ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по разработке профилей защиты и заданий по безопасности

(ISO/IEC TR 15446:2009, IDT)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации
Ташкент

Предисловие

1 ПОДГОТОВЛЕН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований - «UNICON.UZ»

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи и информатизации № 7

3 ПРИНЯТ Постановлением Узбекского агентства стандартизации, метрологии и сертификации от 30.11.2012 № 05-416

4 Настоящий стандарт идентичен международному стандарту ISO/IEC TR 15446:2009 Информационная технология. Методы обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности (ISO/IEC TR 15446:2009 Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets).

Перевод с английского языка (en).

В стандарт включены следующие редакционные изменения:

a) слова «настоящий технический отчет» заменены на «настоящий стандарт»;

b) в разделе 4 для удобства восприятия стандарта приведены все используемые в нем сокращения;

c) из текста стандарта исключен подраздел 15.2 «Соответствие национальным интерпретациям», соответственно нумерация подраздела 15.3 изменена на 15.2;

d) из текста стандарта исключены разделы «Библиография» и «Алфавитный указатель» (Index).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов государственные стандарты Узбекистана, сведения о которых приведены в дополнительном приложении В.

Степень соответствия – идентичная (IDT).

5 ВВЕДЕН ВПЕРВЫЕ

Исключительное право официального опубликования настоящего стандарта на территории Узбекистана принадлежит агентству «Узстандарт»

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 2
5 Цель и структура 3
6 Краткий обзор профилей защиты и заданий по безопасности 4
6.1 Введение 4
6.2 Пользователи настоящего стандарта 5
6.3 Использование профилей защиты и заданий по безопасности . . . 5
6.3.1 Введение 5
6.3.2 Процессы закупки по спецификации 7
6.3.3 Процессы закупки методом отбора 10
6.3.4 Другое использование профилей защиты 12
6.4 Процесс разработки профилей защиты и заданий по безопасности 13
6.5 Чтение и понимание профилей защиты и заданий по безопасности 14
6.5.1 Введение 14
6.5.2 Чтение краткого обзора объекта оценки 15
6.5.3 Чтения описания объекта оценки 16
6.5.4 Цели безопасности для операционной среды 17
6.5.5 Чтение утверждения о соответствии 18
6.5.6 Соответствие профилям защиты 18
6.5.7 Оценочные уровни доверия и другие вопросы доверия 19
6.5.8 Заключение 21
6.5.9 Чтение дополнительной информации 21
7 Введение профилей защиты и заданий по безопасности 22
8 Утверждения о соответствии 22
9 Постановка задачи безопасности 23
9.1 Введение 23
9.2 Неформальные требования безопасности 26
9.2.1 Введение 26
9.2.2 Источники информации 26
9.2.3 Документирование неформальных требований 28
9.3 Идентификация и спецификация угроз 30
9.3.1 Введение 30

9.3.2 Выбор методологии анализа угроз 30
9.3.3 Описание угроз 32
9.3.4 Применение выбранной методологии анализа угроз 37
9.3.5 Практические рекомендации 38
9.4 Идентификация и спецификация политик 40
9.5 Идентификация и спецификация предположений 42
9.6 Оформление постановки задачи безопасности 45
10 Цели безопасности 46
10.1 Введение 46
10.2 Структурирование угроз, политик и предположений 48
10.3 Идентификация целей для не ИТ-среды 49
10.4 Идентификация целей для ИТ-среды 50
10.5 Идентификация целей для объекта оценки 50
10.6 Разработка логического обоснования целей безопасности. 56
11 Определение расширенных компонентов 58
12 Требования безопасности 62
12.1 Введение 62
12.2 Парадигмы безопасности в ISO/IEC 15408 64
12.2.1 Объяснение парадигм безопасности и их использование для моделирования функций безопасности 64
12.2.2 Управление доступом к используемым ресурсам и объектам 65
12.2.3 Управление пользователями 70
12.2.4 Собственная защита объекта оценки 72
12.2.5 Обеспечение безопасной связи. 73
12.2.6 Аудит безопасности 75
12.2.7 Требования к архитектуре 76
12.3 Спецификация функциональных требований безопасности в профиле защиты или задании по безопасности. 77
12.3.1 Выбор функциональных требований безопасности 77
12.3.2 Выбор функциональных требований безопасности из ISO/IEC 15408-2 82
12.3.3 Выполнение операций над функциональными требованиями безопасности 86
12.3.4 Спецификация требований аудита 89
12.3.5 Спецификация требований управления 91
12.3.6 Спецификация функциональных требований безопасности, позаимствованных из профиля защиты 92

12.3.7 Спецификация функциональных требований безопасности, отсутствующих в профиле защиты 93
12.3.8 Спецификация функциональных требований безопасности, отсутствующих в ISO/IEC 15408-2 93
12.3.9 Представление функциональных требований безопасности. . 93
12.3.10 Разработка логического обоснования требований безопасности 95
12.4 Спецификация требований доверия к безопасности в профилях защиты и заданиях по безопасности 96
12.4.1 Выбор требований доверия к безопасности 96
12.4.2 Выполнение операций над требованиями доверия к безопасности 98
12.4.3 Спецификация требований доверия к безопасности, отсутствующих в ISO/IEC 15408-3 99
12.4.4 Логическое обоснование требований доверия к безопасности 99
13 Краткая спецификация объекта оценки 99
14 Профили защиты и задания по безопасности для составных объектов оценки и компонентов объектов оценки 100
14.1 Составные объекты оценки 100
14.2 Компоненты объектов оценки 105
15 Особые случаи 106
15.1 Профили защиты и задания по безопасности для низкого уровня доверия 106
15.2 Пакеты функциональных требований и требований доверия к безопасности. 106
16 Использование автоматических инструментальных средств 107
Приложение А (справочное) Пример определения расширенного компонента 108
Приложение В (справочное) Сведения о соответствии государственных стандартов Узбекистана международным стандартам 111

Введение

Настоящий стандарт является дополнением к стандарту ISO/IEC 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», состоящему из трех частей. В стандарте ISO/IEC 15408 содержатся концепции профилей защиты (ПЗ) и заданий по безопасности (ЗБ). Профиль защиты – это независимая от реализации формулировка требований безопасности определенного типа продуктов ИТ, который может быть затем оценен по ISO/IEC 15408, тогда как задание по безопасности – это формулировка требований безопасности по ISO/IEC 15408 для конкретного объекта оценки (ОО).

Настоящий стандарт соответствует третьему изданию ISO/IEC 15408, которое в отличие от предшествующих изданий обеспечивает более исчерпывающее объяснение того, какие требования должны содержаться в ПЗ или ЗБ. Однако в ISO/IEC 15408 далеко не в полном объеме представлены все исчерпывающие разъяснения или правила относительно того, как разрабатывать ПЗ либо ЗБ, или как использовать ПЗ либо ЗБ на практике при разработке технического задания, проектировании или реализации систем безопасности.

Для восполнения этого пробела и предназначен настоящий стандарт. Он представляет собой результат коллективного опыта и многолетнего труда ведущих экспертов в области оценки по ISO/IEC 15408 и разработки безопасных продуктов ИТ.

Для понимания настоящего стандарта необходимо знать общие принципы в области оценки безопасности информационных технологий. Читателю, недостаточно подготовленному в этой области, рекомендуется вначале ознакомиться с частью 1 стандарта ISO/IEC 15408.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

Ахборот технологияси

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ ВА ВОСИТАЛАРИ

Ҳимоя профиллари ва хавфсизлик бўйича топшириқларни ишлаб чиқиш бўйича қўлланма

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ[1]

Руководство по разработке профилей защиты и заданий по безопасности

Information technology
SECURITY TECHNIQUES AND FACILITIES
Guide for the production of Protection Profiles and Security Targets

Дата введения 2013-03-01
2023-03-01

1 Область применения

Настоящий стандарт представляет собой руководство по разработке профилей защиты и заданий по безопасности.

В настоящем стандарте не рассматриваются вопросы регистрации ПЗ и спецификаций ЗБ, а также связанной с ними задачи - обработки защищаемой интеллектуальной собственности.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие международные стандарты:

ISO/IEC 15408-1:2009 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ISO/IEC 15408-2:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

[1] **С изменением № 1, утвержденным постановлением агентства «Узстандарт» от 08.09.2017 № 05-790и**

ISO/IEC 15408-3:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты

ISO/IEC 18045:2008 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.

(Новая редакция, Изм. № 1)

3 Термины и определения

В настоящем стандарте применяются термины и определения по ISO/IEC 15408-1.

4 Сокращения

В настоящем стандарте применяются следующие сокращения:

ЗБ	-	Задание по безопасности
ИТ	-	Информационная технология
ИФБО	-	Интерфейс ФБО
ОЗУ	-	Оперативное запоминающее устройство
ОО	-	Объект оценки
ОУД	-	Оценочный уровень доверия
ПБОр	-	Политика безопасности организации
ПЗ	-	Профиль защиты
ПЗБ		Постановка задачи безопасности
ПО	-	Программное обеспечение
ПИН	-	Персональный идентификационный номер
ПФБ	-	Политика функции безопасности
СУБД	-	Система управления базами данных
ТДБ	-	Требование доверия к безопасности
ФБО	-	Функции безопасности ОО
ФТБ	-	Функциональное требование безопасности
COTS	-	Commercial Off-The-Shelf (готовый коммерческий)
CRL	-	Certificate Revocation List (список аннулированных сертификатов)

(Исключен, Изм. № 1)

FTP	-	File Transfer Protocol (протокол передачи файлов)
HTTP	-	HyperText Transfer Protocol (протокол передачи гипертекста)
IP	-	Internet Protocol (межсетевой протокол)
IPSec	-	IP Security (протокол защиты сетевого трафика на IP-уровне)
LDAP	-	Lightweight Directory Access Protocol [облегченный (упрощенный) протокол доступа к (сетевым) каталогам]
PKI	-	Public Key Infrastructure (инфраструктура открытых ключей)
SSL	-	Secure Sockets Layer (протокол безопасных соединений, протокол SSL)
TLS	-	Transport Layer Security (протокол безопасности транспортного уровня, протокол TLS)
XML	-	Extensible Markup Language (расширяемый язык разметки)

5 Цель и структура

Настоящий стандарт представляет собой руководство по разработке ПЗ и ЗБ, используемых при оценке безопасности продуктов и систем информационных технологий на основе стандартов серии ISO/IEC 15408. В этом стандарте подробно описывается разработка различных частей ПЗ и ЗБ, а также их взаимосвязи.

Требования настоящего стандарта относятся к третьему изданию стандартов серии ISO/IEC 15408. Более ранние версии стандартов серии ISO/IEC 15408 содержат иные, несовместимые технические требования. Несмотря на это, методики, предложенные в настоящем стандарте, в основном могут быть также применены и к более ранним версиям ISO/IEC 15408.

Настоящий стандарт предназначен для разработчиков ПЗ и ЗБ, но может также представлять интерес для потребителей и пользователей ПЗ и ЗБ, позволяя им понять, чем руководствовались разработчики при разработке ПЗ и/или ЗБ, и получить подтверждение релевантности (степени соответствия) и точности информации, которую они содержат.

Настоящий стандарт будет полезен оценщикам ПЗ и ЗБ, а также лицам, ответственным за мониторинг ПЗ и оценку ЗБ.

Предполагается, что пользователи настоящего стандарта хорошо знакомы со стандартом ISO/IEC 15408-1, в частности с его приложениями А и В, в которых соответственно содержатся описания ПЗ и ЗБ. Разработчики ПЗ и ЗБ предварительно также должны ознакомиться с другими частями стандарта ISO/IEC 15408, ссылки на которые приведены в настоящем стандарте, в том числе с вводным материалом, например, с парадигмой функциональных требований, описанной в ISO/IEC 15408-2.

Настоящий стандарт предназначен для использования только в качестве руководства. С учетом содержания и структуры настоящего стандарта его нельзя рассматривать в качестве стандарта, используемого для оценки ПЗ и ЗБ. Предполагается, что настоящий стандарт полностью соответствует ISO/IEC 15408; тем не менее, в случае любых расхождений между настоящим стандартом и ISO/IEC 15408, последнему, как основополагающему стандарту, следует отдать предпочтение.

Разделы с 1 по 4 содержат вводный и ссылочный материалы.

Раздел 6 содержит введение в ПЗ и ЗБ, и возможность их использования. В разделе 6 также рассматриваются взаимосвязи между ПЗ и ЗБ и проблемы, связанные с процессом их разработки.

В разделах с 7 по 13 приведена информация о том, как следует подробно излагать семь обязательных разделов содержания ПЗ или ЗБ в соответствии со структурой, определенной в ISO/IEC 15408-1 (разделы А.2 и В.2 приложений А и В соответственно).

В разделе 14 рассматриваются специфические вопросы разработки ПЗ и ЗБ для составных ОО, то есть для ОО, которые состоят из двух или более компонентов ОО, каждый из которых имеет собственное ПЗ или ЗБ.

В разделе 15 рассмотрено несколько частных случаев, а именно: содержания ПЗ и ЗБ с низким уровнем доверия; соответствие национальных интерпретаций; пакеты функциональных требований и требований доверия.

В разделе 16 рассмотрены вопросы использования автоматических инструментальных средств при разработке ПЗ и ЗБ.

6 Краткий обзор профилей защиты и заданий по безопасности

6.1 Введение

В настоящем разделе приведен краткий обзор ролей ПЗ и ЗБ при оценке информационной безопасности по ISO/IEC 15408.

6.2 Пользователи настоящего стандарта

Настоящий стандарт предназначен для использования двумя особыми категориями пользователей:

- специалисты в области информационных технологий, дополнительно обладающие знаниями в области информационной безопасности (например, администраторы информационной безопасности/разработчики, понимающие требования безопасности), но не являющиеся специалистами в области оценки информационной безопасности и прежде не знакомые с ISO/IEC 15408;
- специалисты в области информационной безопасности, хорошо знакомые с ISO/IEC 15408, для которых разработка ПЗ и ЗБ является частью их профессиональной деятельности.

Пользователям, относящимся к одной из вышеперечисленных категорий, в этом разделе будет представлена информация, необходимая для понимания цели и структуры ПЗ и ЗБ. Им также будет предоставлена дополнительная информация, необходимая для чтения и понимания ПЗ и ЗБ, идентификации их релевантности и корректности относительно определенных условий. В следующих разделах приведены подробные пояснения к содержанию всех частей ПЗ и ЗБ, необходимые при разработке этих документов.

Пользователям-специалистам содержание этого раздела должно быть уже знакомо. В последующих разделах для специалистов приведены методология, методы и практические рекомендации, которые они смогут использовать при подготовке ПЗ и ЗБ самым эффективным и логичным на настоящий момент способом.

Те же пользователи, которые не являются специалистами в области информационной безопасности, при разработке ПЗ или ЗБ тоже могут пользоваться настоящим стандартом. Но, кроме того, этим пользователям будет необходимо найти, прочитать и понять опубликованные примеры ПЗ или ЗБ с подобными требованиями или воспользоваться услугами других специалистов, которые имеют необходимые знания и опыт.

6.3 Использование профилей защиты и заданий по безопасности

6.3.1 Введение

Стандарт ISO/IEC 15408 в основном используется для оценки продуктов ИТ. Под продуктом ИТ понимается объект любого типа, созданный с использованием информационных технологий, независимо от того, является ли этот объект системой ИТ, разработанной исключительно для одной организации, или пакетом COTS-продуктов, предназначенным для продажи множеству разных, не связанных между собой заказчиков.

Если говорится о продуктах ИТ или просто о продуктах, то рекомендации настоящего стандарта относятся ко всем таким объектам. Если рекомендации настоящего стандарта предназначены только для

продукта определенного типа, то говорится о системах или COTS-продуктах, или используется некоторая другая, явно специфическая формулировка.

Так как продукты ИТ могут использоваться во многих областях и в различных средах, то понятие безопасности изменяется вместе с продуктами. Следовательно окончательный результат оценки по ISO/IEC 15408 никогда не может быть сформулирован как «этот продукт ИТ безопасный», а только как «этот продукт ИТ соответствует спецификации безопасности».

В стандарте ISO/IEC 15408 стандартизированы спецификации безопасности, чтобы (в том числе):

- назначать полномочия для доступа к специфическому содержимому при необходимости оценки продукта по спецификациям безопасности;
- производить сравнение спецификаций безопасности различных продуктов.

В ISO/IEC 15408 представлены два разных вида спецификаций безопасности: ПЗ и ЗБ. Различие между ними двумя наилучшим образом объясняется теми ролями, которые они будут играть в процессе закупки заказчиком типового продукта у разработчика.

В данном случае заказчик, разработчик и продукт - это абстрактные понятия. Заказчик – это лицо, желающее купить продукт. Им может быть физическое лицо, организация, группа организаций, государственное учреждение и т.п. Разработчик – это лицо, желающее продать продукт. Им может быть один программист, небольшая компания, большая компания, совместно работающая группа компаний и т.п. Наконец, продуктом может быть небольшое программное приложение или смарт-карта, большая операционная система или отдельная компьютерная система, содержащая сотни различных компонентов.

Когда заказчик хочет приобрести продукт, он имеет по существу две возможности:

- заказать его разработчику, детально изложив свои требования, а разработчик создаст продукт, который предназначен только для этого заказчика и точно соответствует его требованиям. Это возможно дорого обойдется заказчику, но он получит желаемое. Этот процесс называется процессом закупки по спецификации;
- выбрать продукт из множества существующих продуктов. Это вероятно обойдется дешевле, но в результате продукт может будет, может не будет точно соответствовать требованиям заказчика. Этот процесс называется процессом закупки методом отбора.

Когда безопасность ИТ имеет важное значение, то процесс закупки усложняется. Для среднего заказчика это заключается в том, что ему трудно:

- сформулировать собственные требования по безопасности информации;

- самостоятельно определить, соответствует ли уровень безопасности ИТ данного продукта заявленному и в достаточной ли мере он удовлетворяет его требования;

- определить, какие характеристики безопасности имеет этот продукт, и соответствуют ли они его требованиям.

Для того, чтобы облегчить заказчику процесс закупки и исключить вышеуказанные затруднения, можно использовать оценку продукта по ISO/IEC 15408, и в этом случае ПЗ и ЗБ играют важную роль. В двух следующих подразделах будет рассмотрено, как оценка может помочь в процессах закупки по спецификации и методом отбора.

Конечно, продукты ИТ автономно не работают. Продукт используется заказчиком в определенной среде, в которой могут быть предусмотрены свои собственные меры безопасности. Иногда для продукта делаются предположения, какие определенные типы средств безопасности могут существовать в пределах этой среды. Эти предположения также формулируются в соответствующих разделах ПЗ или ЗБ.

6.3.2 Процессы закупки по спецификации

6.3.2.1 Введение

В процессе закупки по спецификации заказчик разрабатывает спецификацию, предоставляет эту спецификацию разработчику, а затем разработчик на основе этой спецификации создает продукт. Далее должны быть выполнены следующие шаги, которые более подробно будут рассмотрены ниже:

a) заказчик должен сформулировать свои неформальные требования безопасности;

b) заказчик должен преобразовать эти неформальные требования безопасности в более формальную спецификацию, пригодную для использования разработчиком;

c) разработчик на основе этой спецификации должен создать продукт.

В результате заказчик должен убедиться в том, что этот продукт для него полезен. Следовательно, важно качество каждого из этих шагов.

6.3.2.2 Неформальные требования безопасности

Процесс определения неформальных требований безопасности, который определяет «в чем заключается задача безопасности и как ее сформулировать?» не рассматривается в ISO/IEC 15408 и, следовательно, не рассматривается в настоящем стандарте. Но это не означает, что этот процесс неважен или легко осуществим каким-либо способом.

Тем не менее, ISO/IEC 15408 допускает, что заказчик, способен определить свои неформальные требования безопасности. Если же он сделает это неправильно, то в результате приобретенный им продукт не будет удовлетворять адекватным требованиям безопасности.

