию доверия к безопасности.

На практике, выполнение операции «итерация» может потребоваться в тех случаях, когда требуются разные «уточнения» для одного и того же компонента доверия к безопасности, который используется для разных частей ОО, либо когда в ПЗ/ЗБ определены различные наборы ТДБ для разных компонентов составного ОО (см. п. 14.1.4). 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 выполнено в следующих целях:
а) в целях предписания разработчику использовать конкретные инструментальные средства разработки, методики, модели жизненного цикла, методы анализа, системы обозначений, определенные стандарты и так далее;
б) в целях предписания действий оценщика, например:
- компонент ADV_IMP.1 определяет, какие части представления реализации ОО должны быть оценены;
- компонент ADV_IMP.1 идентифицирует известные уязвимости, которые необходимо рассматривать как «явные» уязвимости в контексте данного ОО.

10.2.3 Спецификация в профиле защиты требований доверия к безопасности, не включенных в Стандарт

Если в ПЗ включается ТДБ, для которого в ОК нет соответствующего компонента доверия к безопасности, то рассматриваемое ТДБ должно быть определено в стиле компонентов из ОК.

Сформулированные в явном виде ТДБ должны содержать определение следующих аспектов:

а) действий разработчика;
б) требований к содержанию и представлению свидетельств, которые должен представить разработчик;
в) 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 в стиле изложения компонентов доверия к безопасности, определенных в части 3 ОК. Поэтому отдельное требование необходимо оформлять в виде отдельного элемента требований (см. п.2.4.1 части 3 ОК). При этом необходимо использовать терминологию, приведенную в п. 2.4 части 3 ОК.

10.3 Спецификация требований безопасности в ЗБ

10.3.1 Спецификация функциональных требований, приведенных в ПЗ

Если в ЗБ заявлено соответствие одному или нескольким ПЗ, то, вероятно, ФТБ уже специфицированы в ПЗ. В таких случаях необходимо принять решение – специфицировать ФТБ в ЗБ полностью (для того, чтобы весь текст был в одном месте) либо включить в ЗБ ссылку на ФТБ, специфицированные в ПЗ, и специфицировать либо те ФТБ, которых нет в ПЗ, либо те, которые отличаются от специфицированных в ПЗ.

Предпочтителен последний подход, так как при этом упрощается ЗБ. Пользователей ЗБ больше интересуют функции безопасности ИТ, чем ФТБ. Это же относится и к оценщику ОО (т. к. содержание свидетельств оценки – проектной, тестовой документации, руководств – в краткой спецификации ОО проще привязать к функциям безопасности ИТ, чем к ФТБ). Основная цель спецификации ФТБ в ЗБ – продемонстрировать соответствие ФТБ ЗБ

функциональным требованиям соответствующих ПЗ и функциональным требованиям, определенным в части 2 ОК. 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 (например, курсивом). 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. п. 13.2.6).

10.3.2 Спецификация функциональных требований, отсутствующих в ПЗ

В некоторых случаях необходимо специфицировать ФТБ, которые отсутствуют в соответствующем ПЗ. Это может быт, когда:
а) для ОО отсутствует подходящее ПЗ, соответствие которому может быть заявлено в ЗБ;
б) спонсор (заказчик) считает, что преимущества от включения требования дополнительной по отношению к ПЗ функциональности оправдывают дополнительные расходы на оценку.

В этих случаях целесообразно использовать подход к спецификации ФТБ, аналогичный подходу, описанному в п.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).

10.3.3 Спецификация в задании по безопасности функциональных требований, не включенных в Стандарт

Разработчик ЗБ может сформулировать ФТБ в ЗБ в явном виде, то есть без ссылки на функциональные компоненты, определенные в части 2 ОК. При этом необходимо следовать инструкциям, представленным в п.10.1.5. Наряду с этим, нет необходимости для формулируемых в явном виде ФТБ определять операции, описанные в ОК («назначение», «выбор»), если не предполагается их повторное использование в ПЗ, других ЗБ, функциональных пакетах.

10.3.4 Спецификация в задании по безопасности требований доверия к безопасности

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 ОК).

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 тех случаях, когда спонсор (заказчик) оценки считает, что получаемые преимущества оправдывают дополнительные расходы на оценку. В этих случаях спецификация ТДБ должна быть выполнена с использованием описанных в п.10.2 инструкций и соответствовать целям безопасности. Требования доверия к безопасности, которые не основаны на компонентах доверия к безопасности, определенных в ОК, могут быть включены в ЗБ аналогично тому, как они включаются в ПЗ (см. п.10.2.3).

10.4 Требования безопасности для среды

10.4.1 Требования безопасности для ИТ-среды

В ПЗ/ЗБ должны включаться требования безопасности для ИТ-среды. Далее приводятся примеры тех случаев, когда необходимость задания требований безопасности для ИТ-среды очевидна:
а) 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.
б) 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 (таким образом, что одно приложение не может 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/ЗБ функциональных компонентов, определенных в части 2 ОК, в том случае, когда включаемые для удовлетворения зависимостей требования

безопасности с большим успехом могут быть выполнены ИТ-средой по сравнению с ОО.

Требования безопасности для ИТ-среды и предположения о среде различаются в следующем:
а) предположения не требуют доказательств (являются очевидными) при анализе;
б) требования безопасности необходимы для того, чтобы обеспечить достижение 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 ОК. Любое отклонение от этих компонентов должно сопровождаться строгим обоснованием в ПЗ/ЗБ.

В некоторых случаях нецелесообразно формулировать функциональные требования безопасности для ИТ-среды на основе функциональных компонентов, определенных в части 2 ОК. 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 количество 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/ЗБ могут не включаться, вследствие того, что данные требования не имеют непосредственного отношения к реализации ОО.

Необходимость во включении в ПЗ/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. Второй случай имеет место, если появляется необходимость в детальном согласовании требований безопасности ИТ в ПЗ/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. п. 12.2.1).

Предпочтительнее (для исключения смешивания различных уровней абстракции) представлять требования безопасности для не-ИТ-среды в отдельном (под)разделе «Требования безопасности для не-ИТ-среды», а не трактовать их как цели или предположения безопасности. (Под)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/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/ЗБ).

11. Краткая спецификация объекта оценки

Настоящая глава 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 включить следующее:
а) определение функций безопасности ИТ;
б) ссылки на механизмы или методы защиты, используемые для осуществления функций безопасности ИТ (необязательно);
в) изложение мер доверия к безопасности, которые удовлетворяют сформулированным требованиям доверия к безопасности.

Основные части раздела «Краткая спецификация ОО» представлены на рисунке 5:

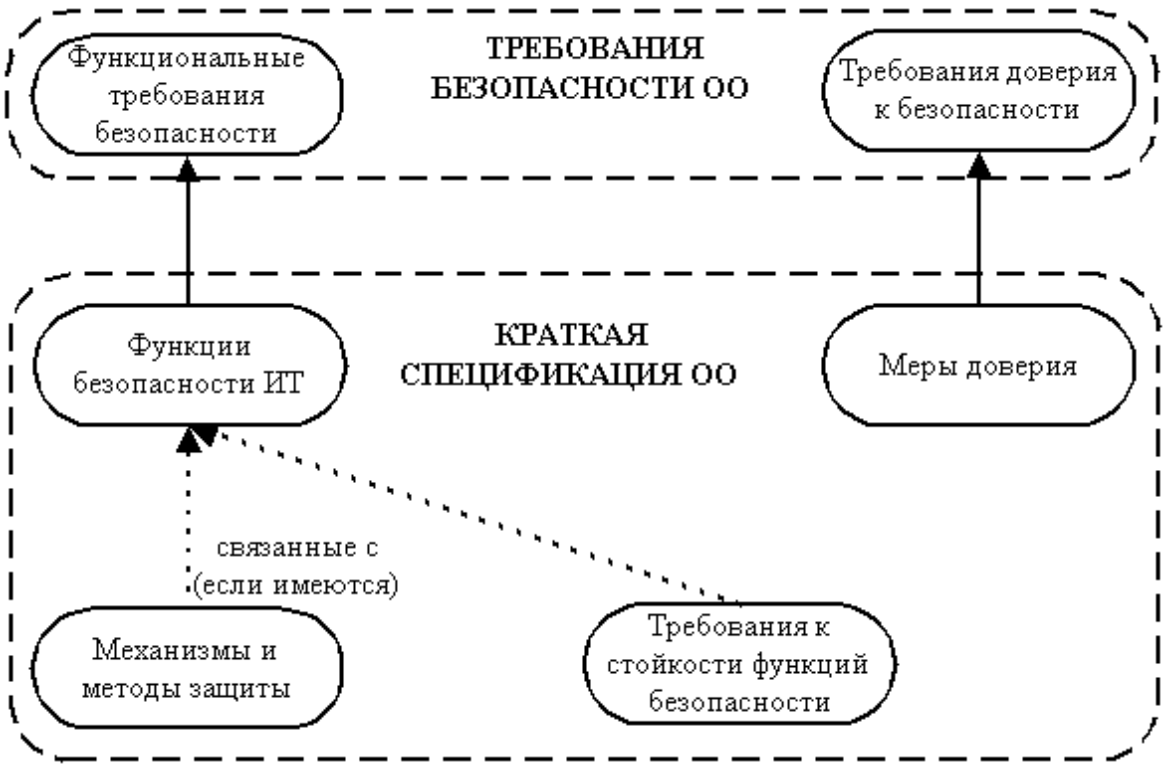

Рисунок 5–Содержание раздела «Краткая спецификация ОО»

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 таким образом, чтобы представить функциональные возможности безопасности ОО в более понятном для пользователя ЗБ виде по сравнению с ФТБ. В частности:
а) функции безопасности ИТ могут быть изложены таким образом, чтобы показать, что ОО фактически делает для обеспечения безопасности.
б) функции безопасности ИТ могут быть специфицированы таким образом, чтобы более точно отражать документацию ОО, например, путем использования специфической для ОО терминологии. Это может повысить рентабельность оценки ОО, облегчая верификацию уровней представления ФБО (ЗБ, проектная документация). Один из возможных подходов заключается в спецификации одной функции безопасности ИТ, удовлетворяющей нескольким ФТБ, если известно, что эти ФТБ выполняются теми же самыми основными механизмами при проектировании и реализации (разработке) ОО. Данный подход выгоден для сокращения количества доказательств соответствия представления, которое должен

обеспечить разработчик.
в) 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 типа «субъект», «объект» или «роль администратора». Поэтому раздел «Краткая спецификация ОО» может быть охарактеризован как развитие требований, которым должен удовлетворять 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.

11.1 Спецификация функций безопасности информационных технологий

Как изложено выше, раздел ЗБ «Краткая спецификация ОО» должен включать спецификацию функций безопасности ОО. Задание по безопасности должно демонстрировать, что функции безопасности ИТ покрывают все ФТБ, а также то, что каждая функция безопасности ИТ отображается, по крайней мере, на одно 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. Это может быть направлено на то, чтобы упростить спецификацию функциональной возможности и облегчить соответствующую оценку.