При определении заказчиком требований часто возникает множество проблем, связанных с ними, особенно в области безопасности. Типичными недостатками требований заказчика являются:

a) незавершенность (представлены не все требования). Если, например, для этого продукта не были учтены все важные угрозы;

b) отсутствие требований к специфической среде, в которой должен функционировать продукт или эта среда не описана достаточно четко;

c) недосказанность: некоторые подразумеваемые требования к продукту имеют большое значение, но они не были включены. В этом случае эти требования не будут учтены разработчиком;

d) нетестируемость: требования сформулированы двусмысленно, в результате чего будет невозможно проверить, удовлетворяет ли продукт этим требованиям или нет;

e) излишняя детализация: реализация фактически уже написана, но она не устраивает заказчика. Если впоследствии требования изменяются, то зачастую становится неясно, как должны быть внесены эти изменения;

f) использование неоднозначных терминов: например, «средства связи должны быть безопасными», при этом определение термина «безопасные средства» отсутствует;

g) противоречивость: среди требований могут содержаться и внутренне противоречивые требования.

При предоставлении разработчику требований заказчика с подобными недостатками обычно возникают проблемы, так как разработчик может истолковать эти требования неправильно. При оценке безопасности может возникнуть еще гораздо больше проблем, так как оценщики могут интерпретировать эти требования иначе, чем заказчик и разработчик.

Исходя из этих соображений, важным этапом в процессе закупки по спецификации является процесс формализации требований заказчика. Для требований безопасности в соответствии с ISO/IEC 15408 этот процесс формализации производится с помощью ПЗ, являющимся по своей сути документом, в котором определены требования безопасности заказчика в формализированном и стандартизированном виде.

6.3.2.3 Использование профилей защиты в качестве спецификаций

ПЗ обычно разрабатываются большими организациями, группами совместно работающих организаций, государственными учреждениями и т.п., так как эта работа требует значительных инвестиций.

ПЗ содержит много разделов, но наиболее важным в качестве спецификации безопасности является раздел «Функциональные требования безопасности». Эти требования обязательно должны быть записаны специальным языком, который состоит из терминов с однозначными определениями, используемых в ISO/IEC 15408. Использование этого языка в ПЗ гарантирует:

a) однозначность: чтобы разработчик смог понять требования и правильно их интерпретировать;

b) тестируемость: язык содержит только тестируемые термины. В результате чего впоследствии возможно будет произвести оценку продукта на соответствие требованиям ПЗ;

c) отсутствие излишней детализации: для языка обязательно используется определенный уровень абстракции. Это полностью совпадает с требованиями потребителя: он хочет, чтобы что-то было сделано, но не хочет вникать в то, как это делается;

d) максимальная завершенность: язык состоит из отдельных конструкций (например, «если эта функция необходима, тогда и другая функция также потребуется»), это позволяет обеспечивать включение подразумеваемых требований.

6.3.2.4 Разработка продукта по ПЗ

Заказчик имеет возможность задать одному или нескольким разработчикам формализированные требования из соответствующего ПЗ. Каждый разработчик будет использовать этот ПЗ в качестве основы при разработке продукта. Первым этапом этого процесса будет разработка ЗБ.

При разработке ЗБ используется наиболее подходящий ПЗ, в этом случае требования определяются на основе ПЗ (и в принципе описываются) заказчиком, а ЗБ, представляющее собой спецификацию продукта, пишется разработчиком.

Разработчик конечно же не может произвольно составить ЗБ, основываясь на ПЗ заказчика: его ЗБ должно соответствовать ПЗ.

Это означает, что продукт должен удовлетворять всем требованиям заказчика, но:

- в ЗБ может быть определено больше требований, чем в ПЗ: в результате чего заказчику будет предложен продукт с большим набором функциональных возможностей в области безопасности, чем которые содержатся в его требованиях (только при условии, что эти дополнительные функциональные возможности соответствуют ПЗ), из-за того, например, что продукт будет продан нескольким заказчикам, предъявляющим аналогичные, но немного отличающиеся требования, или из-за того, что продукт будет являться производным от существующего стандартного продукта;

- ЗБ будет содержать больше подробностей, чем ПЗ: тогда как ПЗ объясняет «что» будет обеспечивать безопасность, то ЗБ также объясняет и «как»: разработчик в общих чертах намечает, как он сможет реализовать требования заказчика.

ПЗ позволяет разработчику ЗБ маневрировать, предлагая заказчику что-либо равнозначное, обеспечивающее безопасность с помощью других функциональных возможностей. Более подробно этот процесс описан в 6.5.6.

В ЗБ, которое используется впоследствии как «спецификация требований безопасности» в процессе разработки, для разработчика определяются функциональные возможности безопасности, которым должен соответствовать его продукт.

В результате процесса разработки должен быть получен продукт, который может быть передан заказчику, который, в свою очередь, сможет установить и использовать этот продукт. Естественно, этот продукт должен выполнять операции, описанные в ЗБ.

6.3.2.5 Роль оценки в процессе закупки по спецификации

Выше были описаны роли заказчика и разработчика в процессе закупки по спецификации. На основе этого процесса разработчик имеет право просто сказать заказчику (без последующего подтверждения):

a) мое ЗБ соответствует вашему ПЗ;

b) мой продукт соответствует моему ЗБ;

c) следовательно, мой продукт соответствует вашему ПЗ и удовлетворяет вашим требованиям.

Если заказчик принимает эти утверждения, то процесс на этом заканчивается.

Тем не менее, если заказчику потребуется независимая проверка этих утверждений, то для проверки соответствия продукта заданным требованиям он сможет привлечь третью сторону (орган оценки) для проведения оценки безопасности этого продукта по ISO/IEC 15408. Во время этого процесса орган оценки использует ПЗ, ЗБ, продукт и ISO/IEC 15408, чтобы подтвердить два утверждения:

a) ЗБ соответствует ПЗ;

b) продукт соответствует ЗБ.

Следует отметить, что несмотря на то, что оценка была проведена, все еще остаются открытыми два вопроса:

a) *доказательство равнозначности неформальных требований безопасности заказчика и профиля защиты.* Как уже было сказано раньше, этот процесс не входит в область рассмотрения ISO/IEC 15408, но если это выполнено неправильно, то ПЗ не будет соответствовать требованиям заказчика и, следовательно, продукт вероятно также не будет соответствовать его требованиям;

b) *оценка не является «доказательством» соответствия*. Оценка по ISO/IEC 15408 никогда не предоставит полную гарантию, что продукт соответствует ПЗ, она может предоставить только определенную гарантию в зависимости от глубины и области оценки, заданной в ПЗ или ЗБ.

6.3.3 Процессы закупки методом отбора

6.3.3.1 Введение

В предшествующем подразделе говорилось о заказчике, предоставляющем спецификацию, и о разработчике, реализующем эту спецификацию. В этом же подразделе будет рассмотрена ситуация, когда заказчик не имеет возможности приобрести продукт, разработанный специально для него: он должен будет выбрать его из существующих продуктов.

Следовательно, закупка в этом случае основывается не на утверждениях о соответствии продукта формализированным требованиям заказчика (то есть ПЗ), а на сравнении заказчиком существующих продуктов.

В процессе закупки продукта ИТ методом отбора:

a) разработчик должен разработать продукт и спецификацию к нему, предоставить спецификацию заказчику;

b) заказчик должен определить по спецификации (возможно сравнив эту спецификацию со спецификациями других разработчиков), является ли конкретный продукт наиболее пригодным продуктом для его закупки.

Так как заказчик в результате этого процесса хочет знать, что «этот продукт пригоден для меня», важное значение имеет качество каждого из этих шагов.

6.3.3.2 Использование спецификации, предоставленной разработчиком

В процессе закупки методом отбора заказчик должен воспользоваться спецификацией, предоставленной ему разработчиком.

Если эта спецификация неформальная, то возможно, что в ней присутствуют те же недостатки, рассмотренные в 6.3.2.2, что и в неформальных требованиях заказчика. По этой причине спецификация должна быть также формализирована, для этого используется ЗБ. В данном случае ЗБ идентично ЗБ, рассмотренному в 6.3.2.4, с одним очевидным различием: поскольку оно не основано на ПЗ заказчика, то оно может не соответствовать требованиям этого ПЗ (оно может соответствовать требованиям ПЗ других типов).

Поскольку разработчику не известны специфические требования заказчиков, он предварительно должен проанализировать потребность рынка и только потом разработать ЗБ. Следовательно, ЗБ заведомо не будет соответствовать любым специфическим требованиям заказчиков.

Разработчик создает продукт согласно ЗБ: этот процесс аналогичен процессу, описанному для процесса закупки по спецификации.

6.3.3.3 Сравнение заданий по безопасности разных разработчиков

Заказчик теперь может сравнить ЗБ многих продуктов и выбрать тот продукт, который лучше всего удовлетворяет его требованиям (вероятно, заказчика также будут интересовать требования, не относящиеся к области безопасности, например, стоимость продукта). В этом случае заказчик несомненно должен каким-либо образом определиться со своими неформальными требованиями безопасности (см. 6.3.2.2) и сравнить их с предложенными ему ЗБ. Если один или несколько продуктов соответствуют требованиям заказчика, то выбор сделан. В противном случае, заказчик должен будет выбрать «наиболее подходящий» продукт или найти некоторое другое решение (то есть изменить свои требования).

6.3.3.4 Роль оценки в процессе закупки методом отбора

Аналогично процессу закупки по спецификации разработчик может просто утверждать, что его продукт соответствует ЗБ и, если заказчик соглашается с этим утверждением, процесс закупки на этом заканчивается.

Несмотря на все вышесказанное, общепринято, что разработчик должен предоставить заказчику сертификат соответствия, подтверждающий, что независимая третья сторона (орган оценки) утвердила ЗБ и произвела оценку безопасности по ISO/IEC 15408 для подтверждения соответствия продукта требованиям ЗБ. Заказчик также имеет возможность поручить органу оценки произвести оценку продукта на соответствие требованиям ЗБ, если для него это существенно или он не доверяет разработчику, или если у разработчика отсутствует сертификат соответствия.

Следует отметить, что при использовании продуктов, прошедших оценку, до сих пор остаются открытыми два вопроса:

a) *доказательство равнозначности неформальных требований безопасности заказчика и задания по безопасности*. Как уже было сказано раньше, этот процесс находится за пределами области рассмотрения ISO/IEC 15408, но если он выполнен неправильно, то ЗБ не будет соответствовать требованиям заказчика, и, следовательно, продукт не будет также соответствовать его требованиям;

b) *оценка не является «доказательством» соответствия*. Оценка по ISO/IEC 15408 никогда не предоставит полную гарантию, что продукт соответствует ЗБ, она может только предоставить определенную гарантию в зависимости от глубины и области оценки, заданной в ЗБ.

6.3.4 Другое использование профилей защиты

Профили защиты используются и в других случаях. Например, органы стандартизации или ассоциации производителей могут использовать ПЗ в качестве лучших практических стандартов для определения минимального уровня безопасности для специфических типов приложений. Государственные органы и торговые ассоциации могут санкционировать использование этих ПЗ. В этом случае, как от заказчиков, так и от разработчиков, вероятно, потребуется соблюдение этих ПЗ, а также они смогут потребовать или предложить дополнительные функциональные возможности безопасности для удовлетворения своих собственных специфических потребностей.

Организации, разрабатывающие ПЗ или санкционирующие их использование для подобных целей, несут большую ответственность, когда гарантируют, что эти ПЗ содержат минимум требований (ПЗ требуют не более того, чем это абсолютно необходимо) и эти требования выполнимы (ПЗ не требуют тех функциональных возможностей или гарантий, которые не могут обеспечить разработчики).

ПЗ может также разрабатываться для обозначения потребности в средстве защиты информации определенного типа, даже если эта потребность не является общепризнанной на момент публикации и подобные средства (пока) не существуют. Разработчики продуктов должны с осторожностью интерпретировать такие ПЗ. Иначе после завершения разработки соответствующего продукта может выясниться, что требования устарели или спонсоры ПЗ отказываются закупать этот продукт, поскольку они нашли другие способы для удовлетворения своих требований.

В довершение ко всему, ПЗ являются спецификациями требований безопасности. Необходимо остерегаться от попыток неправильного использования ПЗ при задании требований других типов, если же это было сделано явно, то эти требования должны рассматриваться как неприемлемые.

6.4 Процесс разработки профилей защиты и заданий по безопасности

Порядок представления требований для ПЗ и ЗБ, изложенный в приложениях A и B ISO/IEC 15408-1, а также в предыдущих частях этого раздела, предполагает, что требования ПЗ и ЗБ всегда разрабатываются логически «нисходящим» способом, например (в случае ЗБ) это происходит следующим образом:

a) вначале описывается задача безопасности;

b) затем отождествляются цели безопасности, соответствующие этой задаче безопасности;

c) далее задаются требования безопасности, удовлетворяющие целям безопасности для ОО;

d) потом выбираются существующие функции безопасности, удовлетворяющие требованиям безопасности.

В этом случае очень велика вероятность того, что процесс разработки требований ПЗ и ЗБ приобретет неоднократно повторяющийся (циклический) характер. Например, при определении требований безопасности может возникнуть необходимость уточнения целей безопасности или даже задачи безопасности. В общем случае может потребоваться несколько циклов, в процессе которых будут тщательно изучены взаимосвязи между угрозами, политиками безопасности организаций, целями безопасности, требованиями и функциями безопасности, особенно при разработке логического обоснования. Только тогда, когда устранены все выявленные несоответствия в логических обоснованиях, можно допустить, что разработка ПЗ или ЗБ закончена.

Во время циклического процесса разработки ПЗ или ЗБ может появиться новая информация в области рассматриваемой задачи безопасности, в результате чего может потребоваться внесение изменений в документ, в котором отражаются изменения во внешней среде, например:

a) могут быть обнаружены новые угрозы;

b) могут измениться политики безопасности организаций;

c) при возникновении ограничений по стоимости и времени может потребоваться внесение изменений в установленное разделение ответственности между предполагаемым ОО и предполагаемой средой ОО;

d) изменения в предполагаемом потенциале атаки могут повлиять на постановку задачи безопасности объекта оценки.

Также возможно (особенно, если ОО является уже разработанным продуктом), когда автор ПЗ или ЗБ уже ясно представляет идею функциональных возможностей безопасности, которые обеспечит ОО (даже если они еще не отражены как функциональные требования безопасности в ISO/IEC 15408). В таких случаях на определение задачи безопасности и целей безопасности неизбежно будет влиять осведомленность о типовых решениях в области обеспечения безопасности ОО. Процесс разработки ПЗ/ЗБ в известной мере будет в таких случаях «восходящим».

6.5 Чтение и понимание профилей защиты и заданий по безопасности

6.5.1 Введение

Этот подраздел предназначен для той категории пользователей настоящего стандарта, которые не являются специалистами в области оценки безопасности ИТ. Специально для этих пользователей далее будут рассмотрены те места в ПЗ или ЗБ, в которых могут быть скрыты потенциальные упущения или недостатки, особенно в области оценки.

Для досконального понимания содержания ПЗ и ЗБ недостаточно только прочесть приложения А и В ISO/IEC 15408-1 с подробными описаниями ПЗ и ЗБ. Также рекомендуется просмотреть другие опубликованные и повсеместно используемые ПЗ и ЗБ, которые можно получить из многих соответствующих реестров. Самым большим среди этих реестров является информационный портал проекта «Общие критерии».

В ПЗ или ЗБ невозможно кратко сформулировать каждую, взятую по отдельности, характеристику безопасности или простой набор характеристик безопасности: ПЗ или ЗБ содержит описание комплексного набора характеристик безопасности, недостаточно тщательное знакомство с которым может привести к неожиданному результату при закупке или использовании продукта.

Далее будут подробно рассмотрены основные разделы ПЗ или ЗБ, которые можно сравнительно легко понять, но которые содержат основную информацию, необходимую для понимания требований характеристик безопасности, представленных в ПЗ или в ЗБ на соответствующий продукт. К этим разделам относятся:

a) краткий обзор ОО;

b) описание ОО;

c) цели безопасности для среды;

d) утверждение о соответствии.

6.5.2 Чтение краткого обзора объекта оценки

В общем случае краткий обзор ОО является тем разделом ПЗ или ЗБ, с которым в первую очередь необходимо ознакомиться, поскольку он предназначен для потенциальных потребителей ОО, которые просматривают списки прошедших оценку ОО/продуктов с целью найти ОО, которые могут удовлетворять их требованиям безопасности и могут использоваться вместе с их аппаратными, программными и программно-аппаратными средствами. Краткий обзор ОО содержит три заслуживающих внимания подраздела:

a) использование ОО и его основные функции безопасности;

b) тип ОО;

c) аппаратные, программные и программно-аппаратные средства, необходимые для функционирования ОО, но не входящие в его состав.

Подраздел «Использование ОО и его основные функции безопасности» содержит общие положения, в которых описываются без излишних технических подробностей возможности ОО с точки зрения безопасности, которые могут быть использованы в контексте безопасности. Он должен быть достаточно коротким (несколько параграфов), так что его чтение и осмысление не потребует значительных усилий.

В подразделе «Тип ОО» приводится описание общего семейства продуктов ИТ, к которому принадлежит ОО (например, межсетевые экраны, смарт-карты, интранет, локальные сети и т.п.). ISO/IEC 15408 предписывает, что краткий обзор ОО может содержать перечни любых приемлемых требований заказчика для этого типа ОО, но которые могут не поддерживаться ОО. В особенности, если в подразделе «Тип ОО» заказчик хочет получить подтверждение, что ОО:

a) предоставляет определенные функциональные возможности безопасности, а если ОО не предоставляет эти функциональные возможности, то в кратком обзоре ОО это должно быть указано;

b) может использоваться в определенной среде, а если ОО нельзя использовать в такой среде, то в кратком обзоре ОО это должно быть указано.

Следует отметить, что подраздел «Тип ОО» - единственное место в ПЗ или ЗБ, где требуется наличие таких предупреждений. Автор ПЗ или ЗБ может по своему усмотрению повторять эту информацию в примечаниях в подходящих местах, но не обязан это делать.

Если эти представленные предупреждения могут повлиять на предполагаемое использование этого ОО, то потребитель должен серьезно рассмотреть еще раз возможность его использования с этими ограничениями.

Чтобы ОО был способен выполнять свои функции, особенно когда он является программным средством, то тогда иногда должна быть

обеспечена уверенность в аппаратных средствах и, возможно, программно-аппаратных и других программных компонентах. В этом случае необходимо, чтобы в кратком обзоре ОО были указаны эти внешние относительно ОО аппаратные, программные и программно-аппаратные средства.

ПЗ или ЗБ не должны содержать полное и детальное описание всех этих аппаратных, программных и программно-аппаратных средств, но их характеристики должны быть описаны достаточно полно и подробно, чтобы потребитель смог определить основные внешние аппаратные, программные и программно-аппаратные средства, вместе с которыми нужно использовать ОО.

Потребитель должен тщательно выяснить, не содержит ли ОО каких-либо нестандартных компонентов, и впишутся ли эти компоненты в существующую инфраструктуру, бюджет, политики компании и т.п.

6.5.3 Чтение описания объекта оценки

Важно понимать, что если в описании ОО говорится о том, что была выполнена оценка известного продукта XYZ по ISO/IEC 15408, то это вовсе не означает, что все его функции безопасности (или даже большинство этих функций) этого продукта прошли оценку. Возможно, что в действительности были рассмотрены только некоторые из существующих функций безопасности этого продукта, а оценка остальных функциональных возможностей безопасности не производилась. Запрещено вводить в заблуждение потребителей ссылками на ОО, но разработчики могут всегда обойти этот запрет, просто используя название продукта. Потребитель должен проверить, удовлетворяют ли оцененные функциональные возможности ОО его потребностям. Если некоторые функциональные возможности безопасности, которые предполагалось использовать, были исключены, то потребителю нужно самому поинтересоваться, почему это сделано.

Одной из наиболее важных ролей описания ОО является предоставление возможности потребителю ЗБ найти расхождения между заявленными и фактическими функциональными возможностями продукта в области безопасности. С этой целью в описании ОО подробно рассматриваются:

а) физические границы ОО: список всех аппаратных, программно-аппаратных и программных средств, а также соответствующих разделов руководства к ОО. Этот список должен быть составлен на том уровне детализации, который позволит составить общее понятие об этих разделах.

Потребитель должен ознакомиться с этим списком, чтобы убедиться в том, что он не содержит чего-то лишнего, непредвиденного и не желаемого, и что в нем перечислены все предполагаемые компоненты продукта. Если же в этом списке отсутствует какой-либо компонент, то при оценке он был полностью проигнорирован, так как было сделано предположение, что он не существует. Если потребитель намеревается

использовать этот компонент, он не сможет сделать какие-либо выводы о возможностях безопасности на основе оценки;

b) логические границы ОО: логические функции безопасности ОО должны быть представлены на том уровне детализации, который позволит составить общее понятие об этих функциях. В данном подразделе функции безопасности должны быть описаны более подробно, чем в кратком обзоре ОО.

Поскольку информация о физических границах содержится в списке компонентов ОО, то в информации о логических границах должны быть описаны функции, выполняемые ОО. Эти функции уже были кратко рассмотрены в подразделе «Использование ОО и его основные функции безопасности» краткого обзора ОО (см. 6.5.2), в подразделе «Описание ОО» они рассматриваются гораздо более подробно. Наиболее важной особенностью этого подраздела является описание ожидаемой потребителем определенной функции, выполняемой продуктом, например, удаленное (дистанционное) управление (например, эта функция была описана в рекламе этого продукта в техническом журнале), но в описании логических границ удаленное управление не упоминается. Следовательно, удаленное управление не проходило оценку, и поэтому оно не должно использоваться, если потребитель хочет использовать этот продукт в своей конфигурации, прошедшей оценку.

Вследствие вышеизложенного, очень важно внимательно ознакомиться с описанием ОО, чтобы определить, действительно ли была произведена оценка всех взаимосвязанных функций безопасности, необходимых потребителю. В противном случае при оценке потребителю не будет гарантирована работа этой функции.

6.5.4 Цели безопасности для операционной среды

Операционная среда, в которую будет встроен ОО, является местом общего расположения. Для того, чтобы ОО работал правильно, на эту среду должны быть наложены определенные ограничения. Например, если ОО является сервером высокой готовности, то к этому ОО должен быть ограничен доступ инженерно-технического персонала. В этом ОО могла бы быть предусмотрена защита от несанкционированного доступа (несмотря на то, что серверы, исключающие несанкционированный доступ, встречаются очень редко). Таким образом в общем случае для операционной среды этого ОО должно быть выдвинуто требование - для обеспечения безопасности сервера запирать на замок помещение, в котором он установлен.

Эти и другие аналогичные требования для среды описываются в разделах ПЗ или ЗБ «Цели безопасности для среды». Выполнение этих требований необходимо для того, чтобы ОО удовлетворял предъявленным ему требованиям безопасности. Эти требования не являются руководящими принципами, а являются необходимыми условиями для того, чтобы ОО функционировал заранее заданным образом.

Все требования вышеуказанных разделов, адресованные потребителю или его организации, должны быть полностью выполнены: ОО не сделает этого сам. Если хотя бы одно из этих требований будет не выполнено, то ОО не сможет надежно функционировать. Следовательно, необходимо, чтобы потребитель самостоятельно определил, возможно ли обеспечить выполнение указанных требований в его организации, и если одно из этих требований не выполнимо, то это ОО в этой организации нельзя использовать.

6.5.5 Чтение утверждения о соответствии

Утверждение о соответствии, как правило, находится в начале ПЗ или ЗБ. Оно, как правило, состоит из единственного предложения нижеприведенного содержания.

Этот ПЗ/ЗБ соответствует требованиям:

- стандарта ISO/IEC 15408. В этой части утверждения необходимо указать использованную версию ISO/IEC 15408;
- части 2 ISO/IEC 15408 либо части 2 ISO/IEC 15408, расширенной другими компонентами требований. В этой части утверждения приводится описание того, исходя из каких соображений были заданы функциональные требования безопасности, и их приемлемость с точки зрения потребителя;
- части 3 ISO/IEC 15408 либо части 3 ISO/IEC 15408, расширенной другими компонентами требований. В этой части утверждения приводится описание того, исходя из каких соображений, были заданы требования доверия к безопасности. В том случае, когда используются требования части 3 ISO/IEC 15408, расширенной другими компонентами требований, разработчик ПЗ и ЗБ разрабатывает свои собственные тесты функций безопасности ОО, а потребитель, со своей стороны, должен поинтересоваться, почему это было необходимо;
- реестра пакетов, который необходим для утверждения о соответствии ОО. Обычно существует только один такой пакет, называемый оценочным уровнем доверия ОУД 1, ОУД2, …, ОУД7, часто сопровождаемый «расширением». ОУД будут рассмотрены в 6.5.7. Очень редко можно найти пакет любого другого типа, определенного с точки зрения потребителя, потребитель снова должен поинтересоваться, почему это было необходимо;
- реестра ПЗ с утверждениями о соответствии ПЗ или ЗБ. Этот реестр будет рассмотрен в 6.5.6.

6.5.6 Соответствие профилям защиты

ЗБ может содержать раздел с утверждением о соответствии ПЗ (но он не является обязательным). Также и в ПЗ может потребоваться утверждение о соответствии другим ПЗ. При необходимости утверждение о соответствии включается в ПЗ или ЗБ. Стандартом ISO/IEC 15408 не допускается частичное соответствие в любой форме, так что если утверждение о соответствии ПЗ включено, то ПЗ или ЗБ должны полностью соответствовать одному или нескольким ссылочным ПЗ.

Соответствие ПЗ означает, что ПЗ или ЗБ (а если это ЗБ продукта, прошедшего оценку, то и продукт тоже), удовлетворяют всем требованиям этого ПЗ.

При чтении ПЗ также можно найти одно из двух утверждений, что ЗБ и другие ПЗ «строго соответствуют» или «очевидно соответствуют». Для публикуемых ПЗ, как правило, требуется очевидное соответствие. Это означает, что в ЗБ, утверждающих о соответствии ПЗ, должно предлагаться решение общей задачи безопасности, описанной в ПЗ, любым аналогичным или с большими ограничениями способом, чем способ, описанный в ПЗ.

Выражение «аналогичный, но с большими ограничениями» в принципе означает, что в ПЗ и ЗБ могут содержаться совершенно разные утверждения, относящиеся к разным логическим объектам, и использоваться разные принципы и т.п. при том условии, что в итоге ЗБ будет требовать тех же самых или больших ограничений для ОО, и тех же самых или меньших ограничений для среды ОО.

Строгое соответствие используется только в том случае, когда не должно быть каких-либо различий между ПЗ и ЗБ, например, в процессе закупки методом отбора (см. 6.3.3). Конечно, при необходимости ЗБ может быть дополнено другими ограничениями. Если же потребителю продукта не требуется его строгое соответствие требованиям ПЗ, то вряд ли у него возникнет необходимость использовать этот ПЗ.

6.5.7 Оценочные уровни доверия и другие вопросы доверия

Из краткого обзора и описания ОО потребитель сможет понять, что может делать ОО, то есть для выполнения каких функций он предназначен. Однако, только одного функционального назначения ИТ продукта недостаточно. Продукты с одним и тем же функциональным назначением могут использоваться с разными параметрами настройки. Например, смарт-карта, изготовленная по одному проекту, может использоваться в качестве:

- проездного автобусного билета с небольшой суммой на «дорожные расходы»;
- кредитной карты с лимитом кредита, например, в 10 000 денежных единиц;
- средства контролируемого доступа к засекреченному военному объекту.

В первом случае, некто доволен и «низкокачественной» смарт-картой. Если хакеру удастся взломать проездной билет, то он возможно сможет бесплатно пользоваться автобусом до тех пор, пока не будут изменены параметры карты. Убыток потенциального дохода (при условии, что другие карты не будут взломаны), для автобусной компании будет не значительным.

Во втором и, несомненно, в третьем случаях необходимо гораздо большее доверие к правильной реализации функционального назначения

карты, так как взлом только одной карты может иметь значительные последствия.

В ISO/IEC 15408 доверие формализировано в 27 категорий (так называемых семейств доверия). В каждой категории определяются разные уровни соответствия, из них самый высокий уровень - наилучший.

Например, при оценке продукта разработчиком определяется класс тестового покрытия, который определяет, насколько данный тест охватывает проверкой все заданные требования:

- 0: неизвестно, выполнил ли разработчик тестирование продукта;
- 1: разработчик выполнил некоторые тесты на некоторых интерфейсах продукта;
- 2: разработчик выполнил некоторые тесты на всех интерфейсах продукта;
- 3: разработчик выполнил самое большое количество тестов на всех интерфейсах продукта.

Из этого примера можно увидеть, что с каждым уровнем объем работы увеличивается, а степень неопределенности уменьшается.

Протокол результатов, состоящий из индивидуальных рейтингов для всех 27 семейств доверия, неспециалисту почти невозможно интерпретировать. Для того, чтобы предоставить неспециалистам возможность оценить доверие по ISO/IEC 15408 существуют семь заранее заданных рейтингов, называемых оценочными уровнями доверия (ОУД). Эти уровни образуют возрастающую шкалу от ОУД 1 до ОУД 7, где ОУД 1 - самый низкий уровень, а ОУД 7 - самый высокий.

Каждый ОУД может быть представлен в виде определенной комбинации 27 компонентов доверия, каждый из которых может быть идентифицирован в семействе доверия конкретным номером. Например, в ОУД1 для 13 компонентов доверия присваивается номер 1 и для других 14 компонентов доверия - номер 0, тогда как в ОУД2 для 7 компонентов доверия присваивается номер 2, для 11 компонентов доверия - номер 1 и для других 9 компонентов доверия - номер 0.

ОУД имеют строгую иерархическую структуру, если в ОУДn определенному компоненту доверия присвоен определенный номер, тогда в ОУДn+1 этому компоненту доверия будет присвоен тот же или больший номер. Таким образом ОУДn+1 обеспечит более строгое доверие, чем ОУДn.

Недостатком более высокого доверия является, конечно, большая стоимость. В области тестового покрытия, описанного выше, класс 0 может означать, что стоимость тестирования практически равна нулю, но с каждым более высоким классом разработчик должен выполнять тесты и затем подтверждать выполненные тесты, а оценщик должен определить, правильно ли разработчик выполнил тестирование и подтвердил его и т.п. Большее доверие почти всегда означает большую стоимость. Конечно, большее доверие также уменьшает риск неправильного выполнения

заданных функциональных возможностей или наличия уязвимых мест, доступных для пользователей.

Перечни всех ОУД вместе с их описаниями и характеристиками доверия, которые обеспечивают ОУД, приведены в ISO/IEC 15408-3.

Нельзя сказать, что ОУД являются самым совершенным механизмом, более пригодным для оценки некоторых типов продуктов, чем другие механизмы. Тем не менее, в настоящее время ОУД являются единственным широко распространенным методом предоставления характеристик доверия ISO/IEC 15408, которые может понять неспециалист.

6.5.8 Заключение

В заключении этого подраздела можно сделать два вывода:

a) (очевидно), что ЗБ может быть понято после прочтения нескольких подразделов;

b) (менее очевидно), что эти подразделы могут содержать важные предостережения, и поэтому крайне необходимы для понимания ограничений оценки.

Когда потребитель решает, что ему необходим межсетевой экран, соответствующий требованиям ОУД4, он не предполагает, что межсетевой экран, сертифицированный по ОУД4 ISO/IEC 15408, может иметь ограничения, которые сделают его полностью непригодным для потребителя, и этот межсетевой экран не сможет обеспечить необходимую ему безопасность в полной мере.

Например, потребитель предполагает использовать межсетевой экран двояко: для маршрутизации пакетов и для получения услуг HTTP/FTP прокси-сервера. Маршрутизатор может находиться в составе ОО - межсетевого экрана, оцененного по ОУД4. Но межсетевой экран в качестве маршрутизатора может предоставить только элементы управления маршрутизацией пакетов. В худшем случае, когда потребитель найдет оцененный межсетевой экран, который предлагает услуги прокси-сервера, но логическая область которого ограничена только маршрутизацией пакетов, тогда потребитель должен сам поинтересоваться, почему это так.

6.5.9 Чтение дополнительной информации

Вышеописанные разделы ПЗ или ЗБ являются основными разделами ПЗ и ЗБ, содержащими наиболее полезную информацию для неспециалистов. Если потребителю будет необходимо больше узнать о продукте, он может ознакомиться с краткой спецификацией ОО, в которой более детально описывается, каким образом производится ввод в эксплуатацию ОО. В этом разделе может содержаться много непонятных сокращений, например, типа FIA_UID.2.1. Тем не менее, краткую спецификацию ОО, которая удовлетворяет всем требованиям оценщиков, могут также без затруднений понять и потребители продукта.

Потребителям, которым необходимо понять содержание других разделов ПЗ или ЗБ, могут помочь нижеследующие разделы настоящего стандарта. Хотя они предназначены для использования экспертами при

определении ПЗ или ЗБ, но содержащаяся в них информация также поможет потребителям понять соответствующее содержание.

7 Введение профилей защиты и заданий по безопасности

В этом разделе содержатся рекомендации по написанию раздела «Введение» ПЗ или ЗБ.

Введение ПЗ состоит из следующих элементов:

- ссылка на ПЗ;
- краткий обзор ОО.

Введение ЗБ состоит из следующих элементов:

- ссылки на ЗБ и ОО;
- краткий обзор ОО;
- описание ОО.

Единственной не очевидной частью краткого обзора ОО является описание использования и основных функций безопасности ОО. Чаще всего использование ОО наилучшим образом описывается в заключении раздела «Постановка задачи безопасности» ПЗ или ЗБ (см. раздел 9), тогда как основные функции безопасности описываются в заключении раздела «Цели безопасности». Это гарантирует соответствие введения более подробным разделам ПЗ или ЗБ.

8 Утверждения о соответствии

Этот раздел представляет собой подробные пояснения к разделам ПЗ или ЗБ «Утверждения о соответствии», соответственно описанным в приложениях А и В ISO/IEC 15408-1.

В разделах ПЗ или ЗБ «Утверждения о соответствии» описывается насколько ПЗ или ЗБ соответствует:

a) *ISO/IEC 15408*. Должна быть точно указана версия ISO/IEC 15408, использованная при написании (а также возможно и при оценке) ПЗ или ЗБ. В том случае, когда был использован неофициальный перевод ISO/IEC 15408 с английского языка на какой-либо другой язык, это также должно быть указано. Также должно быть указано, что были использованы какие-либо списки опечаток или интерпретации «Общих критериев», или подтверждающие документы;

b) *ПЗ*. Здесь приводится перечень тех профилей защиты, о соответствии которым утверждается в ПЗ или ЗБ;

c) *пакетам*. Здесь приводится перечень тех пакетов, на которые имеются ссылки в ПЗ или ЗБ. Обычно утверждается о соответствии одному из ОУД, определенному в ISO/IEC 15408-3, возможно с расширением. Это утверждение о соответствии также относится и к любому ОО, разработанному в соответствии с этим ПЗ или ЗБ.

Когда ПЗ определен, то необходимо также определить, насколько этот ПЗ соответствует другим ПЗ и ЗБ. Существуют два вида соответствия:

a) *строгое*. В принципе, это означает, что это ПЗ должно содержать все требования соответствующих ПЗ/ЗБ;

b) *очевидное*. В принципе, это означает, что требования этого ПЗ должны быть «эквивалентны» требованиям соответствующих ПЗ/ЗБ.

В том случае, когда ПЗ разрабатывается как точная и полная спецификация для закупаемого или разрабатываемого продукта, предназначенного только для личного пользования, то требуется его «строгое» соответствие. Если ПЗ предназначается для какой-либо другой цели, то используется «очевидное» соответствие.

Если же необходимо соответствие ПЗ функциональному пакету или другому ПЗ, то его постановка задачи безопасности, цели безопасности и требования безопасности должны быть совместимыми с этим пакетом или ПЗ.

В том случае, когда при разработке ПЗ или ЗБ в него добавляются дополнительные требования к требованиям, содержащимся в ПЗ, на которое имеется ссылка, то делать это надо очень осторожно, чтобы исключить возможность появления несогласованности, так как невозможно одновременно реализовать все требования в каком-либо ОО.

9 Постановка задачи безопасности

9.1 Введение

Этот раздел содержит руководство к разделу «Постановка задачи безопасности» спецификации ПЗ или ЗБ. К содержанию разделов «Постановка задачи безопасности» ПЗ и ЗБ предъявляются одни и те же требования.

Цель постановки задачи безопасности заключается в том, чтобы формальным способом определить характер и область действия задачи безопасности, которую предполагается адресовать ОО (рисунок 1).

Разделы «Постановка задачи безопасности» в некоторых ПЗ и ЗБ могут отсутствовать (раздел 15), но там, где они имеются, эти разделы, вероятно, будут являться наиболее важными разделами ПЗ или ЗБ, и очень опасно поручать их разработку внешним подрядным организациям.

Применимость результатов оценки сильно зависит от ЗБ, а применимость ЗБ сильно зависит от качества ПЗБ. Следовательно получение хорошей ПЗБ зачастую оправдывает затраты значительных ресурсов и применение строго определенных процессов и исследований. Если задача поставлена некорректно или описана неоднозначно, тогда и все остальное содержание ПЗ или ЗБ также будет некорректным.

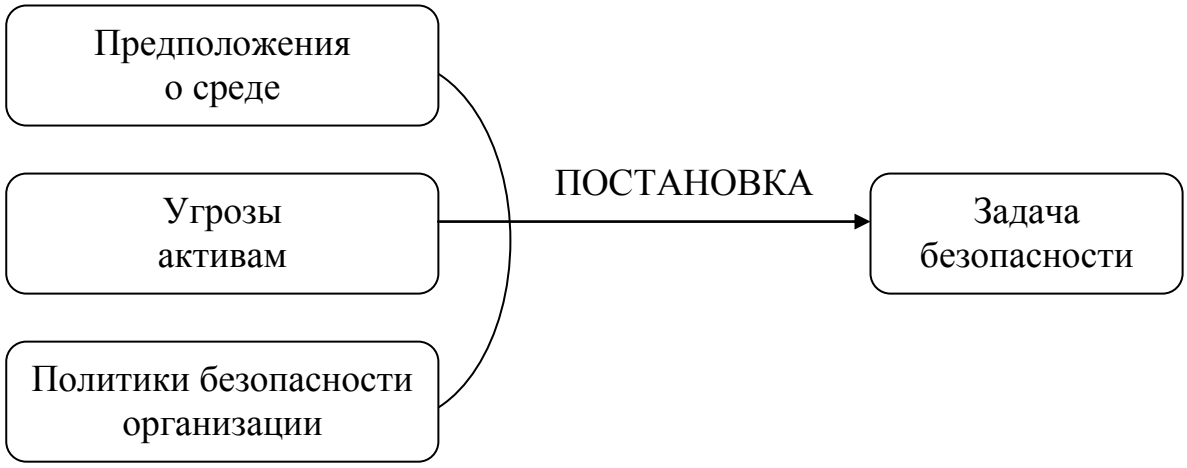

Рисунок 1 - Постановка задачи безопасности

Независимо от того, кем является потребитель - разработчиком или заказчиком, и независимо от того, будут ли ПЗ или ЗБ использованы в процессе закупки по спецификации или методом отбора, для него будет иметь первостепенное значение *получение правильной ПЗБ*.

В последующих разделах ПЗ и ЗБ показывается, как задача безопасности будет адресована ОО в комбинации с его средой. Следовательно, важно должным образом проверить, является ли ПЗБ понятной, лаконичной и непротиворечивой.

При разработке ПЗБ не предполагается и не предписывается использование какого-либо конкретного процесса или методологии; потребитель может использовать любой предпочтительный для него метод. В помощь начинающему разработчику ПЗ и ЗБ в настоящий раздел включено подробное описание простой методологии, которая надежна, проверена на практике и создана для работы в ряде организаций и сред. Она основана на ряде действий, выполняемых в следующей последовательности:

a) идентификация и утверждение неформальных требований безопасности;

b) идентификация и подробное описание потенциальных угроз с помощью формального анализа угроз;

c) документирование применяемых политик;

d) документирование существующих предположений;

e) согласование и проверка завершенной спецификации ПЗБ.