Например:
а) функция безопасности ИТ может отображаться более чем на одно ФТБ (это может иметь место в случае с поддерживающими функциями); или
б) ФТБ может отображаться более чем на одну функцию безопасности ИТ (это может иметь место в случае с функциями, которые определяют основное назначение ОО с точки зрения обеспечения безопасности информации).

При выполнении таких преобразований необходимо:
а) не потерять детали, содержащиеся в ФТБ;
б) не допустить слишком сложного отображения ФТБ на функции

безопасности ИТ, увеличения стоимости рассмотрения и оценки ЗБ, а также увеличения вероятности ошибок.

11.2 Спецификация механизмов безопасности

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

Необходимо отметить, что ссылки на механизмы безопасности в ЗБ не обязательны.

На механизмы безопасности целесообразно ссылаться в следующих случаях:
а) для системы ИТ существует требование использования конкретного механизма безопасности;
б) для продукта ИТ есть необходимость в реализации конкретных механизмов безопасности (например, с учетом рыночного спроса на такие механизмы и методы).

11.3 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) возможна большая детализация, например, ссылки на конкретные инструментальные средства, методы или подходы, используемые разработчиком для удовлетворения требований доверия к безопасности, такие как:
а) обозначения, которые необходимо использовать в требуемых формальных спецификациях;
б) методики разработки и модели жизненного цикла;
в) инструментальные средства управления конфигурацией;
г) инструментальные средства анализа покрытия тестами;
д) методы анализа скрытых каналов.

12. Обоснование ПЗ

Настоящая глава представляет собой руководство по формированию раздела ПЗ «Обоснование».

Назначение раздела ПЗ «Обоснование» заключается в том, чтобы показать, что 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, в то же время он может быть полезен и для других пользователей ПЗ.

На рисунке 6 представлены ключевые аспекты раздела ПЗ «Обоснование».

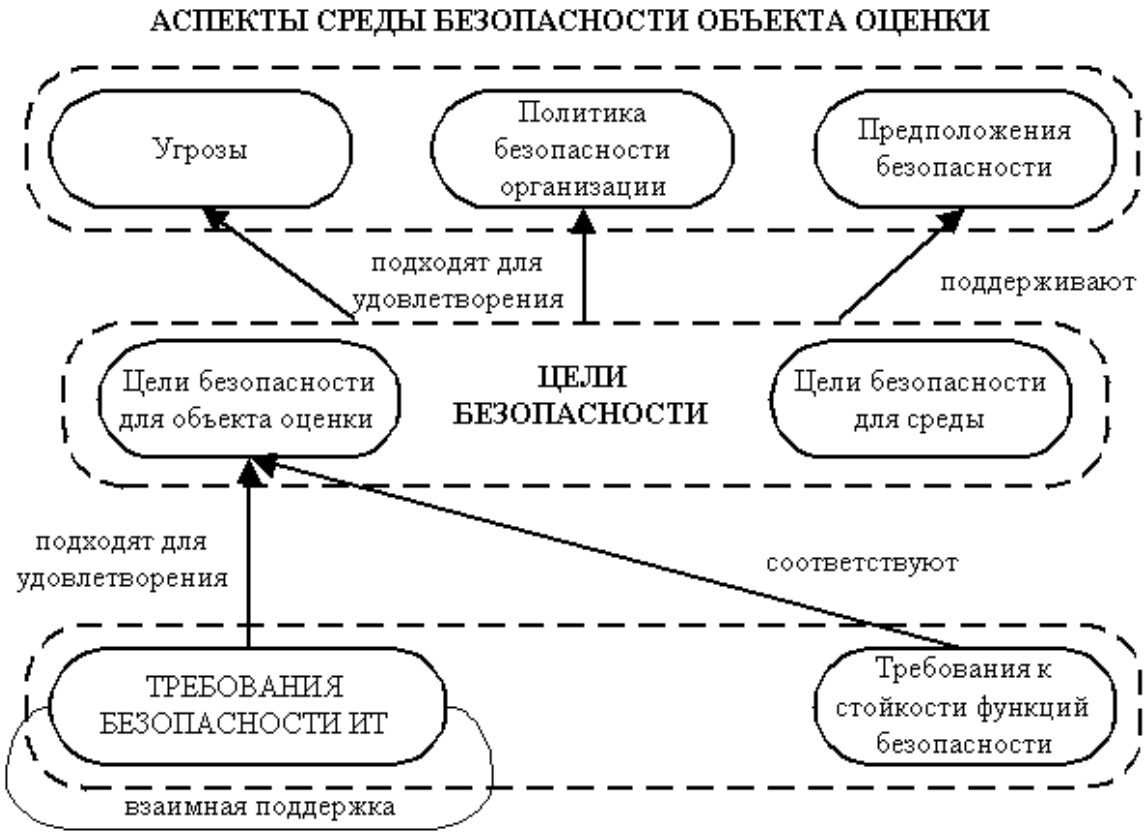

Рисунок 6–Требования к разделу ПЗ «Обоснование»

Дополнительно, «Обоснование ПЗ» должно показать, что:
а) формулировка требований доверия к безопасности является надлежащей;
б) неудовлетворенные зависимости требований безопасности ИТ, включенных в ПЗ, не являются необходимыми.

В разделе «Обоснование ПЗ» настоятельно рекомендуется использование таблиц, сопровождаемых, где необходимо, неформальным объяснением, поскольку это делает раздел более кратким и упрощает его использование.

12.1 Представление в профиле защиты логического обоснования целей безопасности

Логическое 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 то, что достижение этих целей необходимо.

Данная задача может решаться следующим образом.

Во-первых, перекрестные ссылки: угрозы, ПБОр, предположения – цели безопасности, охватывающие аспекты среды безопасности ОО, целесообразно оформить в виде таблиц.

При этом пользователю ПЗ при изучении данных таблиц должно быть наглядно видно, что:
а) каждая цель безопасности охватывает, по крайней мере, одну угрозу, правило ПБОр или предположение безопасности;
б) 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 неформальным объяснением:
а) для каждой угрозы – относительно того, что изложенные цели безопасности предусматривают эффективные контрмеры по отношению к угрозам, т.е. цели безопасности показывают, что событие, указанное в спецификации угрозы, будет:
- либо обнаружено, и его последствия компенсированы (или ущерб от его наступления ограничен),
- либо предотвращено (или снижена до приемлемого уровня вероятность его наступления);

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

Объяснение должно:
а) показать роль каждой цели безопасности в противостоянии угрозе или удовлетворении ПБОр;
б) показать, как при помощи целей безопасности для среды безопасности ОО осуществляется поддержка целей безопасности для ОО.

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

12.2 Формирование логического обоснования требований безопасности в профиле защиты

12.2.1 Демонстрация пригодности требований безопасности

Назначение этой части раздела ПЗ «Обоснование» заключается в том, чтобы показать, что 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 сформировать таблицу, в которой сопоставить каждую цель безопасности с ФТБ, которое удовлетворяет данной цели. Таблица должна показывать следующее:
а) каждая ФТБ учитывает, по крайней мере, одну цель безопасности;
б) каждая цель безопасности связана, по крайней мере, с одним ФТБ.

Последнего будет достаточно для обоснования необходимости каждого ФТБ (т.е. будут исключены избыточные ФТБ).

Во-вторых, сформированная 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, то есть и те, которые непосредственно удовлетворяют цели безопасности (основные ФТБ), и те, которые предназначены для их поддержки (поддерживающие ФТБ).

При формировании объяснения необходимо рассмотреть следующее:

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

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

Хотя это и не обязательно, рекомендуется включать в ПЗ объяснение роли включенных в ПЗ требований безопасности для не-ИТ-среды.

В следующем разделе приводятся рекомендации по представлению обоснования пригодности ТДБ.

12.2.2 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:

а) 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 использовать 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);
б) не является избыточным по отношению к среде безопасности и сформулированным целям безопасности;
в) является достижимым, т.е. для данного типа ОО сформулированные требования доверия к безопасности являются технически выполнимыми (с точки зрения стоимости и затрат времени на оценку безопасности ОО).

12.2.3 Обоснование 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:
а) присутствующие в формулировках целей безопасности для ОО в явном и неявном виде требования к стойкости функций безопасности;
б) 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.

12.2.4 Демонстрация взаимной поддержки требований безопасности

Назначение данной части раздела «Обоснование ПЗ» заключается в том, чтобы показать, что требования безопасности ИТ (и, в частности, ФТБ) полны и внутренне непротиворечивы. Это достигается демонстрацией их взаимной поддержки, а также того, что они представляют собой «интегрированное и эффективное целое». В этих целях рекомендуется следующий подход:
а) демонстрация того, что, где необходимо, зависимости компонентов функциональных требований и требований доверия к безопасности удовлетворены;
б) демонстрация внутренней непротиворечивости (согласованности) между

требованиями безопасности ИТ;
в) демонстрация того, что, где необходимо, включены поддерживающие ФТБ, предназначенные для защиты механизмов безопасности, реализующих другие ФТБ, от нападений типа «обход» и «несанкционированное изменение».

Далее рассмотрим каждый из перечисленных аспектов взаимной поддержки.

Анализ зависимостей компонентов

Данный анализ наиболее эффективно может быть представлен посредством 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 должен включать:
а) демонстрацию на уровне ФТБ удовлетворения зависимостей для каждой итерации функционального компонента;
б) идентификацию каждой неудовлетворенной зависимости и обоснование отсутствия необходимости в ее удовлетворении.

Необходимость проведения анализа зависимостей на уровне ФТБ обусловлена тем, что, если компонент включается 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 включается в ПЗ неоднократно в целях инициализации различных атрибутов безопасности, то, вероятно, и FMT_MSA.1 необходимо включить в ПЗ то же самое количество 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 неполон, так как ФТБ компонента FMT_MSA.1 могут не охватывать все атрибуты безопасности, упомянутые в ФТБ компонента FMT_MSA.3.

Удовлетворение зависимости может не требоваться, когда она не соответствует ОО или данная зависимость 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 построением таблицы, которая:
а) включает одну или несколько строк (по числу вхождений компонента в ПЗ) для каждого функционального компонента, включенного в ПЗ;
б) назначает уникальную метку или номер каждой строке с тем, чтобы каждое ФТБ было идентифицировано уникальным образом;
в) идентифицирует функциональный компонент, ассоциированный с каждой строкой;
г) для каждого функционального компонента формирует список зависимостей от других компонентов в соответствии с ОК;
д) для каждой идентифицированной зависимости либо 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 ОК), 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 ОК 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 таблице должна быть ОУД4.

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

Внутренняя непротиворечивость

Демонстрацию внутренней непротиворечивости требований безопасности ИТ рассмотрим на примере ФТБ. Так, если ПЗ включает требования по подотчетности и, в то же время, по анонимности действий пользователя, то в разделе «Обоснование ПЗ» должно быть показано, что эти требования не находятся в противоречии. В данном случае требуется показать, что в

качестве событий аудита, требующих подотчетность пользователя, не рассматриваются те, для которых требуется анонимность.