Независимо от используемой методологии предполагается, что ПЗБ представляет собой формализованное описание существующего неформального требования безопасности. Согласно рекомендуемой методологии вначале должны быть выполнены идентификация и утверждение

неформального требования, даже если оно отсутствует в ПЗ или ЗБ. Неформальное требование может быть очевидным и хорошо описанным. В других случаях большую часть работы при разработке ПЗБ может составить только идентификация неформального требования и получение подтверждения от руководства и других заинтересованных сторон, что это требование корректно и полностью соответствует их требованиям безопасности.

Вышеуказанная методология также содержит два других аспекта, которые позволяют значительно сэкономить время и избежать неопределенностей и сомнений на последующих этапах разработки ПЗ/ЗБ. К этим аспектам относятся:

a) документирование учтенных угроз;

b) разработка логического обоснования ссылки на неформальное требование безопасности при ПЗБ.

Учтенными угрозами являются угрозы, которые могут или не могут быть отнесены к продукту, но которым, если необходимо, будут противодействовать функциональные возможности безопасности, включенные в ОО по другим причинам. Если эти угрозы в ПЗБ не были задокументированы, то весьма вероятно, что при рассмотрении ПЗ/ЗБ относительно них могут возникнуть определенные вопросы, или при изменении требования функциональная возможность не сможет отреагировать на это изменение и оказать противодействие учтенной угрозе.

Оценка рассматриваемой ПЗБ не требует доказательств: не нужно пытаться выяснять происхождение содержащихся в ней требований безопасности. Если для ПЗБ не разработано логическое обоснование, то всегда существует риск, что часть неформального требования может быть утеряна в процессе создания ПЗБ, и это не обнаружится до начала использования продукта, когда окажется, что он не пригоден. Следовательно, логическое обоснование обеспечивает важную проверку согласованности и полноты.

В общем случае при ПЗБ необходимо избегать, где это возможно, любых рассуждений о форме ОО, отвечающей предъявляемым к нему требованиям, например, подробностей относительно функций безопасности ОО. Рассуждения о том, как будет решена задача безопасности ОО, должны быть оставлены для последующих разделов ПЗ или ЗБ. Конечно, когда частное решение является обязательной частью неформального требования безопасности, это решение должно стать частью ПЗБ, тогда будет обеспечено и его документирование, и обоснованы ограничения для последующих проектных решений.

9.2 Неформальные требования безопасности

9.2.1 Введение

Существует множество документов относительно задачи безопасности и предполагаемых путей ее решения, которые должны быть определены и изучены до начала постановки задачи безопасности. Содержащиеся в этих документах требования и ограничения используются при формировании неформального требования безопасности. Далее будет необходимо идентифицировать и задокументировать это требование, что всегда представляет некоторую трудность. Таким образом, эти действия становятся первым шагом рекомендуемой методологии.

9.2.2 Источники информации

9.2.2.1 Краткий обзор

Существует множество методов, согласно которым аспекты неформального требования безопасности могут быть идентифицированы. Далее будут рассмотрены некоторые из них. Возможно, что для конкретной организации общая методология, описанная в настоящем стандарте, не применима. В этом случае требования безопасности должны быть тщательно и основательно продуманы. И все-таки возможно, что предлагаемые далее источники информации могут быть полезны.

9.2.2.2 Обязательные функциональные возможности

Функциональные возможности безопасности могут быть частью предназначения рассматриваемого продукта. Это особенно относится к COTS-продуктам, услуги безопасности которых могут быть существенной частью спецификации продукта и доступны через программные интерфейсы приложений (Application Program Interface, API) или человеко-машинные интерфейсы (Human Computer Interface, HCI).

Если функциональные возможности безопасности являются частью документированного требования пользователя, то они являются частью ПЗБ.

9.2.2.3 Определение рисков

Если для предлагаемой системы и даже для COTS-продукта риски информационной безопасности были уже определены, тогда с помощью элементов управления безопасностью ИТ необходимо эти риски снизить. Эти риски являются частью задачи безопасности.

Существует множество методологий определения рисков. При использовании всех этих методологий обычно предполагается, что для существования риска необходимы три фактора:

a) актив, некоторая часть которого может быть повреждена некоторым способом;

b) угроза, то есть что-то или кто-то, которые могут нанести вред активу;

c) уязвимое место, то есть путь, по которому актив может быть поврежден.

Если какой-либо из этих трех факторов отсутствует, то и риск не существует. Эта форма модели принята в ISO/IEC 15408. Если же при определении рисков фактически была использована несовместимая модель риска, то могут возникнуть проблемы с преобразованием результатов в форму, подходящую для использования в ПЗБ.

9.2.2.4 Определение угроз

Упрощенным методом определения рисков является определение угроз. Этот метод допускает, что если существует угроза, то активы могут быть повреждены и, следовательно, риск существует. В этом случае идентифицированные угрозы являются частью задачи безопасности.

Определение угроз особенно подходит для случая, когда субъект, пытающийся идентифицировать и поставить задачу безопасности, не является владельцем активов, которые необходимо защитить, и поэтому не может определить риски или величину активов.

9.2.2.5 Политика руководства организации

Требование безопасности может возникнуть в результате принятия руководством организации политики, например, в конкретной организации элементы управления безопасностью ИТ всех систем должны соответствовать определенному стандарту.

Такая политика иногда называется «политикой минимальных стандартов» либо «политикой допустимых норм», или «политикой исключения рисков». Политика может быть произвольной, например, она может быть разработана с учетом опыта аналогичных организаций, или она может иметь логическое обоснование, например, эта политика должна соответствовать требованиям законодательства или условиям договоров, заключенных с заказчиками.

Несомненно, что даже там, где политика разработана на основе законодательства или договоров, может случиться так, что сертифицированные элементы управления безопасностью не подойдут для конкретной системы или организации, или могут быть применены только частично.

9.2.2.6 Презентационная политика

Требование безопасности может возникнуть из желания продемонстрировать, что в организации или COTS-продукте имеются надежные элементы управления безопасностью ИТ. Эта политика может возникнуть из-за потребностей маркетинга или желания использовать передовой опыт.

Задачи безопасности этого типа хорошо согласуются с оценкой по ISO/IEC 15408, поскольку в результате независимой успешной оценки с использованием апробированного средства оценки будет получен официальный сертификат, подтверждающий, что элементы управления существуют. Для идентификации подходящих элементов управления могут быть использованы опубликованные ПЗ.

Недостаток политик этого типа заключается в том, что они основаны на результатах сертификации или демонстрации соответствия, а не на выборе элементов управления безопасностью, которые важны для

определенного продукта. Это может стать причиной возникновения проблем, которые будут обнаружены при обосновании в ПЗБ необходимости элементов управления. Использование элементов управления придется рассматривать как решения политики, автор которой возможно не захочет признать истинную причину своего выбора.

9.2.2.7 Политика оценки

Организация может иметь политику, согласно которой используются продукты ИТ, оценка которых выполнена по схеме, основанной на ISO/IEC 15408 или «Общих критериях», независимо от элементов управления безопасностью, которые они реализуют.

Выполнить это требование будет сложно. Если задачу безопасности нельзя адресовать в какой-либо раздел политики, то она, следовательно, была определена не правильно.

Тем не менее, такие политики на практике встречаются, и на их основе задаются требования к разрабатываемому ЗБ.

9.2.3 Документирование неформальных требований

Наилучшим источником информации для задачи безопасности являются результаты определения рисков безопасности. Достаточно иметь доступ к результатам определения рисков, только маловероятно, что они будут исчерпывающими. В большинстве методологий по определению рисков вводится понятие прямой пропорциональности, то есть риск может быть допустимым, если вероятность ущерба очень мала или последствия ущерба не значительны. Впоследствии определение как приемлемого, так и неприемлемого рисков позволит трансформировать задачу безопасности в рабочий проект. Если окажется, что элементы управления, необходимые для устранения конкретного риска, трудно реализуемы или их трудно оценить, то все же можно достичь приемлемого общего уровня риска, используя другие элементы управления с разными способами противодействия другим потенциальным рискам.

Конечно, определение рисков, выполненное третьей стороной с учетом своих собственных целей, не может составить такое же заключение о рисках, которое должен сделать потребитель. В таких случаях потребитель должен использовать результаты определения рисков с осторожностью.

Если не возможно описать часть задачи безопасности на основе рисков, то у нее практически бесспорно будет произвольная основа, которая не может быть модифицирована или скорректирована. Важно, чтобы это было отмечено в неформальном описании.

Важная информация может относиться не только к продукту ИТ, который нужно разработать, но также к его среде. Среда определяет уровень доверия, который может быть установлен для персонала, организационных и физических элементов управления. К общим помещениям и закрытой серверной комнате предъявляются разные требования безопасности. Если этими требованиями будет установлено, что в помещение допускается только определенный персонал и там

разрешаются только конкретные организационные и физические элементы управления, то эти требования будут являться важной частью постановки задачи безопасности.

На основе информации о рисках и элементах управления могут быть приняты проектные решения относительно того, как должны быть реализованы определенные функции безопасности, например, принято решение об использовании биометрической аутентификации вместо паролей или об использовании определенных протоколов связи, например, протокола SSL/TLS, который обеспечивает определенные характеристики безопасности.

Некоторые части задачи безопасности не могут быть решены с помощью технических средств, они могут быть решены только с помощью персонала, организационных и физических элементов управления. Тем не менее, они являются частью задачи безопасности и должны быть задокументированы. На самом деле, любой аспект задачи безопасности, который уже решен, должен быть задокументирован как часть неформального требования безопасности.

Когда вся доступная информация будет отсортирована и проверена на отсутствие несогласованности, она затем должна быть подразделена на три части:

a) потенциальные атаки, которые должен учитывать продукт;

b) атрибуты или функции безопасности, которыми должен обладать продукт;

c) атрибуты или функции безопасности, которыми не должен обладать продукт.

Эти различия важны, так как они будут рассматриваться впоследствии в других случаях. Потенциальные атаки должны быть рассмотрены как угрозы для ОО и приняты контрмеры. Атрибуты и функции безопасности, которыми продукт должен обладать, включая обязательные решения безопасности, должны соответствовать ПБОр. Атрибуты и функции, которые продукт не должен иметь, должны быть отражены в соответствующих предположениях, которые будут рассмотрены ниже.

Другие части неформального требования, полученные из других источников, могут частично совпадать или даже противоречить друг другу. Такая ситуация для атрибутов или функций безопасности встречается нередко и является подсознательной реакцией на определенную потенциальную атаку. Подобным же образом атаки определенного типа подсознательно могут считаться слишком трудными или слишком дорогими и при этом не эффективными, поэтому заявленные соответствующие функции безопасности не нужны. Подобные несогласованности должны быть устранены прежде, чем неформальная спецификация будет использована в перспективе. Необходимо стремиться к тому, чтобы каждый аспект неформального требования был сформулирован только один раз.

9.3 Идентификация и спецификация угроз

9.3.1 Введение

Как только будет задокументировано неформальное требование безопасности, а атаки и атрибуты идентифицированы, то логично, что следующим шагом в подготовке к ПЗБ станет проведение анализа угроз с целью идентификации угроз, позволяющих реализовать атаки. Все угрозы, воспринимаемые как существенные для рассматриваемого ОО, должны быть идентифицированы.

Анализ и спецификация угроз обычно является более сложным и трудным делом, чем определение политики и предположений, и поэтому сначала лучше всего определить их. С другой стороны, если неформальные требования большей частью были получены из решений политики или обязательных требований (см. 9.2), то возможно, что вначале будет легче разработать те разделы ПЗБ, которые содержат политики и предположения (см. 9.4 и 9.5), после чего выполнить анализ угроз, а потом пересмотреть политики и предположения.

Если политики и предположения могут быть определены без затруднений, то тогда их можно немедленно использовать для учета угроз, которые далее не надо рассматривать, анализ угроз таким образом будет упрощен.

Для выполнения анализа угроз необходимо выполнить три действия:

a) решить, какую методологию анализа нужно использовать;

b) идентифицировать пользователей этой методологии;

c) применить методологию.

9.3.2 Выбор методологии анализа угроз

Лучшей методологией идентификации потенциальных угроз будет та, на основе которой было получено неформальное требование безопасности. Если это требование было получено на основе результатов определения рисков, тогда список угроз может быть доступен уже после первого определения рисков. В другом случае будет возможно идентифицировать соответствующие угрозы из другой имеющейся в наличии и доступной информации.

К сожалению, в большинстве случаев исчерпывающая информация бывает не доступна, и поэтому должен быть выполнен повторный анализ угроз.

Существует множество методологий, которые могут быть использованы для выполнения анализа угроз. Тем не менее, большинство разработчиков ПЗ и ЗБ используют один из трех методов:

a) анализ с помощью дерева угроз;

b) поиск базы данных об угрозах;

c) специальная идентификация.

Среди вышеперечисленных методов анализ с помощью дерева угроз является наилучшим документально оформленным и общепризнанным методом. Он основан на конструкции деревьев решения, этот хорошо известный метод декомпозиции широко используется при решении задач управления рисками и при проектировании надежности.

Анализ с помощью дерева угроз начинается с самого общего абстрактного описания полного набора потенциальных угроз для конкретного типа продукта ИТ, а затем добавляются большие подробности с помощью итеративного метода и на каждом этапе описания угроз детализируются. Метод называется деревом угроз, поскольку первое абстрактное определение рассматривается как корень дерева, а каждый новый уровень последующей детализации создает набор новых, более детальных узлов, соединенных с корнем. Каждый из этих узлов затем становится корнем нового поддерева. В конечном счете, описания вершин деревьев станут в достаточной мере конкретными, потребность в их дальнейшей детализации отпадет, и они могут быть использованы в качестве существующих угроз, которые должны быть определены в ПЗ или ЗБ. Дерево также обеспечивает логическое обоснование для выбора угроз, включаемых в ПЗ или ЗБ, и дает уверенность в том, что все существенные угрозы были учтены.

Вторым альтернативным методом анализа угроз является поиск базы данных, основанный на обстоятельном просмотре одной или нескольких определенных баз данных с характерными угрозами с целью увидеть, какие элементы соответствуют определенным атакам для рассматриваемого продукта ИТ. Соответствующие базы данных доступны из многих источников. Самые большие национальные схемы оценки предоставляют информацию о характерных угрозах обычно по запросу, форма которого допускает возможность поиска базы данных.

К преимуществам поиска базы данных относятся достаточно широкий выбор и диапазон угроз, принимаемых во внимание, и то, что они представлены и определены логичным способом. Единственным недостатком этого метода является то, что специфические угрозы для конкретного продукта могут быть не включены в базу данных и, следовательно, не идентифицированы. К тому же описания угроз в базе данных могут быть слишком общими, чтобы их можно было легко идентифицировать и применить для рассматриваемого продукта. Также может обнаружиться, что слишком много угроз покажутся применимыми, и поэтому будет необходимо произвести их произвольную выборку.

При применении третьего альтернативного метода анализа угроз происходит идентификация угроз неструктурированным способом, базирующемся только на анализе рассматриваемого продукта ИТ. Его лучше не использовать, так как разработчик или владелец задачи должны в этом случае «мыслить неординарно». Нарушители могут быть гораздо более опытны или изобретательны в обнаружении существующих угроз.

Если и задача безопасности, и окружающая среда хорошо определены, то построение дерева угроз обычно является наиболее эффективным методом. Если задача определена только в общих чертах, или среда - неопределенная или произвольная, то простой последовательный поиск базы данных об угрозах может более оперативно предложить список потенциальных угроз, чем методологический нисходящий анализ. Это особенно относится к разработчикам COTS-продуктов, которые обычно в большинстве случаев не могут знать, в каких реальных средах будут использованы их продукты.

Если неформальное требование безопасности было задано первоначально политикой или предписанными функциями безопасности, то не удивительно, что при проведении анализа угроз не будут идентифицированы все существующие угрозы и даже противодействующие им обязательные атрибуты безопасности.

В зависимости от использованной методологии анализа угроз и происхождения неформального требования безопасности, угрозы могут быть идентифицированы, но впоследствии учтены или идентифицированы как аналоги других требований (например, политики). Документирование всех возможных угроз ISO/IEC 15408 не предусматривается, несмотря на то, что в этом случае впоследствии будет очень трудно понять ПЗБ в целом и в частности при необходимости ее модификации и фиксации изменений. Необходимо документировать только учтенные угрозы. Обычно это можно сделать способом, описанным в 9.5.

9.3.3 Описание угроз

9.3.3.1 Введение

Если все предшествующие версии ISO/IEC 15408 содержали требование, чтобы каждая угроза была только идентифицирована и обоснована, то третье издание ISO/IEC 15408 требует, чтобы каждая угроза была описана относительно агента угрозы, активов и негативного воздействия - с объяснением того, что имеются в виду активы определенных типов, поскольку в случае COTS-продуктов реальные активы, которые нужно защищать, неизвестны разработчику ПЗ или ЗБ.

9.3.3.2 Агенты угроз

В ISO/IEC 15408 агенты угроз определены как «логические объекты, которые могут оказать негативное воздействие на активы». При описании угроз в ПЗ и ЗБ предпочтительно использовать по возможности простые описания агентов угроз. Должен использоваться фиксированный список, состоящий из пяти типов агентов угроз:

a) нарушители;

b) авторизованные пользователи;

c) привилегированные пользователи;

d) администраторы;

e) владельцы системы и разработчики.

Нарушителем является лицо, которое не имеет полномочий на доступ к активам, защищаемым продуктом ИТ. К нарушителям также относятся лица, которые являются авторизованными пользователями, но скрывают свою личность. Поскольку нарушитель не известен владельцу системы, то существуют незначительные средства сдерживания, не считая тех случаев, когда атака нарушителя обнаружена и его личность установлена, например, путем отслеживания телефонных звонков или если его узнали сотрудники службы охраны.

Авторизованным пользователем является лицо, которое имеет полномочия на использование продукта ИТ в соответствии с установленной политикой безопасности, и может иметь доступ к защищаемым продуктам активам с разрешения владельца этих активов. Авторизованные пользователи известны владельцу системы и от нанесения ущерба активам их должно сдерживать существование ответственности за свои действия.

Привилегированным пользователем является лицо, которое уполномочено использовать продукт ИТ способом, не соответствующим установленной политике безопасности, и может иметь доступ к активам без явного разрешения владельца актива. В большинстве случаев привилегированными пользователями являются системные администраторы. Тем не менее, существуют и другие типы привилегированных пользователей, например, эксплуатационный персонал аппаратных средств и программного обеспечения. Привилегированные пользователи не могут быть остановлены при нанесении ущерба продукту ИТ, но они могут быть впоследствии признаны ответственными за свои действия.

Администраторами называют тех лиц, которые отвечают за обеспечение правильного функционирования продукта ИТ, когда-то установленного в конкретной среде. Следовательно, администраторы отвечают за установку элементов управления, которые защищают активы от ущерба, а также обнаруживают повреждения активов. Администраторы могут быть ограничены в своих действиях, но если они выполняют свои действия неправильно, то ущерб активам может быть нанесен другими лицами.

Владельцами системы и разработчиками называют тех лиц, которые отвечают за спецификацию, проектирование и реализацию системного или COTS-продукта, но которые заведомо не будут использовать свой опыт и знания, чтобы получить доступ к защищаемым активам. Хотя они и не смогут непосредственно нанести ущерб активам, но в том случае, когда они принимали неправильные решения, продукт не сможет должным образом защищать активы.

Одно или несколько из этих определений могут использоваться для описания одного лица в разные промежутки времени. Различие будет заключаться только в том типе угрозы, которую это лицо представляет, действуя как агент угрозы определенного вида в конкретный промежуток времени.

В вышеприведенном списке отсутствует только один возможный вид агента угрозы, который может иметь важное значение для некоторых задач безопасности – природные катаклизмы (так называемый «форс-мажор»), например, землетрясения, в этом случае человеческий фактор отсутствует. Обычно ответственность за рассмотрение таких угроз несут владелец системы и разработчик, несмотря на то, что эти угрозы не сформулированы или не возникнут. В некоторых случаях, описание такого агента как «никто» или «природа» может быть более ясно или более приемлемо для владельца задачи.

9.3.3.3 Типы активов

Основные активы, учитываемые при анализе угроз, должны быть правильно идентифицированы. В большинстве случаев методологии анализа угроз могут оперировать или уязвимостями, или соотношениями «нарушители - негативные воздействия», но независимо от того, какая используется методология, активы должны быть четко и хорошо описаны.

В системе ИТ часто имеется возможность точной идентификации активов, которые нужно защищать, это сформулировано в соответствующем разделе описания системы. Как будет фактически использоваться COTS-продукт зачастую неизвестно и, следовательно, тем не менее, существует возможность идентификации типов активов, для защиты которых предназначен этот продукт.

Активы систем ИТ обычно относятся к одному из трех нижеперечисленных классов:

a) информационные;

b) процессные;

c) физические.

Информационные активы представляют собой данные, которые представляют ценность для владеющей ими организации. Возможные типы информационных активов:

- общие данные;
- системные данные;
- базы данных «Специалисты»;
- данные клиентов.

В базах данных «Специалисты» содержится информация, которая представляет ценность только для некоторых пользователей. Примерами могут быть база данных персонала (представляет ценность только для отдела кадров) или база данных заказчиков (представляет ценность только для отделов обработки заказов и реализации).

Данные клиентов могут содержать их персональные данные, не принадлежащие владельцу системы, для которых установлен особый режим обработки и защита которых закреплена на законодательном уровне.

В системе обычно имеется возможность идентификации имен и характеристик фактических баз данных или других информационных активов, которые должны быть защищены.

В самом простом случае все данные могут рассматриваться как данные, имеющие равную ценность и одинаково подверженные рискам атак, и поэтому их можно представить как один информационный актив, примерно называемый «данные пользователя».

Тем не менее, часто возникает необходимость различать системные данные, то есть отличать данные, используемые ФБО, от других данных. Если системные данные будут модифицированы или удалены, то возможно, что ФБО станут действовать неправильно, в результате чего появится возможность проведения других типов атак, а если при этом будут модифицированы и другие данные, а искажены только непосредственно задействованные данные, то ФБО будут продолжать свое функционирование и защищать другие активы.

Этот случай является до некоторой степени общим для этих двух типов информационных активов: первый - это данные ФБО, а другой - все другие данные, защищаемые продуктом.

Иногда разные типы данных ФБО могут быть уязвимы для разных атак или в случае их компрометации могут возникать разные последствия, и поэтому необходимо их различать. К особым типам данных ФБО могут быть отнесены:

- данные конфигурации ФБО;
- база данных с данными аутентификации;
- записи аудита.

Иногда должны быть выделены очень редко встречающиеся и специфичные формы данных, которые могут быть подвержены специфичной атаке, например, криптографические ключи.

Процессные активы представляют собой приложения, с помощью которых данные обрабатываются или анализируются. Различие процессных активов от информационных активов заключается в том, что относящиеся к ним данные имеют небольшую ценность без возможности обработки с помощью соответствующих приложений. К возможным типам процессных активов относятся активы:

- финансовые;
- телекоммуникационные;
- логистические;
- производственные;
- делопроизводства.

Финансовые приложения могут включать платежные ведомости, управление инвестициями или операции с бухгалтерскими счетами.

Приложения «Системы телекоммуникаций» могут обрабатывать электронную почту или информацию внутренней/корпоративной сети.

Приложения «Логистические системы» могут выполнять обработку заказов, управление складами или планирование ресурсов.

Производственные приложения могут осуществлять управление производственными процессами в режиме реального времени.

Приложения «Делопроизводство» предназначены для ведения автоматизированного делопроизводства в организациях.

В системе обычно существует возможность идентификации имен и характеристик фактических процессов, которые нужно защищать.

Процессные активы подвержены только модификации или атакам типа «отказ в обслуживании». Например, функциональные возможности программного обеспечения взаимодействующих приложений могут быть изменены возможно для того, чтобы удалить проверку полномочий или чтобы изменить обработку финансовой информации. Для всех процессных активов обычно достаточно одного названия - «программное обеспечение приложений» или т.п.

Физические активы представляют собой оборудование для обработки актуальной информации, используемое для работы с информацией и процессными активами. К возможным типам физических активов относятся:

- критическая сетевая инфраструктура;
- портативные персональные компьютеры;
- центры обработки данных.

Обычно в задаче безопасности ОО не рассматриваются вопросы защиты физических активов, физическая защита ОО либо отсутствует, либо предусматривается с помощью предположений относительно среды использования ОО. Вследствие этого физические активы, как правило, в ПЗ или ЗБ не фигурируют. Однако существуют методы, которые могут быть использованы для защиты физических активов, например, автоматическое прекращение работы при отключении электропитания, и в таких случаях в ПЗ или ЗБ могут быть отражены вопросы защиты физических активов.

Необходимо иметь в виду, что не следует идентифицировать слишком много активов или типов активов. Если два актива или два типа активов будут подвергаться одной и той же атаке, последствия которой будут для них одинаковы, то эти активы должны быть сгруппированы в комбинированный тип актива. Многие ОО защищают только два типа активов: данные ФБО и данные пользователя. Более шести типов активов вероятно неуместны для всех ОО, кроме ОО, для которых предполагается использовать очень сложные или оригинальные возможности защиты.

Некоторые активы или типы активов, которым необходима защита, могут быть исключены из раздела «Постановка задачи безопасности». В этом случае эти активы должны быть внесены в отдельный список: эта информация будет впоследствии необходима для объяснения, почему эти активы не были учтены при проведении анализа угроз.

9.3.3.4 Негативные воздействия

В ISO/IEC 15408 отсутствует какое-либо руководство по описанию негативных воздействий. Относительно агентов угроз рекомендуется следующее – агентам угроз должны соответствовать наборы простых (по возможности) действий. Одним из самых простых и наиболее

исчерпывающих наборов действий на настоящий момент является следующий набор:

- несанкционированный доступ;
- несанкционированная передача прав доступа;
- отрицание факта санкционированного доступа;
- отсутствие подотчетности.

Было установлено, что этот простой набор предусматривает почти все угрозы, которые вероятно могут быть обнаружены практически, хотя иногда конкретные негативные воздействия могут иметь совсем другие последствия, которые для упрощения обоснования должны быть описаны отдельно. Также могут быть и другие, специфичные типы негативных воздействий, которые естественно не относятся ни к одной из вышеуказанных групп. Это должно стать очевидным при рассмотрении неформального требования безопасности, в этом случае должно быть приведено отдельное объяснение.

Альтернативным методом является описание негативных воздействий с точки зрения последствий успешной атаки, например, нарушение конфиденциальности. Этот метод редко используется вследствие того, что он неоправданно специфичен и имеет ограниченное применение.

9.3.4 Применение выбранной методологии анализа угроз

После выбора методологии анализа угроз и подготовки необходимой для этой методологии информации необходимо составить список потенциальных угроз.

Большинство потенциальных угроз практически может быть быстро учтено. Существуют два конкретных метода: определение не допустимых или допустимых угроз и определение угроз, уже учтенных в политике.

Многие типы угроз будут учтены уже при определении неформального требования безопасности или они будут исключены из области применения продукта ИТ, или уже было принято решение о допустимости этих угроз, поскольку связанные с ними риски незначительны или переданы третьей стороне (например, страховой компании).

Исключением являются только COTS-продукты, например, разработчик операционной системы может принять решение не включать в продукт антивирусную защиту, предполагая, что покупатель захочет купить дополнительный продукт антивирусной защиты другого разработчика или будет использовать продукт в среде, изолированной от вирусов.

Обычно для обнаружения допустимых угроз для систем необходима оценка активов, которую производитель COTS-продукта не может выполнить.

Существенная информация о снижении угроз обычно становится очевидной из списка запрещенных для этого продукта действий. Если

такого списка нет, его необходимо составить. Запрещенные действия должны быть записаны в форме предположения (см. 9.5).

Независимо от анализа реальных угроз для многих продуктов ИТ решение о включении функциональных возможностей безопасности принимается заранее. Это является общим случаем для COTS-продуктов, например, разработчик операционной системы обычно хочет включить функции идентификации и аутентификации пользователей, даже если разрабатываемый продукт предназначается для одного пользователя.

Если эта предписанная функциональная возможность будет учитывать конкретный тип угроз, то в этом случае отсутствует необходимость в последующем исследовании, чтобы убедиться в том, действительно ли эта угроза существует; защита будет предусмотрена независимо от этого.

Какими угрозами для важной информации можно пренебречь, обычно очевидно из списка атрибутов, которыми должен обладать продукт ИТ. В противном случае, наличие этих атрибутов должно быть подтверждено и добавлено к этому списку. Это должно быть также записано в форме утверждения политики (см. 9.4).

Все остальные угрозы должны быть определены и учтены, составлен полный список потенциальных угроз, в котором каждая угроза должна быть описана с учетом агентов, активов и негативных воздействий.

Некоторые угрозы могут быть применимы только к конкретной системе, но решение о том, какие элементы управления безопасностью в границах среды будут противодействовать этим угрозам, предварительно было принято в разделе «Область применения» задачи безопасности. Это станет возможным только тогда, когда для парирования некоторых угроз в среде будут приняты соответствующие меры (например, когда необходима физическая защита). Должен быть составлен список всех этих угроз, в котором следует сделать примечание, что он будет необходим при формулировании целей безопасности для среды.

Однако нельзя преждевременно принимать решение о том, как будут парированы угрозы, порождаемые ОО или его средой. Иначе после того, как будут выбраны и разработаны элементы управления, станет невозможным последующее проектирование.

9.3.5 Практические рекомендации

Наличие угроз означает, что существуют возможные пути атак на продукт ИТ. Следовательно, угрозы должны быть сформулированы с учетом этого. Наилучший способ для этого - использование такой формы глагола как «может».

Пример - T.UNAUTH Неуполномоченное лицо может попытаться получить доступ к ресурсам ОО и использовать их.

Описание каждой угрозы должно начинаться с ее уникального названия, которое будет использоваться для ссылок. Содержание описаний угроз должно быть кратким и точным. Общепринято, что

названия угроз начинаются с буквы «Т», это способствует их идентификации.

Методологии, описанные в этом разделе или какие-либо другие, нельзя использовать безоговорочно. Они должны быть адаптированы и интерпретированы с учетом требований конкретной задачи безопасности. Если на практике не получается разработать конкретную форму классификации, то следует начать это делать заново, используя другой метод.

Угрозы могут быть объединены, если аналогичны их агенты, активы и негативные воздействия. Это уменьшит размер списка угроз и потом сэкономит время, а впоследствии для противодействия этим угрозам зачастую будут использоваться одни и те же элементы управления. В то же время, когда воздействия угрозы явно различаются в зависимости от факторов похожих агентов угроз или соответствующих активов, то будет целесообразно разделить эту угрозу на множество угроз, которые будут более точно сформулированы, это будет способствовать большему пониманию и впоследствии позволит сэкономить время.

Информация, указывающая на то, что угрозы могут быть учтены, часто выражена косвенно с помощью утверждения.

Пример - На должность администраторов могут быть приняты надежные и компетентные лица, не имеющие злых умыслов.

Это утверждение сформулировано с точки зрения агента угроз и эффективно снижает большинство типов угроз, обычно ассоциированных с этим типом агента. Некоторые из этих типов угроз характерны для администраторов и могут быть, следовательно, полностью устранены. Другие типы угроз все еще будут существовать, но можно будет ограничиться только другими соответствующими агентами угроз, например, обычными пользователями. Не следует забывать добавлять предположение, которое позволит уменьшить объем этих угроз в перечне предположений.

В некоторых случаях будет не возможна идентификация только тех агентов угроз или негативных воздействий, которые связаны с неприемлемым риском. Например, неспособность базовой абстрактной машины обеспечить выполнение заданной ей модели безопасности. В этих случаях бессмысленно создавать описания, основанные на догадках или воображении. Неприемлемые угрозы должны быть определены в задаче безопасности, они должны быть названы и соответственно обоснованы.

Как только будет подготовлен окончательный список угроз, его надо будет обязательно проверить на наличие полноты и согласованности. Была ли предусмотрена защита от всех возможных угроз, которые были классифицированы по типам активов или типам агентов угроз? Существуют ли для отражения подобных угроз аналогичные способы?

Если отсутствуют, то имеется ли для этого веская причина? Несмотря на то, что впоследствии при подготовке ПЗ или ЗБ могут быть обнаружены все несогласованности и упущения, выполнение проверок на этом этапе в дальнейшем позволит сократить время и объем доработки.

Возможно, что в результате анализа угроз не были идентифицированы какие-либо угрозы, которые содержались в соответствующем списке ОО. Это может случиться, например, когда ПЗ разрабатывается только на основе требований общей корпоративной или государственной политики. Это вполне допустимо при оценке по ISO/IEC 15408; если подраздел «Угрозы» остался не заполненным, это означает, что не были определены какие-либо специфические угрозы.

9.4 Идентификация и спецификация политик

Постановка задачи безопасности также должна содержать список необходимых ПБОр, которым должен соответствовать ОО. Политики обычно значительно легче определить и описать, чем угрозы. В том случае, когда используется рекомендованная выше методология, то уже имеется список атрибутов или характеристик безопасности, которыми должен обладать продукт ИТ. Каждый из этих списков может быть переработан в ПБОр.

Политики содержат утверждения о том, что должен делать продукт ИТ независимо от потенциальных угроз или других условий. В подобных требованиях обычно используется форма глагола «должен».

Пример - P.IDAUTH Администраторы для получения доступа к функциям или данным любого ОО должны пройти процедуру аутентификации.

Как и в случае с угрозами, каждая политика должна иметь уникальное название, которое будет использоваться для ссылок. Описания политик должны быть краткими и точными. Общепринято, что названия политик начинаются с буквы «Р», это способствует их идентификации.

Термин «политика безопасности организации» может вводить в заблуждение пользователей вследствие того, что некоторые ПБОр могут относиться только к одной системе, на которую распространяются требования конкретного ПЗ или ЗБ, а не ко всем системам этой организации. В настоящем стандарте обычно используется более простой термин «политики».

Большинство используемых политик должно быть идентифицировано во время идентификации неформального требования безопасности или во время анализа угроз. Несмотря на это, должна быть выполнена заключительная проверка идентификации любых других политик, важных для задачи безопасности.

Политики используются для определения:

- обязательных функций безопасности ОО;

- обязательных технологий/методов, которые будут использоваться при реализации конкретных функций безопасности (которые безоговорочно необходимы для реализации этих функций).

Политики также могут использоваться для защиты от угроз. Они предназначены для этого, если:

- отсутствует уверенность в наличии конкретной угрозы, но независимо от этого в политике принято решение о необходимости защиты от этой угрозы;

- в политике принимается решение о необходимости защиты от конкретной угрозы, при этом, например, определяются:

a) какие элементы управления помогут предотвратить успешную атаку; или

b) что будет происходить во время атаки;

- решение в политике принимается для того, чтобы применить конкретный метод защиты от множества сопутствующих угроз.

В этом случае отсутствует возможность сопоставления величины угрозы с защитой, установленной политикой, если в политике не представлена некоторая дополнительная информация, наличие которой в описании угрозы не предполагается.

По завершению разработки политик необходимо проверить, не требуются ли внесение изменений или пересмотр действующей прежде ПЗБ, например, для исключения угроз, защита от которых теперь предусмотрена в политиках.

Практически большинство политик легко идентифицируются и четко формулируются. Тем не менее, существует несколько общих задач, которые необходимо отметить.

Иногда утверждения политики используются неправильно при формулировке требований для тех функций, которые ОО не должен или не может делать, но которые должны выполняться в среде ОО. Если требование не может быть реализовано ОО, то будет правильно определить его как предположение относительно среды (см. 9.5). Если предлагаемая политика не может быть выполнена ОО, средой или ими совместно, тогда утверждения политики будут бессмысленны или невыполнимы.

Во время постановки задачи безопасности и ее решения, границы предлагаемого ОО возможно будет необходимо изменять, чтобы передавать функции ОО его среде или наоборот. Возможно, что в результате этого политика будет становиться предположениями или предположения будут становиться политиками, или для этого может потребоваться заново определить политики или предположения с учетом новых границ ОО. Также для составных ОО, которые разделяются на несколько компонентов, адресуются разные задачи безопасности, а предположение для одного компонента часто реализуется другим

компонетом как требование политики. В таких случаях, тщательная формулировка утверждений политики позволит использовать их при других ПЗБ в качестве предположений, гарантирующих совместимость и легкую проверку согласованности.

Иногда в процессе подготовки постановки задачи безопасности бывает не ясно, будет ли политика реализована ОО или в его среде. Это допустимо; решение может быть принято при определении целей безопасности, когда требования для функционального назначения безопасности станут более понятными. Как цели ОО, так и цели среды, могут подтверждаться взаимосвязанными политиками. Политика может быть даже реализована частично ОО и частично средой.

Не для всех задач безопасности необходимы политики. Это вполне приемлемо при оценке по ISO/IEC 15408; если подраздел «Политики» остался не заполненным, это означает, что никакие соответствующие политики не были определены.

9.5 Идентификация и спецификация предположений

ПЗБ должна содержать список соответствующих предположений, которые ограничивают или исключают функции безопасности, обязательные для ОО. Если используется рекомендуемая настоящим стандартом методология, то уже имеется список атрибутов безопасности или функций, которыми не должен обладать продукт ИТ. Формулировка каждого из них может быть изменена в соответствии с предположением о среде или о предполагаемом использовании ОО.

Предположения должны содержать утверждения о том, чего не должен делать продукт ИТ, независимо от потенциальных угроз или других условий. Следовательно, они должны быть сформулированы как констатация факта.

Пример - A.PHYSICAL ОО будет находиться в физически защищенном помещении.

Предположения используются в двух случаях:

- чтобы показать, какие конкретные элементы управления или типы элементов управления будут предусмотрены в среде, а не в ОО;
- чтобы показать, какие конкретные угрозы или типы угроз могут быть учтены, поскольку для информационных ресурсов в предполагаемой среде они не существуют или не существенны.

В первом случае предположения могут быть наилучшим образом сформулированы при использовании глагола «будет», так как он подразумевает, что элементы управления должны быть предусмотрены, даже если не в ОО. Во втором случае предположения могут быть сформулированы наилучшим образом при использовании глагола в настоящем времени, например, «является».

Предположения об элементах управления, предусмотренных в среде, должны храниться отдельно от предположений об учтенных угрозах в качестве шаблона, необходимого чтобы облегчить демонстрацию пригодности целей безопасности для противодействия всем идентифицированным угрозам (см. 10.2).

Каждому предположению должно быть присвоено краткое название с целью упрощения использования ссылок. Описания предположений должны быть краткими и точными. Для облегчения идентификации общепринято начинать названия предположений с буквы «А».

Сформулировать предположения понятно и четко гораздо труднее, чем сделать то же для политик или угроз. Необходимо избегать использования таких глаголов, как например, «может» или «должен быть»: предположения являются констатациями факта.

Предположения относительно среды должны быть разделены на три области:

- физическая защита;
- персонал и процедуры;
- технические функциональные возможности за пределами ОО.

В ISO/IEC 15408 определены аспекты среды в части физической защиты, персонала и взаимосвязей. Тем не менее, практический опыт показал, что этого не достаточно. Многие предположения о внешних технических элементах управления естественно попадают под заголовок «Связность».

Пример - A.INTERNET ОО будет изолирован от сети Интернет.

Тем не менее, часто необходимы и другие предположения о технических элементах управления.

Пример - A.NO_DEV_TOOLS В среде ОО не предполагается наличие каких-либо инструментальных средств, которые позволят пользователям добавлять в систему новые функциональные возможности.