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:
а) по определению, ТДБ поддерживают ФТБ, так как они обеспечивают уверенность в том, что функциональные требования удовлетворены;
б) имеется незначительное количество случаев, когда ФТБ поддерживают ТДБ, и это должно быть учтено при формировании «Обоснования ПЗ». Приведем соответствующий пример. Компоненты семейства FPT_SEP «Разделение домена» поддерживают компоненты семейства ADV_HLD «Проект верхнего уровня», способствуя проведению соответствующего разбиения.
в) можно утверждать, что ТДБ являются взаимно поддерживающими и все их зависимости удовлетворены.

Как описано в п. 10.1.1, 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 ОК.

Рассмотрение взаимной поддержки между ФТБ, не охваченными анализом зависимостей, должно включать рассмотрение следующих ФТБ:
а) ФТБ, которые направлены на предотвращение обхода механизмов, реализующих другие ФТБ;
б) ФТБ, которые направлены на предотвращение несанкционированного воздействия на механизмы, реализующие другие ФТБ (включая атрибуты безопасности и другие данные, целостность которых является критичной для ФТБ);
в) ФТБ, которые препятствуют несанкционированному отключению механизмов, реализующих другие ФТБ;
г) ФТБ, предназначенные для обнаружения как неправильной настройки механизмов, реализующих другие ФТБ, так и направленных на них нападений.

Для предотвращения обхода механизмов, реализующих ФТБ, в ПЗ обычно включается компонент FPT_RVM «Невозможность обхода ПБО».

Если реализация функциональных требований безопасности включает 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:
а) 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»;
б) 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. Подобные атаки могут быть предотвращены посредством выполнения следующих ФТБ:
а) ФТБ на основе компонентов семейства FPT_SEP «Разделение домена», которые направлены на предотвращение вмешательства посторонних или воздействия недоверенных субъектов;
б) ФТБ на основе компонентов семейства FPT_PHP «Физическая защита ФБО», которые направлены на обнаружение и противодействие физическому вмешательству;
в) ФТБ, базирующихся на компонентах управления безопасностью, таких как FMT_MSA.1 «Управление атрибутами безопасности», которые ограничивают возможность изменения данных конфигурации или атрибутов безопасности;
г) ФТБ, базирующихся на таких компонентах, как FMT_MTD.1 «Управление данными ФБО» или FAU_STG.1 «Защищенное хранение данных аудита», которые направлены на защиту целостности критичных по безопасности данных;
д) компонентов семейства FPT_TRP «Доверенный маршрут», которые направлены 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. Пример, где возможна деактивация – аудит безопасности; семейство FAU_STG «Хранение событий аудита безопасности» включает 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 аудит безопасности, обеспечивают поддержку других ФТБ, способствуя обнаружению атак или неправильной конфигурации, которая делает ОО уязвимым для атак. Другие функции обнаружения включают компоненты семейств FDP_SDI «Целостность хранимых данных» и FPT_PHP «Физическая защита ФБО».

13. Обоснование ЗБ

Настоящая глава представляет собой руководство по формированию раздела «Обоснование ЗБ». «Обоснование ЗБ» должно показать, что все аспекты среды безопасности (в соответствии с разделом «Среда безопасности ОО») надлежащим образом учтены, и что цели безопасности для ОО надлежащим образом удовлетворяются идентифицированными требованиями безопасности ИТ, которые, в свою очередь, надлежащим образом удовлетворяются функциями безопасности ИТ и мерами доверия к безопасности ИТ. «Обоснование ЗБ» во многом схоже с «Обоснованием ПЗ», но дополнительно включает обоснование содержания краткой спецификации ОО, показывая, что она подходит для удовлетворения требований безопасности.

Как и в случае с «Обоснованием ПЗ», «Обоснование ЗБ», вероятно, будет наиболее интересно оценщику ЗБ, хотя содержание «Обоснования ЗБ» может быть полезно и для других пользователей ЗБ.

На рисунке 7–представлены специфические для ЗБ аспекты «Обоснования ЗБ».

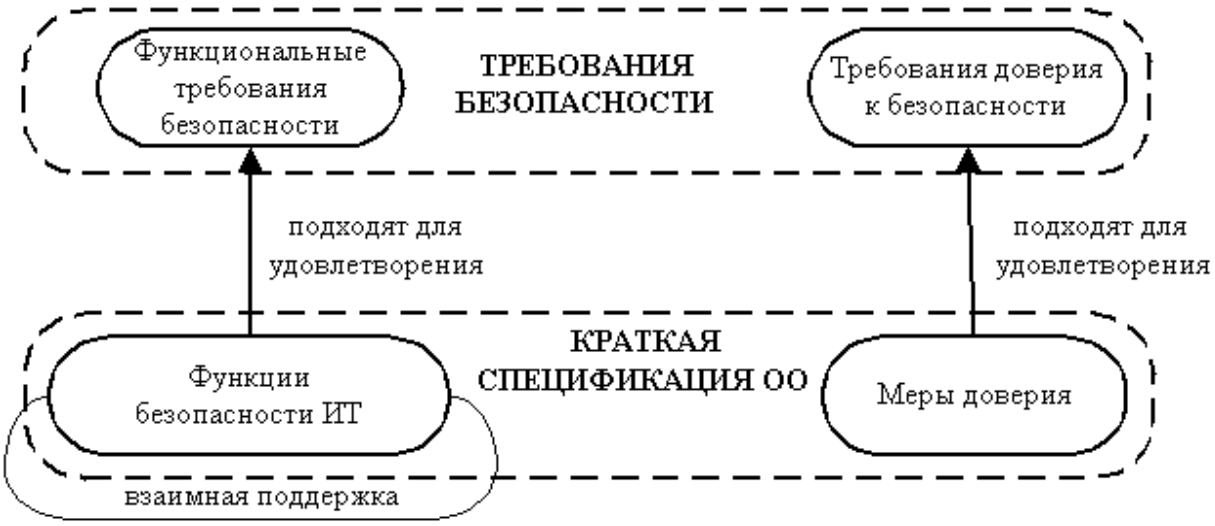

Рисунок 7–Специфические для ЗБ аспекты раздела «Обоснование»

Дополнительно раздел ЗБ «Обоснование» должен показывать, что все требования согласованности с ПЗ выполняются (в соответствии с ASE_PPC.1).

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 тех аспектах, которые не были включены в ПЗ. Если ЗБ не требует согласования с каким-либо ПЗ, то необходимо разработать полное «Обоснование ЗБ» с учетом рекомендаций из главы 12.

По аналогии с разделом ПЗ «Обоснование», для представления раздела ЗБ «Обоснование» рекомендуется использовать соответствующие таблицы, сопровождаемые, где необходимо, неформальными объяснениями.

13.1 Представление логического обоснования целей безопасности в задании по безопасности

Данная часть раздела ЗБ «Обоснования» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.1). Если в ЗБ заявляется о соответствии ПЗ, то рассматриваемая часть «Обоснования ЗБ» должна учитывать только отличия от ПЗ, демонстрируя следующее:

а) при формулировке целей безопасности учтены все дополнительные угрозы;

б) при формулировке целей безопасности учтены все дополнительные правила ПБОр;

в) каким образом дополнительные цели безопасности учитывают соответствующие угрозы и/или правила ПБОр.

13.2 Представление логического обоснования требований безопасности в задании по безопасности

Данная часть «Обоснования ЗБ» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.2.1). Если в ЗБ заявляется о соответствии ПЗ, то рассматриваемая часть «Обоснования ЗБ» должна учитывать только отличия от ПЗ, демонстрируя следующее:

а) при формулировке ФТБ учтены все дополнительные цели безопасности;

б) каким образом дополнительные ФТБ учитывают соответствующие цели безопасности.

13.2.1 Демонстрация пригодности требований доверия к безопасности

Данная часть «Обоснования ЗБ» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.2.2). Если в ЗБ заявляется о соответствии ПЗ, но определены расширенные требования доверия к безопасности, то должна быть обоснована их необходимость и пригодность. При формировании раздела «Обоснование ЗБ» необходимо учитывать все изменения среды безопасности и целей безопасности.

13.2.2 Демонстрация приемлемости требований к стойкости функций безопасности

Данная часть «Обоснования ЗБ» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.2.3).

13.2.3 Демонстрация удовлетворения зависимостей требований доверия к безопасности

Данная часть «Обоснования ЗБ» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.2.4). Если в ЗБ заявляется о соответствии ПЗ, то рассматриваемая часть «Обоснования ЗБ» должна учитывать только отличия от ПЗ и показывать, что все зависимости дополнительных ФТБ и ТДБ удовлетворены.

13.2.4 Демонстрация взаимной поддержки требований

Данная часть «Обоснования ЗБ» должна формироваться на основе рекомендаций, приведенных в предыдущем разделе для «Обоснования ПЗ» (см. п. 12.2.4). Если в ЗБ заявляется о соответствии ПЗ, то рассматриваемая часть «Обоснования ЗБ» должна учитывать только отличия от ПЗ и показывать, каким образом дополнительные требования безопасности:
а) поддерживаются другими требованиями безопасности ИТ;
б) поддерживают другие требованиями безопасности ИТ;
в) не противоречат другим требованиям безопасности ИТ.

13.2.5 Демонстрация соответствия задания по безопасности профилям защиты

В данной части «Обоснования ЗБ» необходимо идентифицировать профили защиты, соответствие которым требуется для ЗБ, и показать, что:
а) все цели безопасности, сформулированные в профилях защиты, включены в задание по безопасности, а все уточнения целей безопасности обоснованы;
б) все требования безопасности, сформулированные в профилях защиты,

включены в задание по безопасности, а все уточнения или другие операции над требованиями безопасности из ПЗ обоснованы;
в) 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 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.

13.2.6 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 виде таблицы. Из таблицы должно следовать, что:
а) каждое ФТБ отображено, по крайней мере, на одну функцию безопасности ИТ;
б) каждая функция безопасности ИТ отображена, по крайней мере, на одно ФТБ.

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

13.2.7 Демонстрация взаимной поддержки функций безопасности

Назначение данной части «Обоснования ЗБ» заключается в том, чтобы показать, что функции безопасности ИТ полны и внутренне непротиворечивы. При этом для демонстрации полноты и внутренней непротиворечивости функций безопасности ИТ необходимо показать, что они являются взаимно поддерживающими и представляют собой «интегрированное эффективное целое». Такой анализ выполняется

аналогично демонстрации взаимной поддержки ФТБ. Рассматриваемый анализ должен учесть влияние дополнительных деталей, введенных в спецификации функций безопасности ИТ по сравнению с соответствующими ФТБ. При этом должны быть даны пояснения относительно взаимной поддержки и взаимосвязей функций безопасности ИТ, связанных со введением в ЗБ таких дополнительных деталей.