Во многих случаях требования политик и контрмеры от угроз должны выполняться как ОО, так и средой. Например, возможно, что для технических элементов управления в пределах ОО потребуются дополнительные организационные или физические меры, при наличии которых он будет работать эффективно. Потребность таких дополнительных мер в среде должна быть определена и выражена как предположения.

Предположения во время оценки не тестируются; они всегда принимаются как достоверные и истинные. Тем не менее, они полезны при демонстрации согласованности и полноты. Когда угрозы определяются методологически, то предположения должны показать логически обоснованную полную защиту. Некоторые угрозы можно игнорировать, а другие необходимо учитывать. В этом случае предположения необходимы

при установлении целей безопасности в части контрмер от угроз, чтобы показать, что предусмотрено их полное покрытие.

Многие предположения могут быть сделаны во время разработки спецификации неформального требования безопасности или во время анализа угроз. Несмотря на это, чтобы определить любые другие важные предположения, должно быть проведено полное исследование, являющееся частью этапа постановки задачи безопасности. Когда принято решение о том, что политика или защита от угроз будут реализованы в среде, то это должно всегда записываться как предположение.

В формулировках этих предположений должны быть отражены рассматриваемые политики и угрозы, от которых зависят цели для среды, которая должна соответствовать этим политикам и угрозам.

Одно предположение может зачастую использоваться для защиты от множества угроз, которые каким-то образом взаимосвязаны. Если был использован метод дерева угроз и были подробно описаны все угрозы, то для защиты среды общего иерархического узла вверх по дереву, предположение может быть сформулировано на уровне общего узла. Если все угрозы, проистекающие из негативных воздействий, учтены администраторами, это может быть выражено одним единственным предположением.

Пример - A.NO_POOR_ADMINISTRATION Администраторы имеют необходимую квалификацию, профессиональную подготовку, время и ресурсы, чтобы выполнять все предназначенные им административные функции, и все эти функции они выполняют правильно.

При формулировке предположений можно проверить, насколько они хорошо сформулированы и необходимы – если утверждение ошибочно, то атаки на ОО могут быть успешными.

Классификация предположений по типам будет полезна при идентификации и детальном изложении целей безопасности. Вначале предположения должны быть разделены на предположения о персонале, организационных и физических мерах безопасности. К следующей категории должны быть отнесены предположения относительно функциональных возможностей безопасности, предусмотренных в операционной ИТ-среде. И, наконец, предположения об учтенных угрозах. Все эти последние предположения должны быть сохранены отдельно, так как они совсем не влияют на цели безопасности.

Для некоторых задач безопасности возможно не потребуется приведение каких-либо предположений, что вполне приемлемо при оценке по ISO/IEC 15408. В этом случае раздел «Предположения» не заполняется.

9.6 Оформление постановки задачи безопасности

Последним этапом разработки ПЗБ является оформление ее спецификации. Это оформление включает две операции:

- подготовку полного списка всех угроз, политик и предположений;
- выполнение проверки согласованности и полноты для подтверждения того, что спецификация ПЗБ точно соответствует задаче безопасности или задачам, адресованным неформальным требованием безопасности.

Для ПЗБ должно быть разработано логическое обоснование, каждый элемент которого должен быть взаимосвязан с неформальными требованиями безопасности и должен демонстрировать полное покрытие без дублирования и избыточности. Если изменятся требования или впоследствии в ПЗБ будут обнаружены недостатки, то с помощью логического обоснования пересмотр ПЗБ значительно упростится, а риск появления ошибок уменьшится.

Также, если изменятся обстоятельства и потребуется пересмотр ПЗБ, информация об идентификации угроз, которые были учтены или проигнорированы, будет чрезвычайно полезной. Рекомендуется всегда включать соответствующие предположения о таких угрозах в отдельный раздел ПЗБ, обособленно от любых предположений об операционной среде. В результате оценщики, проверяющие правильность ПЗБ, будут знать, что эти угрозы должны быть проигнорированы при прослеживании целей безопасности.

Проверка согласованности и полноты включает проверку того, что все ограничения и требования были обоснованы во время анализа требований задачи безопасности, отражены в политиках или предположениях и что для всех определенных угроз были выбраны соответствующие контрмеры или они были учтены каким-либо другим способом. Также все политики, угрозы и предположения, перечисленные в ПЗБ, должны быть исследованы в аспектах оригинального неформального требования безопасности. Наличие согласованности и полноты может быть продемонстрировано с помощью таблиц перекрестных ссылок.

Описание реального требования должно быть точно сформулировано и должно содержать подробное пояснение. Если же в процессе проверки обнаружится реальное противоречие между предположениями и политиками, то должно быть принято решение о пересмотре неформального требования безопасности.

10 Цели безопасности

10.1 Введение

В этом разделе приведены рекомендации по идентификации и спецификации целей безопасности в ПЗ или ЗБ.

Цели безопасности представляют собой *краткое изложение предполагаемого решения задачи безопасности* (ISO/IEC 15408-3, 9.4.1 и 10.4.1). Решение задачи безопасности заключается в определении требований безопасности (раздел 12). Чтобы сформулировать цели безопасности наилучшим образом, необходимо представить их в виде краткого обзора и структуры необходимых функциональных возможностей безопасности, обеспечивая связь между детализированными ФТБ и абстрактной ПЗБ. Иначе говоря, после того, как в процессе ПЗБ будут сформулированы проблемы безопасности, нужно будет выдать указание о том, как они будут адресоваться ОО и его среде.

В ПЗ и ЗБ необходимо различать следующие типы целей безопасности (рисунок 2):

a) цели безопасности для ОО, которые будут удовлетворены техническими (ИТ) контрмерами, реализуемыми ОО;

b) цели безопасности для среды, которые должны достигаться с помощью любых технических мер, реализованных в ИТ-среде, или с помощью не-ИТ (например, организационных) мер.

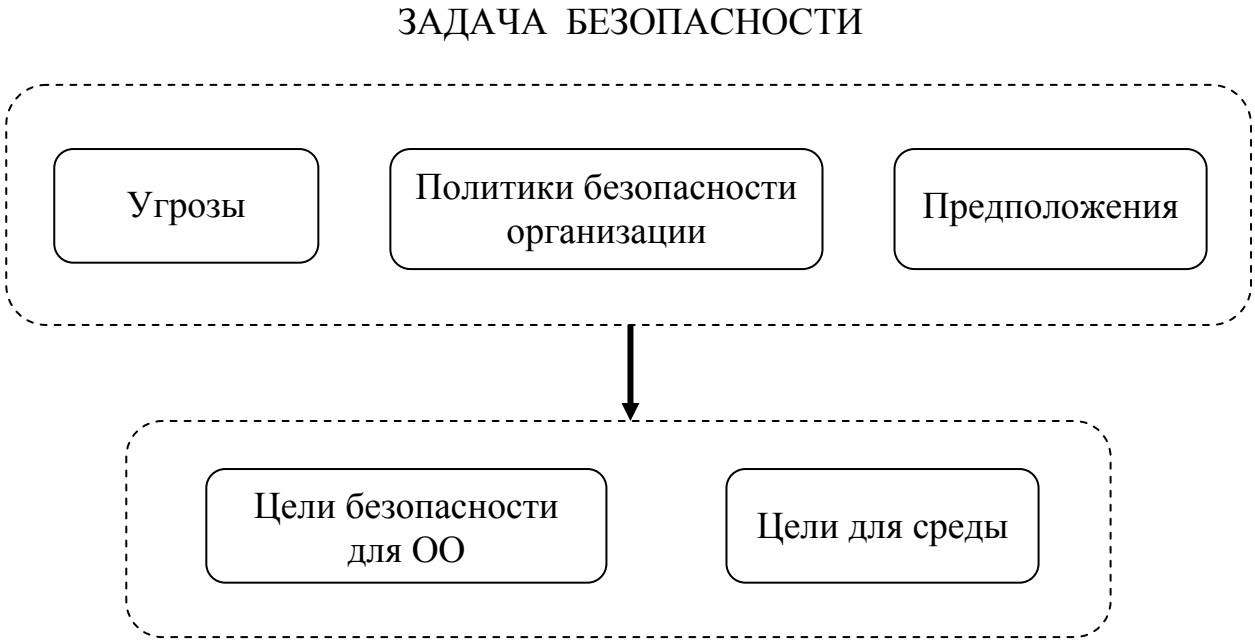

Рисунок 2 – Роль целей безопасности

Во всех ПЗ и ЗБ должны быть определены цели безопасности для операционной среды. При низком уровне доверия ПЗ и ЗБ (раздел 15) отсутствует необходимость в определении целей безопасности для ОО, цели безопасности для операционной среды рассматриваются как аксиоматические, то есть они не должны зависеть от ПЗБ.

Далее будет использоваться предположение, что оба типа целей необходимы, и они взаимосвязаны с ПЗБ.

Цели безопасности должны быть сформулированы как требования. Они должны состоять из кратких, четких утверждений, которые все вместе взятые определяют высокоуровневое решение задачи безопасности, определенной в соответствующей ПЗБ. Для формулировки целей рекомендуется использовать глагол «должен».

Для определения целей безопасности можно использовать любой подходящий метод. В помощь начинающему разработчику ПЗ и ЗБ ниже включено подробное описание простого метода, который надежен, проверен на практике и создан для работы в ряде организаций и сред. Этот метод базируется на серии шагов, выполняемых в следующей последовательности:

a) оформление списка всех угроз, политик и предположений, которые нужно отразить в целях;

b) определение целей для операционной не ИТ-среды;

c) определение целей для операционной ИТ-среды;

d) определение целей для ОО;

e) разработка логического обоснования целей во взаимосвязи с определенными ранее угрозами, политиками и предположениями.

Вследствие того, что в ПЗ или ЗБ цели безопасности играют центральную роль, то вопрос о том, какой уровень детализации целесообразно использовать при формулировке целей безопасности, является важным.

Формулировки целей безопасности должны быть *краткими*. На практике, необходимо соблюдать баланс между следующими двумя соображениями:

a) цели безопасности должны помогать потребителю в том, чтобы он смог понять, какие вопросы безопасности, идентифицированные в ПЗБ, должны быть адресованы ОО, не углубляясь в подробности реализации, кроме тех случаев, когда это было предписано при ПЗБ; в идеальном случае цели безопасности для ОО должны быть независимы от реализации. Таким образом внимание должно быть сосредоточено на том, *какое* решение предполагается достичь, а не *каким образом* оно достигнуто;

b) одновременно необходимо удостовериться в том, что цели безопасности определены, а не просто повторяют информацию, содержащуюся в угрозах и ПБОр ПЗБ, хотя и немного в другой форме.

Единственный способ проверки предположения о правильном выборе уровня детализации целей безопасности - создание логического обоснования для целей и требований безопасности. Если одно логическое обоснование будет простым, а другое в то время - большим, сложным и трудным для восприятия, то цели безопасности или слишком детализированы, или слишком абстрактны.

Однозначное определение набора целей безопасности для ОО гарантирует, что выбранные функциональные требования безопасности для удовлетворения этих целей не чрезмерны. При оценке ОО это поможет минимизировать финансовые и временные затраты.

10.2 Структурирование угроз, политик и предположений

Первой задачей при определении целей безопасности является структурирование полного списка всех существующих угроз, политик и предположений из ПЗБ.

Необходимо помнить, что некоторые угрозы могут быть значимы для ОО, но только после анализа рисков или среды можно решить, что их можно будет учесть или проигнорировать. Если разработчик руководствуется методологией, рекомендованной настоящим стандартом, то он уже включил эти угрозы в ПЗБ, а также записал предположения, в которых идентифицировал эти угрозы как не существующие. Такие угрозы не используются при формулировке целей безопасности, поэтому первым шагом будет являться идентификация этих угроз и соотнесенных с ними предположений, а затем исключение этих угроз и предположений из последующего рассмотрения. Необходимо удостовериться в том, что из ПЗБ очевидно, что эти угрозы исключены таким образом.

Затем остальные угрозы, политики и предположения должны быть разделены по типам, которые относятся к:

- операционной не-ИТ-среде;
- операционной ИТ-среде;
- функциональным возможностям ОО.

Политика, требующая физических элементов управления, может относиться только к не ИТ-среде; угроза вероятной атаки непосредственно на ОО соответствует функциональным возможностям ОО, а предположения могут относиться только к операционной среде. Если политика или требование распространяется на несколько областей, то политику или требование необходимо разбить на части, соответственно предназначенные для каждой области.

Пример - Угроза T.EAVESDROP может быть разделена на две угрозы:

- T.EAVESDROP (обмен информацией), относящаяся к операционной ИТ-среде;

- T.EAVESDROP (внутренняя), относящаяся к функциональным возможностям ОО.

При наличии сомнений необходимо разделить соответствующую политику или угрозу на множество областей. Ненужные записи впоследствии можно легко удалить. С другой стороны, недостающие записи могут стать причиной утраты целей, и это будет очень трудно обнаружить во время проверки правильности ПЗ/ЗБ.

10.3 Идентификация целей для не ИТ-среды

На первом этапе определения целей для не ИТ-среды необходимо взять все предположения, заданные для операционной не ИТ-среды, и перефразировать их на взаимно-однозначной основе в соответствующие цели. Впоследствии эти цели в ПЗ и ЗБ или во время оценки не анализируются, поэтому нецелесообразно определять их унифицированность, обобщение, перекрытие и т.п., при условии, что установленные цели были понятны и четко определены.

Далее необходимо разработать и добавить цели, необходимые для удовлетворения аспектов угроз и политик, которые заданы для не-ИТ операционной среды, вновь переформулировать угрозы или политики, имеющие отношение к целям, но без подробного изложения или объяснения.

Дополнительные цели безопасности для операционной не ИТ-среды могут включать:

a) создание и реализацию процедур для проверки того, что ОО будет использован безопасным способом (и в особенности в соответствии с предположениями о среде);

b) цели обучения и тренинга администраторов и пользователей надежным практическим методам безопасности.

При идентификации целей для не ИТ-среды на этом этапе могут возникнуть сложности, так как они поддерживают цели безопасности для ОО. Если цели для не ИТ-среды очевидны, то их сразу можно учесть. В противном случае впоследствии цели для не ИТ-среды необходимо еще раз рассмотреть и при необходимости дополнить.

Целям среды присваивают названия, начинающиеся с «OE». Это поможет явно отличать их от названий целей ОО, которые начинаются с «O». Цели среды должны быть четко сформулированы и указывать на то, что цель будет достигнута с помощью организационных или физических мер; не ИТ-среда должна быть определена в описании цели однозначно.

При получении целей среды из предположений следует не изменять формулировку предположения, то есть излагать их как факты.

Пример - OE.RESIDUAL Магнитный носитель предварительно размагничивается или измельчается до окончательного уничтожения.

Цели, полученные из угроз и политик, должны быть сформулированы как требования.

Пример - OE.AUD_REVIEW Для выявления нештатных ситуаций и не характерной активности обслуживающий персонал должен через равные промежутки времени просматривать журнал аудита.

Большинство целей операционной не-ИТ-среды будет получено из предположений. В целях, которые получены только в результате анализа угроз, можно указать, что предположения в ПЗБ отсутствуют. Необходимо проверить ПЗБ и при необходимости ее скорректировать.

Для удобства пользования отдельные цели могут распространяться на несколько взаимосвязанных предположений или на предположение и относящиеся к нему угрозы, или на политики и относящиеся к ним угрозы. Такое объединение оправдано только тогда, когда очевиден окончательный результат.

За выполнение целей операционной не ИТ-среды ответственны организации, использующие соответствующий продукт ИТ. Очень важно на данном этапе совместно с персоналом, ответственным за работу системы (или совместно с отделом реализации в случае COTS-продуктов) проверить, что эти цели отражают истинное положение дел и реально достижимы. В противном случае, лучше узнать о проблемах сейчас, а не потом, так как цели все еще можно изменить или оперировать угрозами и политиками другими способами.

10.4 Идентификация целей для ИТ-среды

Методы, используемые для идентификации и определения целей для операционной ИТ-среды, идентичны методам, используемым для идентификации целей не ИТ-среды, описанным в 10.3. Необходимо цели для ИТ-среды отличать от целей не ИТ-среды, поскольку цели ИТ-среды могут стать целями ОО, если впоследствии в процессе спецификации и разработки ОО будут изменены его границы.

Для идентификации целей для операционной ИТ-среды им присваиваются названия, начинающиеся с «OE». В описание ИТ-среды необходимо включать примечание с пояснением, что эти цели будут реализованы техническими средствами за пределами ОО.

10.5 Идентификация целей для объекта оценки

Цели для ОО, в отличие от целей для среды, используются в качестве обоснования для функциональных требований безопасности. Вследствие этого необходимо, чтобы цели для ОО были хорошо сформулированы, их назначение было понятно и чтобы была хорошая согласованность между детализированными требованиями безопасности и задачей безопасности.

Для идентификации целей для ОО не достаточно только изменить формулировку задачи безопасности или перечислить специфические требования безопасности.

Методология, предложенная в этом разделе для формулирования целей для ОО на базе основных областей функциональных возможностей безопасности, выбрана из тех соображений, что она хорошо согласуется с ранжированием функциональных компонентов по семействам и классам ISO/IEC 15408-2. Ширина и глубина достигаются посредством концепции основных и вспомогательных целей в пределах каждой области. Каждая основная цель устанавливает общую стратегию для конкретного аспекта безопасности с учетом передового опыта. Вспомогательные цели имеют дело со специфическими вопросами детализации задачи безопасности.

При использовании этой методологии первым шагом в определении целей ОО должно стать преобразование списка соответствующих угроз и политик, заданных функциональным возможностям ОО; все взаимосвязанные угрозы и политики необходимо сгруппировать. Этот список не должен содержать каких-либо предположений относительно функциональных возможностей ОО, так как предположения делаются только для операционной среды.

Выбор лучшей формы группирования угроз и политик для конкретного ПЗ или ЗБ будет зависеть от типа соответствующего ОО. Выполнение этого группирования в соответствии с внутренней структурой ISO/IEC 15408-2 впоследствии облегчит формирование ФТБ.

Все угрозы и политики предлагается разделить на семь следующих групп:

a) управление доступом (объекты, атрибуты, действия, правила доступа);

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

c) собственная защита ОО (обнаружение сбоя, надежное восстановление и т.п.);

d) защищенная связь (установление канала связи, характеристики соединения, правила);

e) аудит (регистрация событий, реагирование, управление инцидентами, анализы);

f) требования к архитектуре (обязательные характеристики и ограничения);

g) другие функции (те, которые нельзя легко отнести к вышеперечисленным группам, например, доверенный источник времени, генерация случайных чисел).

Между предложенными выше группами и структурой, рекомендуемой для идентификации и спецификации функциональных требований безопасности (см. раздел 12), установлена прямая зависимость.

Для целей безопасности разработчик может выбрать любую структуру и способ организации, но разделение на группы, рекомендован-

ное выше, упростит впоследствии перекрестный контроль и генерацию аргументов относительно их полноты и согласованности.

Следующий шаг – это просто запись определенных типов услуг безопасности, необходимых для каждой из выбранных областей, которые должны соответствовать требованиям задачи безопасности. Чтобы не анализировать и обобщать ПЗБ, необходимо повторно рассмотреть неформальное требование безопасности, из которого была выведена ПЗБ. Обычно при рассмотрении неформального требования безопасности становится очевидно, какие должны быть основные функции безопасности в каждой из основных областей. Некоторые области могут быть не указаны или однозначно идентифицированы как не важные; на этом этапе их можно будет проигнорировать.

Затем полученный список услуг необходимо сравнить со списком сгруппированных угроз и политик. Необходимо решить, какие угрозы и политики важны для каждой услуги. В заключение этого этапа любые оставшиеся угрозы и политики можно будет включить в список услуг под рубрикой «другие».

Далее угрозы и политики, соотнесенные с каждой услугой, надо разделить на общие и специфические требования. Общие требования должны относиться ко всем аспектам определения услуги, специфические требования - для специальных случаев.

И, наконец, надо перефразировать определение услуги в положительное утверждение, адресованное общему требованию. Это утверждение станет основной целью для этой услуги. Каждое специфическое требование необходимо перефразировать в отдельную вспомогательную цель для этой услуги.

Угрозам может быть противопоставлена цель, которая предотвратит угрозу, удалив или заблокировав один из ее необходимых компонентов. Например, лишение способности агента угрозы оказывать негативное воздействие путем перемещения, изменения или защиты актива таким образом, чтобы невозможно было оказать негативное воздействие, или путем устранения агента угрозы (например, добавляя в цель среды физические элементы управления доступом).

Угрозы также могут быть обработаны опосредованно. Примерами этого являются обеспечение подотчетности посредством проведения аудиторских проверок, повышение уровня подготовки пользователей, что будет способствовать исключению случайных ошибок, частое создание резервных копий активов, чтобы их легко можно было восстановить в случае удаления или повреждения.

Реализовать защиту от всех угроз невозможно. В некоторых случаях наилучшим способом действия является обнаружение соответствующего инцидента и генерирование сигнала тревоги или проведение аудита контрольного журнала. Такое типовое проектное решение должно быть выбрано и на этот раз. Если в качестве реакции на инцидент выбрано

обнаружение, то для того, чтобы появилась возможность реагирования на инциденты, будет необходима услуга аудита.

Возможно, что во время процесса спецификации возникнет необходимость в перераспределении угроз и политик. По мере того, как услуги будут становиться все более определенными, появится возможность более легко и точно установить конкретные угрозы или политики, соответствующие вспомогательной, а не основной цели, или наоборот, или возможно, что они даже будут лучше соответствовать другой услуге. Во время этого процесса зачастую происходит и определение целей для операционной среды, которые прежде были пропущены; например, если сигналы тревоги были выбраны в качестве реакции на конкретную угрозу, то для реагирования на сигнал тревоги потребуются администраторы. В некоторых случаях может быть даже принято проектное решение о переносе равноценной защиты для конкретных угроз или политик из целей для ОО в цели для операционной среды или наоборот. Эти изменения необходимо будет повторять несколько раз до тех пор, пока не будет получен четкий список целей, охватывающий все области.

Также при формулировке общих требований защиты (организацию связи следует сразу же отнести к основным целям) иногда в некоторых случаях, чтобы ограничить характер соответствующего технического решения, используются политики. Этот тип ограничения должен быть выражен как вспомогательная цель, связанная с общим требованием.

Некоторые угрозы желательно относить непосредственно к специфической вспомогательной цели, которая учитывает только эти угрозы и никакие другие. В этом случае в формулировке цели будет непосредственно отражен источник (агент) угрозы. Это впоследствии поможет упростить прослеживаемость в логическом обосновании целей, взаимосвязанных с ПЗБ, которая она станет более понятной для потребителей.

Вспомогательная цель может быть адресована нескольким угрозам и политикам. Например, во многих ПЗ и ЗБ цель повторного использования объекта является вспомогательной целью в области управления ресурсом. Имеет смысл выделить ее из других аспектов управления ресурсом, так как обычно имеется небольшое перекрытие в зависимости от адресованных угроз. При этом отсутствует необходимость адресовать эту цель далее другим типам ресурсов, которым может потребоваться проверка, несмотря на то, что другие типы ресурсов могут быть обработаны другими способами, например, некоторые угрозы для ОЗУ не относятся к магнитному носителю. Отличие будет устранено на этапе спецификации требований безопасности, когда в качестве механизмов для других ресурсов будут выбраны другие ФТБ.

Следующим значительным отличием при определении вспомогательных целей является тип необходимого управления. Элементы управления могут быть превентивными (останавливающими начавшийся

инцидент), обнаруживающими (выявляющими наличие инцидента) или корректирующими (устраняющими последствия инцидента). Имеет смысл иметь разные вспомогательные цели для каждого типа управления, если при обработке угроз или политик требуется больше действий, чем может выполнить каждый из этих типов. Такое часто случается, если в описании задачи безопасности требуется глубоко эшелонированная защита, или если основная цель для услуги только уменьшает или ослабляет угрозу, а не блокирует ее.

Цели безопасности, в которых определена необходимость управления доступом и управления потоком информации, относятся к категории превентивных целей. Если в задаче безопасности указывается, что ОО должен выполнять несколько управлений доступом или политик управления потоком информации, то необходимо четко определить цели безопасности для каждой политики. Это поможет упростить логическое обоснование требований безопасности.

В превентивной цели безопасности определяется необходимость идентификации и аутентификации пользователей ОО, в обнаруживающей цели безопасности - необходимость обеспечения в ОО такой функциональной возможности как неотказуемость с подтверждением подлинности источника, а в корректирующей цели безопасности содержится требование, что ОО должен реагировать на обнаруженные вторжения.

Примеры

1 Прежде, чем пользователю будет предоставлен доступ к средствам ОО, ОО должен проверить, что каждый пользователь был однозначно идентифицирован и что предъявленная им идентификационная информация была аутентифицирована.

2 ОО должен иметь в своем составе средства, с помощью которых получатель информации будет иметь возможность сгенерировать подтверждение, которое может быть использовано в качестве доказательства подлинности источника этой информации.

3 После обнаружения событий, которые свидетельствуют о неминуемом нарушении безопасности, ОО должен будет предпринять соответствующие меры для прекращения атаки и минимизации перебоев в предоставлении услуги другим пользователям ОО.

Далее список целей безопасности для операционной среды будет необходимо дополнить целями безопасности, связанными с действиями управления, которые обеспечивают эффективность услуг безопасности, предоставляемых ОО. В некоторых случаях необходимость действий управления очевидна и может быть незамедлительно сформулирована в форме (не-ИТ) цели безопасности. В других случаях, необходимость

действий управления может зависеть от детализированных требований безопасности, использованных при реализации целей безопасности для ОО. Например, цель безопасности «идентификация и аутентификация» может быть реализована путем использования пользователями паролей. В этом случае также должно подразумеваться требование для пользователей, что они должны гарантировать, что они не будут раскрывать свои пароли другим лицам, это требование должно быть правильно сформулировано как требование безопасности для не-ИТ-среды. Не вызовет огорчения или удивления, если на этом этапе будет пропущено подразумеваемое требование этого типа. Это станет очевидно при определении ФТБ, и тогда список целей безопасности может быть скорректирован.

Там, где это только возможно, при формулировании целей безопасности нужно неформально оценивать ожидаемую минимальную эффективность обеспечения безопасности таким образом, чтобы оставшаяся небольшая неопределенность относительно уровня эффективности могла быть обоснована в логическом обосновании ПЗ или ЗБ. Результат оценки может быть выражен:

a) в относительных величинах, например, по отношению к условиям среды или по отношению к предшествующей ситуации;

b) в абсолютных числовых значениях.

Несомненно, что определение абсолютных числовых значений для оценки эффективности является наиболее предпочтительным вариантом, но также и наиболее сложным.

Обычно не предполагается, что цели будут однозначно соответствовать угрозам или политикам. Чаще всего для основной цели необходимо, чтобы политика также могла противодействовать большинству угроз, соответствующих этой услуге. Также угрозы и политики могут воздействовать различно на разные типы активов, и для каждого типа актива будут нужны разные вспомогательные цели.

Существуют и другие методы, которые могут быть использованы для идентификации целей безопасности. Если цели не вытекают из формулировки соответствующей угрозы или политики в ПЗБ, то простым методом, который может хорошо работать для небольших ПЗБ, является разработка отдельной цели для каждой угрозы или политики; при этом формулировка цели повторяется и подставляется к специфическим активам, агентам угрозы и т.п.

Чтобы отличить цели ОО от целей среды, им обычно присваиваются названия, начинающие с «О»; тогда как названия целей среды начинаются с «ОЕ». Цели ОО должны быть четко сформулированы, чтобы указать на то, что меры, реализующие цель, будут частично выполнены ОО.

Формулировка целей ОО иногда начинается с выражения «ФБО должны» или «система должна». ФБО – это та часть ОО, которая реализует ФТБ. Такие разные формулировки используются, исходя из практических соображений, это позволяет уменьшить объем проверок, выполняемых во время оценки ОО. Следовательно, очень корректно использовать

выражение «ФБО»; для любой цели, та часть ОО, которая ее реализует, должна быть частью ФБО. Однако это является, в некоторой степени, неубедительным аргументом и приводит в некоторое замешательство, так как обычно эти цели называются «цели безопасности для ОО», а не «цели безопасности для ФБО». Чтобы добавить цели, реализуемые в среде, необходимо термину «система» дать определение, и тогда вместо выражения «ОО или его среда» гораздо лучше будет использовать этот термин.

10.6 Разработка логического обоснования целей безопасности

Заключительным шагом в определении целей безопасности должна стать разработка логического обоснования, прослеживающего соответствие целей угрозам, политикам и предположениям в ПЗБ для того, чтобы показать, что они все необходимы, и показывающего, что все аспекты всех угроз, политик и предположений в ПЗБ в целях учтены или далее не рассматриваются. Это логическое обоснование необходимо для всех оценочных уровней доверия, за исключением низких, оно проверяется при подтверждении правильности ПЗ/ЗБ.

Простым способом разработки логического обоснования является составление таблиц с взаимосвязями между элементами ПЗБ и целями и наоборот, и проверка на наличие каких-либо несогласованностей, брешей или перекрытий. Когда все угрозы, политики или предположения будут проработаны относительно многочисленных целей, тогда обычно появляется простой дискриминант, который может быть представлен к элементу ПЗБ, чтобы показать, какие части целей учтены – см. пример, приведенный в 10.2. При включении дискриминанта в таблицу преобразования станут гораздо более четкими и более легкими для понимания.

Делая допущение, что каждая цель безопасности может быть взаимосвязана, по крайней мере, с одной угрозой, политикой или предположением, с помощью таблицы сразу же можно будет увидеть, что каждая цель безопасности *необходима*. Конечно, это не будет являться гарантией того, что отсутствуют избыточные цели безопасности, поскольку и другие цели безопасности также могут быть взаимосвязаны с теми же угрозами, политиками и предположениями, и уже обеспечивают необходимое покрытие. Тем не менее, это может быть определено как часть устанавливаемого второго подтверждения выполнения требования к *достаточности*.

Достаточность должна быть доказана путем предоставления неформальных аргументов в дополнение к перекрестным ссылкам на информацию. Для каждой неучтенной угрозы нужно будет привести доказательства, почему соответствующие цели безопасности, взятые все вместе, обеспечат эффективные контрмеры для определенной угрозы. Необходимо отметить, что возможность атаки, основанной на этих угрозах, не обязательно должна быть исключена полностью; возможно

будет достаточно, чтобы обнаружить атаку или восстановиться после успешной атаки, или чтобы свести вероятность атаки к приемлемому уровню. Все, что требуется – это эффективные контрмеры в пределах контекста ПЗБ.

Подобным же образом будет необходимо для всех определенных ПБОр или предположений о среде с помощью неформальных аргументов привести доказательства о том, что соответствующие цели безопасности надлежащим образом обеспечивают полный охват ПБОр или поддерживают предположение.

Следует помнить, что предположения, включаемые в ПЗБ для идентификации угроз, которые могут быть учтены или проигнорированы, не используются при формировании целей безопасности и, следовательно, не должны фигурировать в логическом обосновании целей.

Если требования ПЗ или ЗБ соответствуют требованиям других ПЗ, то в логическом обосновании должно быть показано, что цели безопасности для ОО соответствуют формулировкам целей безопасности ссылочных ПЗ. Если цели безопасности ссылочных ПЗ и цели безопасности разработанного ПЗ сформулированы аналогичным способом, то можно будет показать посредством прямого преобразования, что цели разработанного ПЗ соответствуют и покрывают все цели ссылочных ПЗ. На самом деле, если ПЗ относится к тем ПЗ, которым требуется строгое соответствие, то его формулировки должны быть идентичными и, следовательно, оценщики проигнорируют все, что было указано в логическом обосновании.

Тем не менее, возможно, что структура или формулировки целей ссылочного ПЗ могут быть совсем иными, так что простого соответствия не будет. В этом случае нужно будет показать, что цели безопасности для ОО также удовлетворяют требованиям разделов постановки задачи безопасности ссылочных ПЗ. На основании этого можно доказать, что цели ПЗ обеспечивают тот же охват, как и цели ссылочных ПЗ и, следовательно, они сопоставимы.

Может случиться так, что будет невозможно сформулировать достаточно убедительные аргументы относительно соответствия требований ПЗ или ЗБ с требованиями других ПЗ, а постановки задачи безопасности ссылочных ПЗ явно не покрывают все угрозы в ПЗБ. В этом случае решение отсутствует - COTS-продукты, соответствующие ссылочному ПЗ, могут быть вполне пригодны для заявленных целей; тем не менее, их заявленное соответствие ПЗ не доказуемо. Возможно, что ознакомившись с разделом «Угрозы» в ЗБ на эти продукты и убедившись в том, что в этом разделе рассмотрены и учтены все основные угрозы, можно будет доказать, что эти продукты удовлетворяют требованиям заказчика.

11 Определение расширенных компонентов

Когда разработчик ПЗ или ЗБ при определении функциональных требований безопасности и требований доверия не сможет корректно определить эти требования, тогда ему придется усовершенствовать существующие компоненты из 2 или 3 части ISO/IEC 15408. В этих случаях разрешается использовать расширенные компоненты. Следует иметь в виду, что при возможности необходимо избегать использования расширенных компонентов. Использование расширенных компонентов затрудняет сравнение различных продуктов, основанных на функциональных требованиях безопасности и требованиях доверия, которым удовлетворяют продукты. Вместо этого вначале нужно попытаться использовать существующие в ISO/IEC 15408 компоненты, возможно с помощью уточнений. И только в тех случаях, когда это невозможно, использовать расширенные компоненты.

С помощью уточнений очень часто можно решить проблему, когда окажется, что компонент из ISO/IEC 15408 не соответствует тому специфическому требованию, которое необходимо для ПЗ или ЗБ. Например, когда для разных типов пользователей используются разные требования к их аутентификации. Эти требования можно будет легко сформулировать, используя уточнения для компонентов класса FIA, в которых сформулированы специфические требования, характеризующие тип пользователя, для которого применяется это специфическое требование, а затем использовать разнообразные реализации компонентов, чтобы полностью охватить все разные типы пользователей. Подобным же образом, используя уточнения, можно сформулировать разные требования для управления разными типами пользователей, субъектов, объектов или атрибутов безопасности.

В ISO/IEC 15408-1 предоставлены некоторые примеры уточнений и их использования для более точной формулировки требований, а также содержатся рекомендации по определению расширенных компонентов.

Перед определением расширенного компонента необходимо изучить уже изданные и прошедшие оценку ЗБ или ПЗ на предмет того, не был ли уже ранее определен этот расширенный компонент, тогда его можно будет использовать при определении необходимых функциональных требований безопасности и требований доверия.

Использование уже определенного расширенного компонента из прошедшего оценку ЗБ или ПЗ имеет преимущество в том, что сам компонент был уже проверен на наличие согласованности и соответствия требованиям ISO/IEC 15408 во время оценки этого ЗБ или ПЗ.

При определении расширенных требований необходимо соблюдать следующее правило: они должны быть определены тем же способом, что и существующие в ISO/IEC 15408 компоненты. Это также относится и к присвоению имени расширенному компоненту, способу его формулирования и уровню детализации. Таким образом, желательно при

описании расширенного компонента использовать ту же структуру, которая используется в ISO/IEC 15408. Относительно присвоения имени расширенному компоненту необходимо отметить, что если компонент соответствует какому-либо классу или даже какому-либо семейству, которые уже определены в ISO/IEC 15408, то при присвоении ему имени используют имя класса и (возможно) имя семейства, только добавляя метку, указывающую на то, что этот компонент является расширенным компонентом. При наличии возможности компонент должен быть определен универсальным способом, разрешающим выполнять операции «назначение» и/или «выбор». Это облегчит другим авторам ЗБ или ПЗ сбор и реализацию расширенных компонентов, которые соответствуют их требованиям.

Определение компонента расширенного ФТБ с использованием функциональных компонентов ISO/IEC 15408-2 в качестве модели для представления, включает:

a) определение расширенного ФТБ на том же уровне абстракции, что и функциональные компоненты ISO/IEC 15408-2;

b) использование стиля и фразеологии, соответствующих стилю и фразеологии функциональных компонентов ISO/IEC 15408-2;

c) использование топологии и номенклатуры, приближенной к топологии и номенклатуре компонентов ISO/IEC 15408-2.

Если станет известно, что новый ФТБ аналогичен другим ФТБ существующего класса или семейства, это поможет определить его степень новизны и также использовать формулировки и общие понятия, специфические для данного класса или семейства.

ISO/IEC 15408-2 содержит конкретные характеристики стиля представления функциональных компонентов:

a) большинство функциональных компонентов начинается с фразы «*ФБО должны*» или «*ФБО должны быть способны*», далее идет один из следующих глаголов: «*предоставлять возможность*», «*обнаруживать*», «*осуществлять*», «*обеспечивать*», «*ограничивать*», «*контролировать*», «*разрешать*», «*предотвращать*», «*защищать*», «*предоставлять*»;

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

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

d) каждое требование безопасности должно быть оцениваемо, т.е. должна существовать возможность дать заключение о том, удовлетворяет ли ОО этому требованию.

При формировании расширенного компонента для ФТБ необходимо определить:

a) будет ли разработчик ЗБ или ПЗ выполнять операции «выбор» и «назначение»для ФТБ;

b) предполагается ли наличие каких-либо зависимостей ФТБ от других ФТБ, которые должны быть включены в ПЗ или ЗБ;

c) будут ли описываться какие-либо события, подлежащие аудиту, и если будут, то какая информация о событиях подлежит регистрации;

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

Также необходимо отметить, что отсутствует необходимость определения для ФТБ операций «назначение» или «выбор», если ФТБ предназначен для использования только в ЗБ, то есть не предполагается повторно использовать этот компонент в других ПЗ, ЗБ или функциональных пакетах.

При присвоении имени расширенному ФТБ, не включенному в ISO/IEC 15408-2, необходимо использовать топологию, способ именования и стиль ISO/IEC 15408-2. Имена расширенных функциональных компонентов безопасности должны начинаться с буквы «F» (метки, указывающей на то, что это - функциональное требование), далее следуют соответствующий класс и обозначение семейства, сопровождаемое номером компонента. Если расширенный компонент разработан на основе существующих классов, то при присвоении ему имени используют имя класса, только добавляя метку, которая может быть вставлена в соответствующем месте. Если же расширенный компонент не связан с существующими классами, то при присвоении ему имени необходимо уточнить, что это расширенное требование безопасности - новое, например, обозначив класс компонента как «EX», или в конце имени компонента добавив «EX». Присвоение имени расширенному компоненту нужно пояснить в соответствующих примечаниях ПЗ или ЗБ. Необходимо учитывать то, что способ наименования расширенных компонентов не должен противоречить ISO/IEC 15408-2.

В приложении А приведен пример определения расширенного компонента и объяснение способа его определения. При оценке ЗБ или ПЗ, в которых определен расширенный компонент, этот пример позволит оценщику рассматривать расширенный компонент аналогично компонентам, определенным в ISO/IEC 15408-2.

Способом, описанным в приложении А для расширенного компонента функциональной безопасности, можно также определить расширенный компонент доверия. Это возможно тогда, когда специфические процессы обеспечения доверия общеприняты для типа продукта, описанного в ЗБ или ПЗ, и когда процессы обеспечения доверия не охвачены существующими компонентами ISO/IEC 15408-3. В дополнение к определению компонента доверия в стиле ISO/IEC 15408-3 для определения расширенного компонента доверия необходимо использовать методологию оценки безопасности ИТ, в которой описаны действия, выполняемые оценщиком при проверке изделия на соответствие расширенного компонента доверия. При определении этих действий должны быть использованы структура и уровень детализации,

определенные в ISO/IEC 18045 для компонентов доверия, в соответствии с ISO/IEC 15408-3.

Расширенные компоненты доверия должны содержать определение следующих элементов (более подробно см. ISO/IEC 15408-1, C.3):

a) действия разработчика;

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

c) действия оценщика.