13.2.8 Демонстрация соответствия мер доверия к безопасности требованиям доверия к безопасности

Назначение данной части «Обоснования ЗБ» заключается в том, чтобы показать, что изложенные меры доверия к безопасности надлежащим образом отвечают требованиям доверия к безопасности. Предлагаемый подход к решению данной задачи предусматривает представление отображения мер доверия к безопасности на требования доверия к безопасности, с тем, чтобы показать, что каждое требование доверия к безопасности учтено. Если конкретные меры доверия к безопасности идентифицированы (см. п. 11.3), то рассматриваемое отображение лучше всего может быть представлено в виде таблицы. Эта таблица должна сопровождаться кратким пояснением того, каким образом 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, когда ЗБ включает ТДБ, которые требуют применения конкретных методов, предполагающих высокий уровень доверия к безопасности (например, анализ скрытых каналов или использование формальных методов).

14. Профили защиты и задания по безопасности для составных ОО и ОО, входящих в состав других ОО

Настоящая глава содержит рекомендации по решению конкретных проблем, связанных со следующими случаями композиции:
а) ПЗ и ЗБ формируются 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);
б) ПЗ и ЗБ формируются для ОО-компонента, в которых определяются зависимости от ИТ-среды, которая включает 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, например:
а) 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.
б) 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 количество компонентов. Выбор наилучшего способа декомпозиции составного ОО на ОО-компоненты в целях последующего формирования ПЗ или ЗБ ОО-компонентов возлагается на разработчика ПЗ/ЗБ.

14.1 Составной объект оценки

14.1.1 Описательные части профиля защиты и задания по безопасности

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

14.1.2 Среда безопасности ОО

Раздел ПЗ или ЗБ составного ОО «Среда безопасности ОО» может:
а) либо целиком определять среду безопасности для составного ОО (посредством ссылки на один или более ПЗ, соответствие которым заявляется, с включением дополнительных подробностей, где это необходимо);
б) либо 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 описанных подходов предпочтителен в случае, когда 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. Он также целесообразен, когда разным подмножествам компонентов составного ОО соответствуют разные подмножества активов, подлежащих защите. В этом случае их полное описание в ПЗ/ЗБ составного ОО было бы чрезвычайно сложным, а, следовательно, трудным для понимания пользователем ПЗ/ЗБ. Поэтому описание подлежащих защите активов и источников угроз предпочтительнее помещать в ПЗ или ЗБ ОО-компонентов.

Необходимо отметить, что согласно ОК, если ОО является физически распределенным, может возникнуть необходимость (в целях 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/ЗБ составного ОО и ПЗ/ЗБ ОО-компонентов.

14.1.3 Цели безопасности

Изложение целей безопасности целесообразно осуществить в ПЗ/ЗБ ОО-компонентов. При этом нет необходимости повторять полные формулировки этих целей безопасности в ПЗ/ЗБ составного ОО, однако в ПЗ/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.

14.1.4 Требования безопасности

Изложение требований безопасности ИТ целесообразно осуществлять в ПЗ/ЗБ ОО-компонентов. При этом нет необходимости приводить полные формулировки этих требований в ПЗ/ЗБ составного ОО. Тем не менее, в

ПЗ/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/ЗБ составного ОО, а в ПЗ/ЗБ ОО-компонентов поместить ссылки на эти требования.

В тех случаях, когда ОО-компоненты имеют различные уровни доверия к безопасности, для ПЗ/ЗБ составного ОО может быть сформирован «профиль доверия к безопасности». Это может быть целесообразно, например, тогда, когда какой-либо ОО-компонент предназначен для защиты особо ценных либо наиболее привлекательных для нарушителя активов. Такой подход в явном виде не противоречит ОК, но при этом необходимо контролировать, чтобы в ПЗ/ЗБ не было ситуаций, 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/ЗБ составного ОО специфицирует «профиль доверия к безопасности», то нет необходимости определять общий уровень доверия к безопасности, за исключением, может быть, указания на минимальный уровень доверия к безопасности ОО-компонентов.

Целесообразно при разработке многокомпонентных систем минимизировать количество 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 количества ОО-компонентов с высокими требованиями доверия к безопасности. (Пример – изоляция главного ключа центра сертификации.)

При формировании ПЗ/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/ЗБ составного ОО должен идентифицировать все неудовлетворенные зависимости (если таковые имеются), которые должны быть удовлетворены ИТ-средой составного ОО (если такая ИТ-среда существует).

14.1.5 Краткая спецификация ОО

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.

14.1.6 Обоснование ПЗ

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 подходят для того, 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 показать, 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, которые определены в ПЗ ОО-

компонентов как подлежащие удовлетворению ИТ-средой, либо 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 которые 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.

14.1.7 Обоснование ЗБ

Рекомендации по формированию раздела ЗБ «Обоснование» во многом подобны рекомендациям по формированию раздела «Обоснование» ПЗ составного ОО (см. п. 14.1.6). В частности:
а) 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;
б) 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.

14.2 ОО-компонент

14.2.1 Описательные части ПЗ и ЗБ

Если ОО представляет собой компонент составного ОО, то на это должно быть ясно указано в описательных частях ПЗ/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 все 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.

14.2.2 Среда безопасности ОО

Раздел ПЗ/ЗБ «Среда безопасности ОО» предназначен для того, чтобы определить границы среды безопасности ОО-компонента, и, с точки зрения оценщика – границы оценки ОО-компонента. Например, среда безопасности ИТ для ОО-компонента может включать, 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/ЗБ.

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

14.2.3 Цели безопасности

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

Заметим, 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.

14.2.4 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.

14.2.5 Краткая спецификация ОО

В качестве 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.

14.2.6 Обоснование ПЗ

Если в ПЗ определяются требования безопасности для ИТ-среды, то они должны быть рассмотрены в разделе ПЗ «Обоснование». В частности необходимо:
а) продемонстрировать каким образом требования безопасности для ИТ-среды способствуют удовлетворению целей безопасности для ОО;
б) показать, что все зависимости требований безопасности для ИТ-среды удовлетворены;
в) продемонстрировать взаимную поддержку требований безопасности для ИТ-среды и показать поддержку с их стороны по отношению к требованиям безопасности ИТ.

14.2.7 Обоснование ЗБ

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. п.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

Данная глава Руководства содержит методические рекомендации по формированию пакетов требований безопасности. Концепция пакета представлена в п. 4.4.2.1 части 1 ОК. Пакет можно охарактеризовать следующим образом:
а) пакет представляет собой промежуточную комбинация функциональных компонентов или компонентов требований доверия к безопасности;

б) пакет предназначен для многократного использования при создании более крупных пакетов, профилей защиты и заданий по безопасности;
в) пакет предназначен для определения требований безопасности, которые считаются подходящими для удовлетворения определенного подмножества целей безопасности.

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

Оценочные уровни доверия к безопасности, определенные в главе 6 части 3 ОК, необходимо рассматривать как пример оформления пакетов требований доверия к безопасности.

15.1 Формирование функционального пакета

15.1.1 Разработчики функциональных пакетов

В качестве разработчика функционального пакета может выступать любая организация, заинтересованная в продвижении стандартизованной спецификации функциональных возможностей обеспечения безопасности. Разработка функционального пакета может рассматриваться либо как первый шаг при формировании профиля защиты (или семейства ПЗ), либо как составная часть ЗБ.

Функциональный пакет может, например, быть использован организацией для спецификации стандартного набора функциональных требований безопасности, которые должны удовлетворить разработчики изделия ИТ.

15.1.2 Содержимое функционального пакета

Функциональный пакет представляет собой спецификацию функциональных требований безопасности. Для формулирования данных ФТБ необходимо использовать рекомендации п.10.1 настоящего Руководства. Отдельные ФТБ, входящие в функциональный пакет, должны либо идентифицировать стандартизованные функциональные компоненты из ОК, либо представлять собой требования, сформулированные в явном виде и по форме представления соответствующие оформлению компонентов требований в ОК. 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.

Кроме собственно функциональных требований, в ФП следует включать следующую информацию, представляющую интерес при разработке больших ФП, ПЗ и ЗБ:
а) идентификацию целей безопасности, которым удовлетворяют ФТБ;
б) информацию об использовании функциональных компонентов из ОК или об отклонениях от ОК;
в) обоснование ФТБ, включая:
– демонстрацию адекватности ФТБ для удовлетворения идентифицированных целей безопасности;
– анализ зависимостей между ФТБ;
– 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 ОК. 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, которая бы была полезной при формировании обоснований ПЗ или ЗБ.

15.2 Спецификация пакета требований доверия к безопасности

15.2.1 Разработчики пакетов требований доверия к безопасности

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

15.2.2 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 п.10.2 настоящего Руководства. Отдельные ТДБ, входящие в ПД, должны либо

идентифицировать стандартизованные компоненты доверия к безопасности, определенные в части 3 ОК, либо представлять собой требования, сформулированные в явном виде и по форме представления соответствующие оформлению компонентов требований в ОК. При этом сформулированные в явном виде требования должны сопровождаться четким обоснованием того, почему их было необходимо формулировать в явном виде.

В целях многократного использования ПД должен включать 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 ОК, необходимо рассматривать в качестве образца представления пакетов требований доверия к безопасности.

Приложение 1. Резюме

Данное приложение содержит описание ключевых вопросов, изложенных в главах 7–13 настоящего Руководства.

П1.1. Введение ПЗ/ЗБ

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

П1.2. Описание ОО

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

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

В раздел ЗБ «Описание ОО» описание «границ ОО» включается 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/ЗБ.

П1.3. Среда безопасности ОО

П1.3.1. Предположения безопасности

Идентификация

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

Спецификация

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

Представление

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

П1.3.2. Угрозы

Идентификация

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

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/ЗБ не рекомендуется включать описание угроз, связанных с недостатками в реализации ОО.

Представление

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

П1.3.3. Политика безопасности организации

Идентификация

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

Спецификация

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

Представление

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

П1.4. Цели безопасности

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.

Спецификация

При изложении целей безопасности для ОО необходимо установить (в заданном разработчиком ПЗ/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 другой 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.

Представление

Для упрощения ссылок необходимо, чтобы каждая цель безопасности имела уникальную метку.

П1.5. Требования безопасности ИТ

П1.5.1. Функциональные требования безопасности ОО

Идентификация

В первую очередь необходимо идентифицировать основные ФТБ, которые непосредственно удовлетворяют 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 части 2 ОК. Некоторые зависимости могут быть оставлены неудовлетворенными. При этом необходимо дать объяснение, почему соответствующие ФТБ не используются для удовлетворения целей безопасности.

Спецификация

Необходимо осуществить выбор уровня аудита безопасности, исходя из следующих основных факторов:
- значимости аудита безопасности для достижения целей безопасности;
- технической реализуемости.

Необходимо использовать операцию «итерация» в случае необходимости неоднократного использования функционального компонента, определенного в части 2 ОК.

В ПЗ необходимо осуществить полное либо 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 тех случаях, когда замена общего термина (например, атрибут безопасности) на специфический для рассматриваемого ОО термин делает соответствующие ФТБ более читабельными и понятными.

Представление

Рекомендуется в ПЗ/ЗБ результаты выполнения операций выделять курсивом (либо каким-либо другим 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 части 2 ОК.

Для маркировки ФТБ в ПЗ/ЗБ совсем не обязательно использовать систему маркировки компонентов, принятую в части 2 ОК. Для этих целей разработчик ПЗ/ЗБ может использовать свою собственную систему маркировки ФТБ (например, на основе более информативных меток). При использовании собственной системы маркировки ФТБ разработчик ПЗ/ЗБ должен представить (например, в приложении к ПЗ/ЗБ) отображение представленных в ПЗ/ЗБ ФТБ на соответствующие функциональные компоненты, определенные в части 2 ОК.

П1.5.2. Требования доверия к безопасности ОО

Идентификация

Выбор требований доверия к безопасности необходимо осуществлять с учетом следующих основных факторов:
а) ценности активов, подлежащих защите, и осознаваемого риска их компрометации;
б) технической реализуемости;
в) стоимости разработки и оценки;
г) требуемого времени для разработки и оценки ОО.

П1.5.3. Требования безопасности для ИТ-среды

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).

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.

П1.6. Краткая спецификация ОО (только для ЗБ)

П1.6.1. Функции безопасности ОО

Идентификация

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

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.

П1.6.2. Меры доверия к безопасности

Идентификация

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.

П1.7. Обоснование ПЗ

П1.7.1. Логическое обоснование целей безопасности

Необходимо продемонстрировать (табличным 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.

П1.7.2. Логическое обоснование требований безопасности

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

Необходимо продемонстрировать взаимную поддержку ФТБ следующим образом:

а) показать, что, где необходимо, зависимости компонентов требований безопасности удовлетворены;

б) показать, что ФТБ являются согласованными (не противоречат друг другу);

в) показать, что, где необходимо, включены поддерживающие ФТБ, предназначенные для защиты механизмов безопасности, реализующих

другие ФТБ, от нападений типа «обход», «несанкционированное изменение» и «деактивация».

П1.8. Обоснование ЗБ

П1.8.1. Логическое обоснование целей и требований безопасности

Формирование данных подразделов «Обоснования» в ЗБ аналогично формированию соответствующих подразделов «Обоснования» в ПЗ (см. п. П1.7).

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.

П1.8.2. Логическое обоснование краткой спецификации ОО

Необходимо продемонстрировать (табличным 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 2. Примеры угроз, политики безопасности организации, предположений безопасности, целей безопасности, требований безопасности

В данном Приложении приведены примеры угроз, ПБОр, предположений безопасности, целей безопасности в форме, рекомендуемой для ПЗ/ЗБ. Кроме того, Приложение содержит рекомендации по выбору функциональных компонентов, описанных в части 2 ОК, для спецификации характерных требований безопасности.

Формулировки угроз, ПБОр, предположений безопасности, целей и требований безопасности из данного Приложения могут быть адаптированы для использования в конкретных ПЗ/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/ЗБ, соответствующий текст выделен курсивом.

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

П2.1. 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 тайному каналу) секретную 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 должны 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.

П2.2. 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:
а) идентификационной информации владельца объекта;
б) идентификационной информации субъекта, осуществляющего доступ;
в) явных и неявных прав доступа к объекту, предоставленных субъекту владельцем данного объекта.

ПБОр на основе мандатного принципа управления доступом (P.MAC) – право доступа к информации, маркированной по степени секретности (уровню конфиденциальности), определяется следующим образом:
а) данному лицу разрешен доступ к информации, только если оно имеет соответствующий допуск;
б) данное лицо не может изменять обозначение степени секретности (уровня конфиденциальности) информации в сторону снижения, если у него нет явных полномочий на выполнение таких действий.

Для каждой конкретной организации может потребоваться большая степень детализации ПБОр, чем в приведенных примерах.

П2.3. Примеры предположений безопасности

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

П2.3.1. 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.

П2.3.2. 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.

П2.3.3. 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 таким образом, 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.

П2.4. Примеры целей безопасности для ОО

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 предусматривать средства управления и ограничения доступа к объектам и ресурсам, по отношению к которым они являются владельцами или ответственными; по отдельным пользователям или идентифицированным группам пользователей – 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 (проверки полномочий информации) по отношению к информации, и маркировки секретности (конфиденциальности) 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 недоверенных субъектов или от попыток недоверенных 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 (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.

П2.5. Примеры целей безопасности для среды

В данном подразделе 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:
а) должны быть предприняты соответствующее действия (меры) для того, чтобы гарантировать непрерывное ведение журналов аудита, например, путем регулярного архивирования файлов регистрационных журналов перед очисткой журналов аудита с тем, чтобы обеспечить достаточное свободное пространство (на диске).
б) журналы аудита следует регулярно проверять и принимать соответствующие меры по обнаружению нарушений безопасности или событий, которые, по всей видимости, могут привести к таким нарушениям в будущем.

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 таким образом, что после отказа системы или другой неисправности восстановление системы достигается без ущерба для безопасности ИТ.

П2.6. Пример демонстрации соответствия целей безопасности и угроз

В представленной ниже таблице приведен пример демонстрации соответствия целей безопасности и угроз. Сами же формулировки и угроз, и целей безопасности не всегда соответствуют формулировкам, приведенным выше.

Таблица П2.1

Пример демонстрации 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

Данные на носителях	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.
	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.)
Данные на носителях		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.
Данные на носителях		Реагирование	Восстановление секретного ключа шифрования.
	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 в телекоммуникационных линиях	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	Предупрежде	Установка резервных

	заблокирована из-за повреждения линии.	ние	телекоммуникационных линий. Контроль качества телекоммуникационных линий
		Обнаружение	Обнаружение повреждений (средствами ОС).
		Реагирование	Повторная передача данных.
	Связь заблокирована из-за аномалий в канале связи	Предупреждение	Установка резервных каналообразующих устройств.Контроль качества каналов связи.
		Обнаружение	Обнаружение отказов (средствами ОС).
		Реагирование	Повторная передача данных.
	Несанкционированная повторная передача данных в неразрешенный адрес.	Предупреждение	Управление эксплуатацией системы коммутации (например, наложение ограничений на регистрацию программ)
		Обнаружение	Предотвращение повторной передачи (путем использования порядковых номеров или временных меток).
Прикладные программы (приложения)	Выполнение приложения неуполномоченным лицом.	Предупреждение	Управление правами на выполнение программы.Управление эксплуатацией системы коммутации (ограничение числа дисплеев отображения работы программ).Управление расположением и маршрутом выполнения программ.Обеспечение безопасности в момент

			отсутствия оператора.Наложение ограничений на использование терминалов приложений.
		Обнаружение	Аудит выполнения программ.
		Реагирование	Резервирование / восстановление данных.
	Обращение к данным в библиотеке программ, модификация или удаление данных в библиотеке программ неуполномоченным лицом.	Предупреждение	Управление правами доступа к библиотекам программ.Управление функционированием (ограничение использования команд модификации).Ограничение использования терминалов.
		Обнаружение	Аудит функционирования
		Реагирование	Резервное копирование/восстановление программ
	Незаконное использование программы или затруднение ее использования путем изменения ее атрибутов доступа неуполномоченным лицом.	Предупреждение	Управление правами на выполнение программы.Управление правами на доступ к каталогу библиотеки программ. Управление функционированием (ограничение использования команд модификации)
		Обнаружение	Аудит функционирования
Прикладные программы (приложения)	Аномалии в ходе выполнения программы из-за аппаратного отказа компьютера.	Предупреждение	Использование аппаратной конфигурации с дублированием. Контроль качества аппаратных средств.
		Обнаружение	Обнаружение

			недостатков (средствами ОС)
		Реагирование	Восстановление работоспособности аппаратного обеспечения.
Прикладные процессы и данные	Несанкционированное использование прикладных процессов (например, запросов по Telnet и FTP).	Предупреждение	Управление правами на выполнение программ.Использование межсетевых экранов (фильтров прикладного уровня).Использование инструкций по эксплуатации.
		Обнаружение	Аудит выполнения программ
	Блокировка прикладных процессов (атаки, направленные на переполнение трафика, например, запросы на обработку потока ненужных данных)	Предупреждение	Назначить приоритеты обработки процессов.Запретить передачу электронной почты.
		Обнаружение	Аудит сетевого доступа.
	Отрицание факта обмена данными или отрицание их содержания	Предупреждение	Принятие мер, препятствующих отказу (например, сохранение доказательств, используя третью доверенную сторону или функцию шифрования). Использование инструкций по эксплуатации.
	Отказ от авторства данных.	Предупреждение	Использование удостоверяющих сервисов (например, подтверждения авторства)Использование

			инструкций по эксплуатации
Прикладные процессы и данные	Несанкционированная передача данных	Предупреждение	Управление потоками данных (например, использование межсетевого экрана и применение правил базы данных).Контроль качества прикладных программ.Управление функционированием (например, наложение ограничений на регистрацию программ)
		Обнаружение	Аудит доступа к данным.
	Несанкционированное использование данных или программ путем использования оставшихся в программах отладочных функций	Предупреждение	Управление правами на доступ к данным и на выполнение программ. Управление функционированием (например, ограничение возможности использовать функцию отладки).
		Обнаружение	Аудит выполнения прикладной программы
	Необоснованный отказ от предоставления услуги	Предупреждение	Назначение приоритетов обработки процессов. Контроль качества прикладных программ.Обучение и обеспечение инструкциями эксплуатационного персонала.Контроль качества аппаратных средств обработки данных.Оценка производительности ресурсов обработки данных.
		Обнаружение	Аудит выполнения

			прикладной программы
	Незаконное умышленное изменение, искажение, похищение, удаление или разрушение данных.	Предупреждение	Управление правами на использование данных.Управление созданием и пересылкой данных
		Обнаружение	Обнаружение изменений данных
		Реагирование	Резервное копирование данных.
Прикладные процессы и данные	Несанкционированное выполнение операций	Предупреждение	Управление правами на выполнение операций.Контроль места выполнения операций (удаленный, через Интернет и т.д.)
		Обнаружение	Аудит выполнения операций
	Нарушение конфиденциальности	Предупреждение	Управление правами на использование конфиденциальной информации.Анонимность и использование псевдонимов.Обеспечение правильности завершения сеанса обработки данных.
Отображаемые данные	Просмотр данных неуполномоченным лицом.	Предупреждение	Физическая защита (изоляция) дисплея.Обеспечение выполнения требований эксплуатационной документации.
	Несанкционированное копирование или печать	Предупреждение	Обеспечение защиты во время отсутствия уполномоченного лица. Ограничение использования функций копирования и печати.Обеспечение выполнения требований эксплуатационной

			документации.
		Обнаружение	Контроль подлинности (электронные метки).
Вводимые данные	Данные раскрыты во время ввода	Предупреждение	Контроль доступа в помещение, в котором расположен терминал ввода информации.Обеспечение выполнения требований эксплуатационной документации.
	Введенные данные несанкционированно изъяты (или удалены).	Предупреждение	Контроль носителя, на котором хранятся введенные данные.Обеспечение выполнения требований эксплуатационной документации
		Реагирование	Резервное копирование вводимых данных.
Данные, выводимые на печать	Ознакомление или изъятие данных неуполномоченным лицом.	Предупреждение	Физическая защита печатаемых данных.Обеспечение выполнения требований эксплуатационной документации
	Несанкционированное копирование	Предупреждение	Защита от копирования.Обеспечение выполнения требований эксплуатационной документации.
		Обнаружение	Контроль подлинности(электронная метка)
Данные пользователей	Пользователь (человек, система, терминал) не может быть идентифицирован	Предупреждение	Идентификация доступа.Идентификация (назначение идентификатора каждому пользователю/систе-ме;

			IP-адрес).Ограничение рабочих мест
		Обнаружение	Аудит выполнения идентификации.
	Маскировка путем использования раскрытой идентификационной информации пользователя (человека, системы, терминала).	Предупреждение	Аутентификация пользователя.Контроль идентификационной информации.
		Обнаружение	Аудит выполнения идентификации
	Пользователь не идентифицирован.	Предупреждение	Безотлагательная аутентификация (аутентификация до любых действий пользователя).Надежная идентификация.Аутентификация на основе секретного ключа, пароля, биометрических характеристик.Аутентификация с обратной связью
		Обнаружение	Аудит выполнения аутентификации
Данные пользователей	Маскировка путем использования незаконно раскрытой информации аутентификации.	Предупреждение	Использование нескольких механизмов аутентификации.Управление доступом к серверу (раннее обнаружение атак; регистрация информации о выполнении аутентификации).Защита аутентификационной информации (однонаправленное шифрование). Ограничение путей

			доступа (например, запрет доступа с использованием общих телекоммуникационных линий и Интернет).Использовани е одноразовых паролей
		Обнаружение	Аудит доступа к системе.
		Реагирование	Блокировка работы пользователя.
	Маскировка путем незаконного (логического) вывода аутентификацион ной информации.	Предупрежде ние	Аутентификация (предотвращение логического вывода).Управление доступом к серверу (раннее обнаружение атак; обеспечение невозможности получения доступа к серверу на длительный период).Использование нескольких механизмов аутентификации.Управле ние 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.Минимизац ия 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.
Данные пользователей	Использование недействительного права из-за сбоя журнала регистрации прав пользователей	Предупреждение	Контроль за пользователями (безотлагательное отражение модификации прав пользователей).
		Обнаружение	Аудит доступа к системе.
	Действия пользователя несанкционированно раскрыты (нарушение конфиденциальности).	Предупреждение	Управление правами доступа к регистрационной информации, имеющей отношение к пользователям. Анонимность и использование псевдонимов.Обеспечение правильности завершения сеанса обработки данных.
		Обнаружение	Аудит доступа к системе.
	Отрицание факта передачи данных	Предупреждение	Предотвращение отказа от факта передачи данных. Обеспечение выполнения требований эксплуатационной документации.
		Обнаружение	Аудит обмена данными.
	Отрицание владения данными.	Предупреждение	Автоматическая регистрация владельца в процессе формирования данных.
		Обнаружение	Аудит доступа к системе.
	Отрицание факта	Предупрежде	Предотвращение отказа

	приема данных.	ние	от факта приема данных.Обеспечение выполнения требований эксплуатационной документации.
		Обнаружение	Аудит обмена данными.
	Данные посланы несоответствующему получателю вследствие его маскировки под авторизованного пользователя или ошибки спецификации	Предупреждение	Аутентификация адресата.Обеспечение выполнения требований эксплуатационной документации
		Обнаружение	Аудит обмена данными.
	Маскировка путем подделки информации аутентификации	Предупреждение	Управление правами доступа к аутентификационной информации.Проверка достоверности аутентификационной информации.Управление аутентификационной информацией (например, предотвращение фальсификации, надежная организация процесса аутентификации, физическая защита устройств аутентификации).
		Обнаружение	Управление доступом к серверу (раннее обнаружение атак)
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).
Системные службы и данные	Нарушение безопасности системы вследствие несанкционированного действия или ошибки уполномоченного пользователя.	Предупреждение	Предотвратить ошибки уполномоченного пользователя (например, путем использования запросов подтверждения выполняемых действий).Управление правами пользователя (назначение минимально необходимых прав).Управление аудитом, разработка инструкций, повышение квалификации пользователей и применение штрафов.
		Обнаружение	Аудит функционирования системы.
	Внедрение вирусов	Предупреждение	Проверка на отсутствие вирусов в полученных программах, а также файлах, присоединенных к сообщениям, поступающим по электронной почте.Управление доступом (назначение соответствующих прав

			доступа и защита файлов).Запрет использования данных или программ, полученных извне.Контроль инсталляции программ
		Обнаружение	Аудит работы системы
		Реагирование	Выполнение необходимых ответных действий (например, остановка системы или отключение от внешней системы).
Системные службы и данные	Несанкционированное проникновение в систему.	Предупреждение	Идентификация, аутентификация и подтверждение прав пользователей (авторизация) при доступе в систему.Управление конфигурацией системы (например, подключением оборудования и внешними соединениями).Управление пользователями.
		Обнаружение	Аудит функционирования системы.
	Проникновение в систему, используя известные дефекты протоколов (например, протокола IP).	Предупреждение	Использование межсетевых экранов (фильтрация).Контроль доступа к системным ресурсам.Ограничение доступа к программам или сервисам, реализующим уязвимые протоколы.
		Обнаружение	Аудит функционирования

			системы
	Нарушение безопасности системы вследствие несанкционированной замены системной программы.	Предупреждение	Контроль доступа к библиотеке системных программ.Управление функционированием (разработка документации по использованию системных программ)
		Обнаружение	Аудит доступа к библиотеке программ.
		Реагирование	Резервное копирование программ.
	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.

П2.7. Примеры функциональных требований безопасности

Данный подраздел в качестве примера идентифицирует функции безопасности, функциональные компоненты, описанные в части 2 ОК, 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.

П2.7.1. Требования идентификации и аутентификации

Представленная ниже таблица П2.2 охватывает требования идентификации и аутентификации.

Таблица П2.2

Функциональные компоненты для требований идентификации и аутентификации		
Требования безопасности		Функциональные компоненты
Управление доступом в систему (регистрацией)	Идентификация пользователей	FIA_UID.1–2
	Аутентификация пользователей	FIA_UAU.1–2
	Ограничение числа неудачных входов в систему	FIA_AFL.1
	Доверенный маршрут для входа в систему	FTP_TRP.1
	Управление доступом по времени и местоположению	FTA_TSE.1
Выбор паролей	Управление выбором сгенерированных пользователями паролей (например, минимальная длина, фильтры пароля, история пароля)	FIA_SOS.1
	Автоматическая генерация пароля ОО	FIA_SOS.2
	Окончание действия пароля	FMT_SAE.1
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 (т.е. атрибутами безопасности пользователя)	FMT_MTD.1

П2.7.2. Требования управления доступом

Представленная ниже таблица П2.3 охватывает требования управления доступом.

Таблица П2.3

Функциональные компоненты для требований управления доступом		
Требования безопасности		Функциональные компоненты
Дискреционное управление доступом	Область действия политики безопасности (объекты, субъекты и действия, охватываемые политикой)	FDP_ACC.1–2
	Правила управления доступом субъектов к объектам	FDP_ACF.1
	Отмена прав в соответствии с политикой дискреционного управления доступом	FDP_ACF.1

Управление, основанное на атрибутах дискреционного управления доступом	Изменение прав доступа к объекту	FMT_MSA.1
	Задание атрибутов по умолчанию для вновь создаваемых объектов	FMT_MSA.3
	Изменение владельца объекта	FMT_MSA.1
	Изменение принадлежности к группе пользователей	FMT_MSA.1
Мандатное управление доступом	Область действия политики безопасности (объекты, субъекты и действия, охватываемые политикой)	FDP_IFC.1–2
	Правила управления доступом/информа-ционными 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
	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	Область действия политики	FDP_ACC.1–2

управление доступом	безопасности (на основе ролей, операций)	
	Правила контроля выполнения операций	FDP_ACF.1
	Идентификация ролей	FMT_SMR.1–2
	Осуществление управления доступом на основе разделения действий по доступу между несколькими субъектами	FDP_ACF.1FMT_SMR.2.3
Управление на основе атрибутов ролей	Управление полномочиями/авторизацией пользователей	FMT_MSA.1
	Изменение возможностей ролей	FMT_MSA.1
	Изменение ролей пользователей	FMT_MSA.1
Управление доступом на основе межсетевого экрана	Представление информационного потока в виде субъект-объект (например, на основе адресов и портов источника/адресата)	FDP_IFC.1–2FDP_IFF.1
	Представление информационного потока по отношению к сеансу связи (предполагает использование proxy-серверов)	FTA_TSE.1

П2.7.3. Требования аудита

Представленная ниже таблица П2.4 охватывает требования аудита.

Таблица П2.4

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	Генерация сигнала нарушения и ответная	FAU_ARP.1

вторжений и ответная реакция	реакция на неизбежное нарушение безопасности	
	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 от несанкционированного доступа к данным аудита	FAU_STG.1
Анализ журнала аудита	Использование инструментальных средств анализа журналов аудита	FAU_SAR.1–3

П2.7.4. Требования целостности

Представленная ниже таблица П2.5 охватывает требования целостности (включая данные аутентификации).

Таблица П2.5

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

П2.7.5. Требования доступности

Представленная ниже таблица П2.6 охватывает требования доступности.

Таблица П2.6

Функциональные компоненты для требований доступности		
Требования безопасности		Функциональные компоненты
Использованиересурсов	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

П2.7.6. Требования приватности

Представленная ниже таблица П2.7 охватывает требования приватности.

Таблица П2.7

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
	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

П2.7.7. Требования обмена данными

Представленная ниже таблица П2.8 охватывает требования обмена данными.

Таблица П2.8

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 3. Методические рекомендации по формированию профиля защиты межсетевого экрана

П3.1. Введение ПЗ

Введение разрабатывается с учетом рекомендаций главы 7 настоящего Руководства.

П3.2. Описание ОО

В ПЗ представлено общее описание области применения ОО и его функциональных возможностей по обеспечению безопасности (так как единственное назначение ОО – обеспечение безопасности). Более детально это представлено в ЗБ, в частности:
а) идентификация операционной системы, под управлением которой работает межсетевой экран, и аппаратной платформы;
б) 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).

П3.3. Среда безопасности ОО

П3.3.1. Предположения безопасности

Для межсетевого экрана может быть определен ряд предположений, связанных с обеспечением эффективности функционирования межсетевого экрана. Например:
а) межсетевой экран должен быть универсальным посредником, так как иначе существует возможность его (межсетевой экран) обойти;
б) 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 либо как цели безопасности для среды, либо как требования безопасности, не относящиеся к ИТ.

П3.3.2. Угрозы

Предполагается, что среда для межсетевого экрана включает частную сеть с одной стороны и потенциально враждебную сеть с другой стороны. 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.

Далее приводится 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:
а) источник угрозы – ***нарушитель из потенциально враждебной (внешней) сети***;
б) активы ИТ, подверженные нападению – это ***хосты (узлы) или другие сервисы частной сети***;
в) 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 на межсетевой экран. Например, следующие:
а) определенные способы атак, применяемые нарушителями из враждебной сети, которым ОО не противостоит, такие как перехват сеанса и поиск (сниффинг) данных;
б) частная сеть может стать уязвимой для атак в результате действий злоумышленников из частной сети;
в) уязвимость частной сети со стороны вирусов, которые могут содержаться во входящем трафике – это также угроза, для противостояния которой межсетевой экран не предназначен;
г) частная сеть может стать уязвимой для атак в результате действия или бездействия администратора межсетевого экрана;
д) частная сеть может стать уязвимой для атак в результате непосредственной физической атаки на межсетевой экран.

Ниже приведена возможная (и 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 динамическая (то есть непрерывно изменяющаяся), а, значит, сам ОО должен изменяться, например, определяя полномочия для новых прикладных программ.

П3.3.3. Политика безопасности организации

Должна существовать возможность настройки межсетевого экрана для реализации ряда различных правил ПБОр. В этом примере мало чего можно достичь формулировкой правил ПБОр, которым должен следовать ОО. Тем не менее можно сформулировать в общих чертах политику управления доступом, которая должна осуществляться межсетевым экраном.

П3.4. Цели безопасности

П3.4.1. Цели безопасности для ОО

Цели безопасности для межсетевого экрана можно сформулировать следующим образом:
а) Цель О1 – 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.
б) Цель О2 – 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.
в) Цель О3 – Точно так же там может существовать требование аутентификации полномочий приложений.
г) Цель О4 – Требование к функциональным возможностям аудита, обеспечивающим средства регистрации событий, относящихся к безопасности.
д) Цель О5 – 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.

Это указывает на то, что в ОО должны быть реализованы функциональные возможности по идентификации и аутентификации. Заметим, что, так как в ПЗ не определяются сервисы, которые необходимо обеспечить, то в цели безопасности не определяется подмножество тех сервисов, которые требуют аутентификации. Данный вопрос оставляется на рассмотрение автору ЗБ, который (в обосновании ЗБ) должен обосновать список сервисов, которые требуют (или могут быть соответствующим образом настроены, чтобы требовать) аутентификации конечного пользователя.

ПЗ.4.2. Цели безопасности для среды

Ниже приводится пример цели безопасности для среды, которая является требованием к использованию функциональных возможностей аудита:

Администраторы межсетевого экрана должны обеспечить эффективное использование и управление средствами аудита. В частности, должны быть выполнены соответствующие действие 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 соответствующие действия должны быть предприняты 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.

П3.5. Требования безопасности ИТ

П3.5.1. Функциональные требования безопасности

Для непосредственного удовлетворения целей безопасности для ОО, описанным в предыдущем разделе, могут быть выбраны следующие ФТБ:
а) Цель безопасности О1 может быть удовлетворена соответствующим использованием либо FDP_ACF.1 (Управление доступом, основанное на атрибутах безопасности) и FDP_ACC.2 (Полное управление доступом), либо FTA_TSE.1 (Открытие сеанса с ОО).
б) Цель безопасности О2 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.
в) Цель безопасности О4 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.
г) Цель безопасности О5 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 выбираются главным образом для того, чтобы удовлетворить зависимости. Дополнительные ФТБ могут быть включены, потому что они обеспечивают полезную (если не существенную) поддержку полномочий; и, например, могут включать 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 целями безопасности для ОО.

Далее необходимо, где требуется, использовать операцию назначения.

П3.5.2. Требования доверия к безопасности ОО

Выбор требований доверия должен быть относительно простым. Если авторы ПЗ/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.

П3.5.3. Требования безопасности для ИТ-среды

Совсем 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 этом случае соответствует выбору требований доверия для ИТ, например, ОУД4.

П3.6. Краткая спецификация ОО

П3.6.1. Функции безопасности ОО

При построении функций безопасности ИТ авторы ЗБ могут начинать с ФТБ и получать функции безопасности ИТ из них следующим образом:
а) следует добавить (где необходимо) определенные детали ОО для того, чтобы конкретизировать функциональные возможности, особенно для функций межсетевого экрана по управлению доступом (главное назначение ОО);
б) 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:

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:

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).

ПЗ.7. Обоснование ПЗ

ПЗ.7.1. Обоснование целей безопасности

Демонстрация пригодности целей безопасности для того, чтобы противостоять угрозам, может быть осуществлена:
а) 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;
б) путем аргументации для каждой угрозы, почему идентифицированные цели безопасности являются соответствующими данной угрозе.

Пример объяснения пригодности дается ниже:

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.

П3.7.2. Обоснование функциональных требований безопасности

Демонстрацию пригодности ФТБ для удовлетворения целей безопасности для ОО можно представить следующим образом:
а) показ посредством таблицы, какие ФТБ 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;
б) обеспечение для каждой цели безопасности для ОО аргументации относительно того, почему идентифицированные ФТБ подходят для удовлетворения цели.

Пример обоснования пригодности дается ниже:

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, что эти функции вызываются 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. Она может сопровождаться объяснением содержания таблицы. Вместо рассмотрения каждого требования по порядку (что ведет к повторам), можно выделить общие вопросы, необходимые для понимания содержания таблицы. Например:

Атаки вмешательства предотвращаются:
– FPT_SEP.3, который поддерживает разделение на домены, и, в частности, предотвращает от вмешательства 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 (т.е. основанные на FMT_MTD.1).

П3.7.3. 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 было бы возможно утверждать, что ОУД4 содержит известный набор взаимно поддерживающих и внутренне непротиворечивых компонентов доверия, для которых все зависимости удовлетворены.

Приложение 4. Методические рекомендации по формированию профиля защиты СУБД

Ключевым звеном обеспечения информационной безопасности вычислительных систем является безопасность общего программного обеспечения, основу которого составляют используемые ОС и СУБД.

Суть предлагаемого методического подхода заключается в формировании требований безопасности СУБД в виде профиля защиты с учетом ограничений безопасности, накладываемых на ОС, под управлением которой работает СУБД.

При этом предполагается, что СУБД предназначена для работы с информацией, для которой необходимо обеспечить конфиденциальность, целостность и доступность на основе дискреционного принципа управления доступом.

Далее рассмотрим процесс формирования основных разделов профиля защиты СУБД.

П4.1. Введение ПЗ

Введение разрабатывается с учетом рекомендаций главы 7 настоящего Руководства.

П4.2. Среда безопасности объекта оценки

П4.2.1. 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 A1. Объект оценки (СУБД) работает под управлением операционной системы, которая установлена и функционирует в безопасном режиме, то есть в соответствии с эксплуатационной документацией данного изделия ИТ.

Предположение A2. Ресурсы ОО и операционной системы, под управлением которой он работает, защищены от несанкционированного физического доступа.

Предположение A3. 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.

П4.2.2. 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 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 таким образом, что ставит 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, гарантирующие то, что пользователи с большими полномочиями являются действительно заслуживающими доверия личностями. С учетом таких процедурных мер и должна быть сформулирована цель безопасности, соответствующая угрозе ТЕ1.

П4.2.3. Политика безопасности организации

В качестве ПБОр для СУБД может быть выбрана, например, следующая:

Политика безопасности Р1. Права доступа к определенным объектам базы данных определяются:
а) владельцем объекта;
б) результатом проверки подлинности субъекта, осуществляющего доступ;
в) правами доступа к объекту, предоставленными субъекту;
г) привилегиями, которыми обладает субъект.

П4.3. Цели безопасности

П4.3.1. Цели безопасности для ОО

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 P1.

Цель O3. Объект оценки должен иметь функции управления использованием общих ресурсов пользователями ОО, в том числе – функции ограничения числа параллельных сеансов.

Цель O1 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.

П4.3.2. Цели безопасности для среды

Анализ угрозы TE1 показывает необходимость формулировки цели безопасности для среды, связанной с проблемой привилегированных пользователей.

Данную цель безопасности можно сформулировать следующим образом:

Цель OE1. Лица, ответственные за эксплуатацию ОО, должны обеспечить проведение соответствующих процедурных и кадровых мероприятий, гарантирующих то, что только доверенным лицам назначены привилегии, позволяющие им:
а) модифицировать данные журнала аудита и настройки аудита;
б) 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 OE2. 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 OE2 определяет потребность (выраженную в предположениях безопасности A1, A2, A3) 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.

П4.4. Требования безопасности ИТ

П4.4.1 Функциональные требования безопасности

Можно выбрать следующие функциональные требования безопасности, непосредственно удовлетворяющие описанные выше цели безопасности для ОО:
а) Цель О1, требующая идентификации пользователей объектом оценки (аутентификация предписана операционной системе), может быть удовлетворена ФТБ, определенными в компонентах FIA_UID.1 «Выбор момента времени идентификации» и FIA_USB.1 «Связи пользователь-субъект».
б) 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».
в) 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 компонент из Части 2 ОК 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 таким образом, чтобы удовлетворить зависимости, установленные в Части 2 ОК, или определить другие сопутствующие функциональные возможности.

Например:
а) 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;
б) 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.
в) компонент FDP_RIP.1 «Ограниченная защита остаточной информации»

нужен, чтобы определить функциональные возможности повторного использования объекта в поддержку политики контроля доступа к базе данных.
г) 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 они (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 (см. п. 7.1.2).

Подходящий уровень выбирается, исходя из целей безопасности для ОО. При этом требование аудита не должно быть необоснованно завышено.

П4.4.2. Требования доверия к безопасности ОО

Требования доверия должны быть сформулированы на основе рассмотрения характера (природы) угроз. Для СУБД, предназначенной для хранения и обработки секретной информации, следует использовать требования доверия не ниже ОУДЗ.

П4.4.3. 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 ОУБЗ.

П4.5. Обоснование ПЗ

П4.5.1. Обоснование целей безопасности

Демонстрация соответствия целей безопасности идентифицированным угрозам может быть выполнена следующим образом:
а) 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;

б) логическим обоснованием того, что цели безопасности противостоят угрозам.

Приведем 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.

П4.5.2. Обоснование функциональных требований безопасности

Демонстрацию соответствия ФТБ целям безопасности для ОО можно представить следующим образом:
а) 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;
б) логическим обоснованием соответствия ФТБ целям безопасности.

Приведем 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.

Приведем пример демонстрации взаимной поддержки требований безопасности.
а) 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;
б) компонент FMT_MSA.1 поддерживает компоненты FRU_RSA.1 и FTA_MCS.1, ограничивая возможности уполномоченного администратора изменять квоты пользователей по использованию ресурсов ОО;
в) компонент FAU_STG.1 «Защищенное хранение журнала аудита» поддерживает компонент FAU_GEN.1, защищая целостность журнала аудита.

П4.5.3. Обоснование требований доверия к безопасности

Формирование этого раздела ПЗ не должно вызвать особых трудностей, если ПЗ ссылается на ОУД3 и в нем отсутствуют другие, более сильные требования доверия к безопасности. В этом случае можно утверждать, что ОУД3 содержит известный набор взаимно поддерживающих и внутренне непротиворечивых компонентов доверия, для которых все зависимости удовлетворены.

Приложение 5. Методические рекомендации по формированию профиля защиты доверенного центра инфраструктуры открытых ключей

Предлагаемый методический подход к формированию ПЗ ДЦ учитывает гибкость набора ФТБ, который зависит от типов сервисов, обеспечиваемых доверенным центром, например:
а) доверенный центр может обеспечивать или не обеспечивать сервисы конфиденциальности;
б) доверенный центр может предоставлять сервисы генерации ключей или может предполагать, что подписчики ДЦ выполняют действия по генерации ключей самостоятельно.

Исходя из этого, необходимо определить набор основных и дополнительных сервисов, предоставляемых ДЦ.

Основные сервисы представляют собой минимум сервисов, обеспечиваемых ДЦ, и относятся к регистрации подписчика, а также к выпуску, распределению, аннулированию и хранению в архиве сертификатов открытых ключей аутентификации.

Дополнительные сервисы ДЦ включают 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 ДЦ могут иметь собственные прикладные программы для выполнения таких функций, как генерация ключей, генерация и верификация цифровой подписи и так далее.

Разработка ПЗ ДЦ с учетом основных и дополнительных сервисов создает проблему совместимости с ОК, так как последний не позволяет задавать спецификацию необязательных требований безопасности в ПЗ.

Альтернативный подход разработки ПЗ для каждой возможной комбинации услуг ДЦ, учитывая множество возможных перестановок, представляется непрактичным.

Разрешение данной проблемы заключается в том, чтобы определить основной набор ФТБ в ПЗ, соответствующий основным сервисам ДЦ.

Кроме того, для каждого дополнительного сервиса может быть определен функциональный пакет для идентификации дополнительных ФТБ, необходимых для поддержки этого сервиса.

Сформированный таким образом ПЗ ДЦ может быть использован следующим образом:
а) при разработке задания по безопасности совместно с одним или более определенных функциональных пакетов в зависимости от услуг, предоставляемых ДЦ;
б) как основа для подготовки других ПЗ с учетом конкретного набора услуг ДЦ; такой ПЗ следует формировать на основе комбинации основного набора ФТБ соответственно с одним или более определенных функциональных пакетов. Данный подход приводит к созданию «семейства» ПЗ ДЦ.

П5.1. Введение ПЗ

Введение разрабатывается с учетом рекомендаций главы 7 настоящего Руководства.

П5.2. Среда безопасности объекта оценки

П5.2.1. Предположения безопасности

Для ДЦ важно, чтобы формулировка предположений относительно безопасности ясно устанавливала возможности и границы ОО.

Желательно, чтобы прикладные программы подписчика ДЦ, используемые для генерации цифровой подписи или для

зашифрования/расшифрования информации, рассматривались как находящиеся вне рамок ОО.

Это приводит к следующим двум предположениям.

Предположение А1. Доверенный центр 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, потому что сертификат, выпущенный ДЦ, был бы девальвирован, если отсутствует доверие к выполнению подписчиком соответствующего алгоритма.

Предположение А2 необходимо для полноты (хотя доверенный центр может поддерживать это предположение, предоставляя соответствующие дополнительные услуги). Таким образом, предположение А2 заключается в том, что описанные функциональные возможности обеспечиваются прикладными программами подписчика, которые не включены в возможности ОО «Доверенный центр».

П5.2.2. Угрозы

Для ДЦ защищаемые активы ИТ – это сертификаты открытых ключей, сгенерированные или сохраненные (например, архивированные) ДЦ вместе с ключами, используемыми или сгенерированными ДЦ.

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 раскрытия. Это могут быть ключи, используемые ДЦ 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 ДЦ, но ключи и сертификаты находятся в его пределах.

Менее поддающийся оценке актив – это репутация организации, непосредственно использующей ДЦ; опять же этот актив также может быть скомпрометирован реализацией угроз по отношению к ключам и сертификатам.

Источниками угроз могут быть как злоумышленники, так и подписчики ДЦ, а также уполномоченные пользователи ОО.

В качестве примера можно привести следующие угрозы, имеющие отношение к основным сервисам ДЦ.

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 ДЦ.

Актив ИТ, подверженный нападению, – это секретный ключ подписчика ДЦ.

Форма нападения выражена термином «раскрыт», что 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 ДЦ.

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 ДЦ) 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 ДЦ.

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 доверенным центром предоставляются дополнительные сервисы по созданию резервных копий ключей или генерации секретных ключей.

П5.2.3. Политика безопасности организации

В качестве ПБОр для ДЦ может быть выбрана следующая.

Политика безопасности Р1. Требуется, чтобы ДЦ соответствовал действующему законодательству и нормативным документам в области информационной безопасности.

П5.3. Цели безопасности

П5.3.1. Цели безопасности для ОО

Цели безопасности для ДЦ делятся на цели безопасности основных и дополнительных сервисов. Цели безопасности для ДЦ 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 ДЦ, предоставляемым подписчикам ДЦ.

Цель безопасности О3 напрямую не относится к основным сервисам ДЦ, но, тем не менее, должна быть удовлетворена для поддержки основного

сервиса – генерации ключей. То есть ДЦ должен быть способен подписывать сертификаты открытых ключей, которые он генерирует.

Другие цели безопасности определяются в целях обеспечения надлежащей защиты активов ДЦ. Эти цели относятся к целям «стандартной операционной системы» по идентификации и аутентификации пользователей ДЦ, контролю доступа и аудиту событий, относящихся к безопасности.

В дополнение к «основному» набору целей безопасности для ОО определяются цели безопасности дополнительных сервисов, например, следующие.

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.

П5.3.2. Цели безопасности для среды

Цели безопасности для среды определяются в случае наличия требований для процедур поддержания целостности функционирования ДЦ.

Цель ОЕ1. Лица, ответственные за эксплуатацию ДЦ, должны обеспечить использование соответствующих сервисов проверки процедур:
а) генерации сертификатов (чтобы гарантировать то, что неправильные данные не помещены в сертификат);
б) верификации сертификата (когда необходимо обеспечить информирование подписчиков ДЦ о положительном результате верификации сертификата).

Цель ОЕ2. Лица, ответственные за эксплуатацию ДЦ, должны обеспечить наличие надлежащих процедур аутентификации подписчиков ДЦ и (при необходимости) третьих лиц.

Цель ОЕ1 необходима для того, чтобы предотвратить компрометацию ДЦ 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.

П5.4. Требования безопасности ИТ

П5.4.1. Функциональные требования безопасности ОО

Первоначально выбираются ФТБ, непосредственно удовлетворяющие целям безопасности для ОО. Например, цель О1 требует, среди прочего, возможность 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. УТОЧНЕНИЕ: сертификаты открытых ключей должны быть сгенерированы в соответствии с определенным стандартом (например. X.509).

ругой 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 доверенному центру возможность верификации сертификатов открытых ключей и идентификатора того ДЦ, который сгенерировал сертификат.

УТОЧНЕНИЕ: верификация сертификата должна включать, как минимум:
а) проверку цифровой подписи;
б) проверку срока действия;
в) проверку параметров аннулирования.

Цель безопасности О3 требует возможности генерации цифровых подписей как доказательство происхождения. Это 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 ДЦ.

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 доверенным центром при [назначение: ограничения на цифровую подпись].

После того, как сформирован начальный набор ФТБ, остальные ФТБ выбираются с тем, 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 ДЦ для подписи сгенерированных сертификатов:

ФТБ6. ФБО должны генерировать пары ключей (открытый/секретный) ДЦ в соответствии с определенным алгоритмом генерации криптографических ключей [назначение: алгоритм генерации криптографических ключей] и определенной длиной криптографических ключей [назначение: длины криптографических ключей], которые удовлетворяют 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 криптографическими алгоритмами [назначение: криптографические алгоритмы] и длиной криптографических ключей [назначение: длины криптографических ключей], которые удовлетворяют следующему: [назначение: список стандартов].

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.

Профиль защиты ДЦ также включает набор функциональных пакетов, определяющих ФТБ, необходимые для поддержания безопасности дополнительных сервисов ДЦ, например, следующие:

ФТБ8. ФБО должны выполнять восстановление ключей в соответствии с указанным методом доступа к криптографическим ключам [назначение: метод доступа к криптографическим ключам], который должен удовлетворять следующему требованию: он должен обеспечить защиту секретной ключевой информации от несанкционированного раскрытия и модификации в процессе распределения.

Функциональное требование безопасности 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 ДЦ (ФТБ8). 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 ДЦ возможность верификации сертификатов открытых ключей и идентификатора того ДЦ, который сгенерировал сертификат.

УТОЧНЕНИЕ: верификация сертификата должна включать, как минимум:
а) проверку цифровой подписи;
б) проверку срока действия;
в) проверку параметров аннулирования.

Незначительная модификация ФТБ9 может расширить возможности подписчиков ДЦ по проверке сертификатов подобно тому, как это выполняется доверенным центром.

П5.4.2. Требования доверия к безопасности ОО

Требования доверия 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 с ОК ОУД4 обеспечивает умеренно высокий уровень доверия безопасности проектирования.

П5.4.3. Требования безопасности для ИТ-среды

Для ДЦ 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 ДЦ, хранимых и обрабатываемых ОО.

П5.5. Обоснование ПЗ

П5.5.1. Обоснование целей безопасности

Демонстрация соответствия целей безопасности угрозам может быть выполнена следующим образом:
а) 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;
б) логическим обоснованием того, что цели безопасности противостоят угрозам.

Приведем 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.

П5.5.2. Обоснование функциональных требований безопасности

Демонстрацию соответствия ФТБ целям безопасности для ОО можно представить следующим образом:
а) в виде таблицы, показывающей, какие ФТБ какие цели безопасности удовлетворяют (например, ФТБ3–4 и ФТБ7 соответствует цели безопасности О3): при этом необходимо обеспечить соответствие каждого ФТБ, по крайней мере, одной цели безопасности;
б) логическим обоснованием соответствия ФТБ целям безопасности.

Приведем пример обоснования ФТБ.

Цель О3 удовлетворяется ФТБ3–4 и ФТБ7, обеспечивающими функциональные возможности генерации цифровой подписи.

Так как для каждого дополнительного сервиса ДЦ 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. Это следует делать, рассматривая для каждого ФТБ, в свою очередь, потенциальную необходимость другого ФТБ с целью предотвращения обхода или вмешательства в работу соответствующих ФБО.

Приведем примеры демонстрации взаимной поддержки требований безопасности.

а) ФТБ 6 обеспечивает безопасную генерацию ключей ДЦ и поэтому поддерживает те ФТБ, которые полагаются на использование этих ключей: ФТБ1, ФТБ2.

б) ФТБ3–4,7 обеспечивают сервис цифровой подписи и поэтому поддерживают те ФТБ, которые полагаются на генерацию цифровых подписей: ФТБ1.

в) ФТБ4–5,7 обеспечивают сервис проверки цифровой подписи и поэтому поддерживают те ФТБ, которые относятся к проверке цифровой подписи: ФТБ2.

П5.5.3. Обоснование требований доверия к безопасности

Формирование этого раздела 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.