Элементы, связанные с компонентом доверия, характеризуются следующим образом:

a) элементы действий разработчика определяют действия, которые должны выполняться разработчиком, как правило, при предоставлении свидетельства оценки;

b) элементы содержания и представления предназначены для определения требуемого содержания и «качественных» аспектов свидетельства оценки, которое должен предоставить разработчик;

c) элементы действий оценщика имеют две формы:

- первой формой обычно является следующее действие оценщика:

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

- любые дальнейшие элементы действий оценщика имеют форму утверждения о независимой работе и определяются оценщиком.

Следовательно, все требования к содержанию и представлению свидетельства должны быть не только ясно и понятно сформулированы, в них надо избегать (насколько это возможно) требований субъективной оценки со стороны оценщика. В значительной степени расширенное ТДБ должно определять четкие объективные критерии, на основе которых оценщик может сделать свое заключение. Необходимо привести в примечаниях по применению любые разъяснения относительно расширенного ТДБ, которые будут необходимы для обоснования требования при объективном обсуждении.

Чтобы проверить, что расширенные ТДБ сформулированы в том же стиле, как и компоненты ISO/IEC 15408-3, необходимы гарантии того, что каждое отдельное требование оформлено как отдельный элемент требований. При выборе формулировки расширенного ТДБ следует обращаться к разделу 3 ISO/IEC 15408-1, в котором приведены определения общеиспользуемых терминов.

После определения расширенного компонента доверия необходимо определить элементы действий оценщика, необходимые для подтверждения соответствия оцениваемого расширенного компонента доверия. Для этого используется структура элементов действий, определенная в ISO/IEC 18045. Элементы действий должны быть адресованы ко всем аспектам расширенного компонента доверия и четко объяснять оценщику, как выполнять оценку.

12 Требования безопасности

12.1 Введение

Этот раздел содержит руководство по определению требований безопасности ИТ в ПЗ или ЗБ, дополненное требованиями безопасности ОО.

В ПЗ или ЗБ определяют следующие типы требований безопасности ИТ (рисунок 3):

a) функциональные требования безопасности (ФТБ) ОО. Они содержат требования к функциям безопасности, обеспечивающим достижение целей безопасности для ОО;

b) требования доверия безопасности (ТДБ) ОО. Они определяют требуемый уровень доверия при реализации ФТБ.

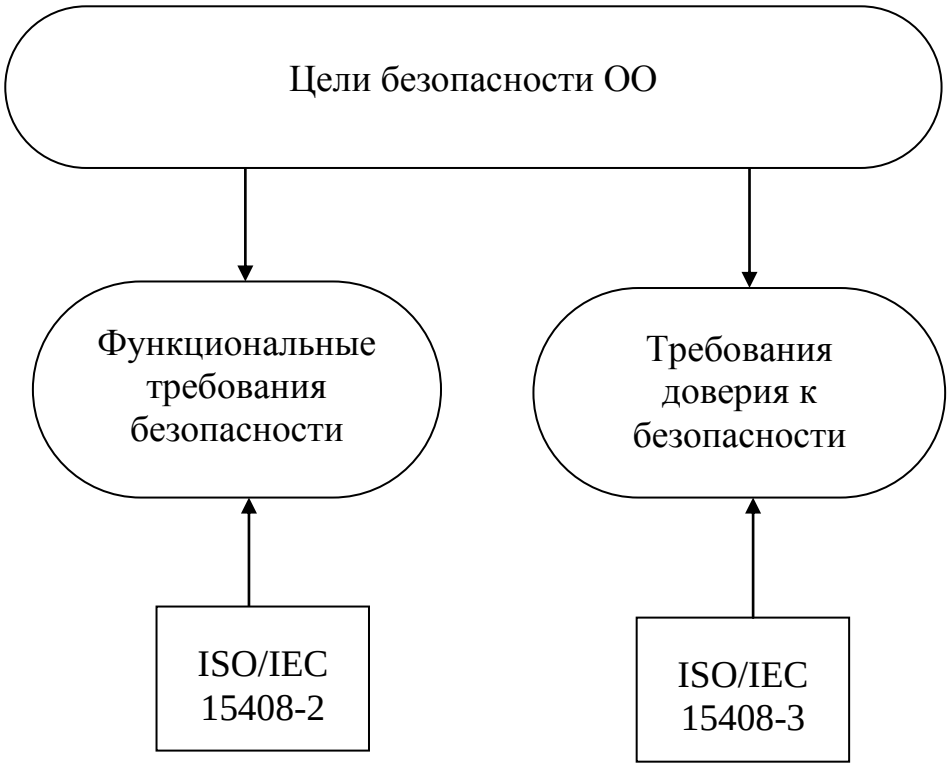

Рисунок 3 – Формирование требований безопасности ИТ

Как показано на рисунке 3, требования безопасности ИТ могут быть сформулированы, где это возможно, с использованием каталога функциональных компонентов, определенных в ISO/IEC 15408-2 и каталога компонентов доверия, определенных в ISO/IEC 15408-3,

соответственно. Использование вышеуказанных каталогов позволяет достичь определенного уровня стандартизации в области представления требований безопасности ИТ, тем самым значительно облегчается сравнение ПЗ и ЗБ между собой.

В ISO/IEC 15408-2 или ISO/IEC 15408-3 могут отсутствовать соответствующие функциональные компоненты или компоненты доверия. В этом случае требования безопасности ИТ могут быть сформулированы независимо от ISO/IEC 15408; однако такие требования безопасности ИТ должны быть однозначными, подлежать оценке и излагаться в соответствии с требованиями стандартов серии ISO/IEC 15408. При отсутствии соответствующих функциональных компонентов в ISO/IEC 15408-2 следует руководствоваться 12.3.7, а относительно компонентов доверия - 12.4.3.

Стандарты серии ISO/IEC 15408 допускают определенную степень гибкости формирования ФТБ и ТДБ на основе компонентов требований, предоставляя для них набор разрешенных *операций*, а именно: назначение, итерация, выбор и уточнение. В 12.3.2 представлены рекомендации по выполнению операций над функциональными компонентами, определенными в ISO/IEC 15408, а в 12.4.2 - аналогичные рекомендации для компонентов доверия.

Каждому компоненту требований безопасности в ISO/IEC 15408-2 и ISO/IEC 15408-3 присвоена в соответствии с определенной классификацией собственная уникальная метка:

a) в ISO/IEC 15408-2, например, метки компонента FAU_GEN.1.2 означают следующее:

- 'F'-метка указывает на то, что это *функциональное требование*;
- 'AU'-метка указывает на то, что ФТБ принадлежит к классу ФТБ «*аудит безопасности*»;
- 'GEN'-метка указывает на то, что ФТБ принадлежит к семейству «*генерация данных аудита безопасности*» класса FAU;
- '1'-метка указывает на то, что ФТБ принадлежит к компоненту «*генерация данных аудита*» этого семейства;
- '2'-метка указывает на то, что ФТБ является вторым элементом компонента FAU_GEN.1;

b) в ISO/IEC 15408-3 используется подобная классификация компонентов, но дополнительно определяется принадлежность каждого элемента к одному из трех наборов элементов доверия путем добавления в конце одной из нижеперечисленных букв:

- 'D' указывает, что компонент принадлежит к набору *элементов действий разработчика*, то есть к набору действий, выполняемых разработчиком;
- 'C' указывает, что компонент принадлежит к набору *элементов содержания и представления*, то есть к набору информации свидетельств, предназначенной для передачи;
- 'E' указывает, что компонент принадлежит к набору *элементов*

действий оценщика, то есть к набору действий, выполняемых оценщиком;

c) в ISO/IEC 15408-3, например, метки компонента ADV_TDS. 1.2C означают следующее:

- 'A'-метка указывает на то, что это компонент требования *доверия*;
- 'DV'-метка указывает на то, что компонент принадлежит к классу *разработка* ТДБ;
- 'TDS'-метка указывает на то, что компонент принадлежит к семейству *проект* ОО в пределах класса;
- '1'-метка указывает, что это компонент проекта *базового уровня* в пределах семейства;
- '2'-метка указывает, что это - второй *элемент* в наборе *элементов доверия*;
- 'C'-метка указывает, что это - элемент в наборе элементов содержания и представления в пределах компонента.

ФТБ и ТДБ выбирают на уровне компонентов: элементы, входящие в компонент, должны быть включены в ПЗ и ЗБ, если в ПЗ и ЗБ включается данный компонент. В процессе выбора требований безопасности ИТ необходимо учитывать следующие два типа зависимостей между компонентами требований безопасности ИТ:

a) компоненты одного семейства могут находиться в *иерархической* связи. Иерархия предполагает, что один компонент включает в себя все требования, определенные в другом компоненте этого семейства. Например, FAU_STG.4 иерархичен по отношению к FAU_STG.3, потому что все функциональные элементы, определенные в FAU_STG.3, также включены в FAU_STG.4. Однако FAU_STG.4 не иерархичен по отношению к FAU_STG.1, и поэтому может потребоваться включение обоих компонентов в разрабатываемые ПЗ и ЗБ;

b) компоненты могут *зависеть* от любого компонента другого семейства. Это означает, что компонент не самодостаточен и его функционирование зависит от функциональных возможностей другого компонента или взаимодействия с ним. Например, компонент FIA_UAU.1 (связанный с требованием аутентификации пользователей и называемый идентификатором) зависит от компонента FIA_UID.1 (связанный с требованием идентификации пользователей).

12.2 Парадигмы безопасности в ISO/IEC 15408

12.2.1 Объяснение парадигм безопасности и их использование для моделирования функций безопасности

Для лучшего понимания структуры классов, семейств и компонентов функциональных требований безопасности, определенных в ISO/IEC 15408-2, в настоящем стандарте рассматриваются более подробно парадигмы функциональных требований, сформулированные в разделе 5 ISO/IEC 15408-2.

Цель парадигм безопасности в ISO/IEC 15408 заключается в том,

чтобы обеспечить основу для моделирования функций безопасности ОО и затем доказать, что цели безопасности в данной модели могут быть выполнены. Указанные парадигмы могут быть использованы для создания абстрактной модели функций безопасности с помощью ФТБ, определенных в ISO/IEC 15408-2. Ниже даны рекомендации, как разработать и описать вышеуказанную модель, используя ФТБ.

12.2.2 Управление доступом к используемым ресурсам и объектам

12.2.2.1 Пояснение

В парадигме ISO/IEC 15408-2 функции безопасности управляют ресурсами защищаемого ОО и регулируют их использование. Ресурсы могут находиться как внутри ОО (например, ОЗУ, время центрального процессора, дисковое пространство, услуги и т.д.) или могут находиться вне ОО, но только в этом случае они будут доступны функциям ОО (по крайней мере, для некоторых логических объектов) для управления (например, сетевые услуги других систем). Межсетевой экран - типичный пример ОО, который управляет использованием ресурсов, не являющихся его частью.

Примеры ресурсов, которым может потребоваться управление для достижения целей безопасности:

- память (ОЗУ и дисковое пространство);
- время центрального процессора;
- периферийные устройства или каналы связи сети;
- функции.

Пользователи в ISO/IEC 15408-1 определяются как «любой логический объект (человек или ИТ) вне ОО, который взаимодействует (или может взаимодействовать) с ОО». И там же субъекты определяются как «действующий логический объект в ОО, который выполняет операции над объектами». Пользователи и субъекты - действующие логические объекты, которые запрашивают услуги от ОО и таким образом оперируют объектами и ресурсами.

Для достижения целей безопасности для ОО использование его ресурсов регулируется правилами, которые ОО должен выполнять. Эти правила могут регулировать использование ресурсов, а также регистрировать использование этих ресурсов.

Ниже представлен преднамеренно неполный список параметров, которые могут быть оценены как часть некоторых правил:

- тип и идентификатор логического объекта, который инициировал запрос;
- другие атрибуты логического объекта, который инициировал запрос;
- тип и идентификатор запрашиваемого ресурса;
- другие атрибуты запрашиваемого ресурса;
- тип запроса;
- время и дата;

- внутреннее состояние ОО.

Для выполнения правил, основанных на этих параметрах, ОО нужно их поддерживать и управлять этими параметрами:

- для внешних логических объектов (так называемых «пользователей») необходимо идентифицировать и возможно также аутентифицировать внешний логический объект - по крайней мере до необходимого предела, установленного правилами. Если правила основаны только на внешнем логическом объекте, принадлежащем специфическому набору или группе внешних логических объектов, для ОО достаточно идентифицировать (и возможно аутентифицировать) набор или группу;

- очень часто ОО поддерживает список внешних логических объектов (возможно с их атрибутами безопасности), которым разрешается использовать услуги, управляемые ФБО. В этом случае необходимо, чтобы в функциях было предусмотрено управление списком внешних логических объектов и их атрибутов безопасности (в том случае, если впоследствии в этот список предполагается внесение изменений и дополнений).

Та часть ОО, которая обеспечивает выполнение функций безопасности для удовлетворения целей безопасности, а также все другие части ОО, которые имеют возможность модифицировать или обходить функции безопасности называется «функциями безопасности ОО» (ФБО). В зависимости от архитектуры ОО ФБО может быть реализована как целый ОО или как его определенная часть. Если ФБО реализована только как часть ОО, важно, чтобы другие части ОО, не являющиеся ФБО, не могли управлять или обходить ФБО способом, который нарушает цели безопасности.

Оба внешних логических объекта, а также субъекты, которые запрашивают услуги, используя управление ресурсами, будут использовать интерфейсы ФБО (ИФБО).

В некоторых случаях субъекты действуют от имени внешних логических объектов. В этих случаях внешний логический объект (или пользователь) будет «связан» с субъектом. Для отображения этого связывания атрибуты безопасности субъекта, являющиеся частью этого процесса связывания, будут часто изменяться. Примером является ОО, чьи атрибуты безопасности внешнего логического объекта наследует субъект, но могут существовать более сложные правила, полученные как часть процесса связывания, и определяющие атрибуты безопасности субъекта.

Ресурсы могут быть сгруппированы относительно «объектов» и для ОО разрабатываются специальные правила по использованию этих объектов, которые отличаются от правил по использованию ресурсов, которые создает объект. Типичным примером является ОО, который выполняет правило максимальных квот дискового пространства (ресурсы) и правила управления доступом к файлам (объекты), созданных из ресурсов дискового пространства. Этот пример показывает, что отдельный ресурс может подвергаться воздействию разных правил, задаваемых ОО, то есть один набор правил регулирует использование ресурса, а другие

наборы правил предназначены для объектов, созданных из ресурсов.

Обычно для разных типов объектов используются разные правила, регулирующие доступ и использование объектов. Во избежание путаницы ISO/IEC 15408 позволяет группировать набор правил для разных объектов, субъектов и операций в разные «политики функции безопасности» (ПФБ) и ссылаться на ПФБ в индивидуальных ФТБ, чтобы обозначить ту политику функции безопасности, которой соответствуют ФТБ. Для ПФБ непременно должна быть определена область применения, то есть определен набор субъектов, пользователей, объектов, ресурсов и операций, к которым применяется политика. Это определение должно быть однозначным, это будет являться гарантией того, что область применения ПФБ хорошо определена. Тогда правила, предписанные операциями для субъектов или пользователей, при использовании объектов или ресурсов, будут определены как часть ПФБ. Как уже было сказано выше, правила обычно основываются на специфических атрибутах субъектов, пользователей, объектов или ресурсов. Атрибуты, влияющие на правила ПФБ, называются «атрибутами безопасности». Требования по управлению атрибутами безопасности, которые играют некоторую роль в ПФБ, являются также частью ПФБ, в которой определяется, каким образом в зависимости от ПФБ инициализируются атрибуты безопасности логического объекта при его создании, импорте или регистрации (для пользователей). Короче говоря, в ПФБ описываются правила доступа и использования определенного набора объектов или ресурсов определенным набором действующих логических объектов (пользователей или субъектов), использующих определенный набор операций вместе с функциями управления атрибутами безопасности, используемых в этих правилах.

Типичным примером является политика управления доступом для объектов файловой системы в операционной системе. Действующие логические объекты - это процессы, некоторые из которых действуют от имени пользователя, и поэтому они должны иметь обязательно атрибуты безопасности, полученные из связанных атрибутов безопасности пользователя. Операции - это те же системные вызовы, которые управляют объектами файловой системы, например, открывают файл для чтения, записи или коррекции, рассматривают или изменяют атрибуты файла, создают или удаляют файл. Кроме того, существуют операции, которые управляют атрибутами безопасности процессов или объектов файловой системы. Типичными примерами атрибутов безопасности, которые играют некоторую роль в ПФБ, могут быть следующие:

- атрибуты безопасности объекта: списки управления доступом, тип файла;
- атрибуты безопасности пользователя: идентификаторы пользователя, роли пользователя;
- атрибуты безопасности процесса: идентификатор процесса, уровень доверия процесса.

Другие ПФБ могут регламентировать операции внешних логических объектов, выполняемые непосредственно без промежуточного субъекта. Например, система межсетевого экрана, которая регламентирует каким образом сетевые услуги и функции также могут использоваться внешней системой. Кроме этого к ним относятся действующие логические объекты (внешние системы, инициирующие запрос), объекты (внешние запрашиваемые системы) и операции (сетевые услуги). Правила ПФБ могут базироваться на идентификаторе внешних систем, участвующих в операции, типе выполняемой операции (например, использование порта), контексте операции (например, если соединение с конкретным портом было предварительно установлено) и/или содержании сетевых пакетов.

Нет ничего необычного в том, что может быть определено несколько ПФБ для одного и того же набора пользователей, субъектов, объектов и операций. Например, первая ПФБ - политика дискреционного управления доступом, а дополнительная ПФБ - политика полномочного управления доступом. Несмотря на то, что набор пользователей, субъектов, объектов и операций, к которым обращается ПФБ, один и тот же, правила ПФБ и набор атрибутов безопасности, используемых в этих правилах, различны, и это будет являться обоснованием для определения двух ПФБ.

12.2.2.2 Применение

Основой для модели ОО относительно ресурсов и объектов, а также операций, разрешенных с этими ресурсами и объектами ОО (или посредством ОО) активным логическим объектам (любой внутренней или внешней части ОО) является политика управления доступом. Значит первым шагом создания модели ОО, используемой для определения ФТБ по управлению доступом является идентификация ресурсов, объектов, операций, выполняемых ОО, а также субъектов и пользователей, которые инициируют эти операции. В создаваемую модель должны быть включены только те типы ресурсов, объектов, операций, субъектов и пользователей, которые могут быть непосредственно получены из целей безопасности и общих функциональных возможностей ОО, описанных в начале ПЗ или ЗБ. При разработке ЗБ для существующего продукта или системы логические объекты, определенные в модели, должны иметь место и в ОО. Кроме того, чтобы гарантировать согласованность и полноту определяемых функциональных требований безопасности, может возникнуть необходимость дополнений начальных наборов ФТБ.

Если в модели будут определены логические объекты, которые отсутствуют в ОО, то во время оценки возникнут проблемы, так как ISO/IEC 15408 предполагает, что ФТБ и логические объекты, указанные в ФТБ, являются абстракциями логических объектов, которые имеются в ОО, и, следовательно, они могут быть детализировано отображены как логические объекты при проектировании и реализации ОО.

Следующим шагом создания модели ОО должно стать определение правил регулирования доступа, использования ресурсов и объектов посредством операций субъектов и/или пользователей, определенных в

модели, которая удовлетворяет целям безопасности. Кроме того, при определении ЗБ для существующего ОО, правила должны, конечно, стремиться стать абстракцией реального поведения ОО для логических объектов, определенных в модели, так что правила, реализованные в ОО, являются строгой детализацией правил в модели.

Частью определения правил является идентификация используемых в них параметров. Необходимо определить «атрибуты безопасности» ресурсов, пользователей, субъектов и объектов. Эти атрибуты безопасности должны быть внесены в соответствующий список, поскольку эти правила могут понадобиться для инициализации и управления.

При определении этих правил необходимо отметить, что правила для разных наборов ресурсов, объектов, пользователей, субъектов или операций будут разными. Для упрощения описания модели необходимо сгруппировать наборы («типы») ресурсов, объектов, пользователей, субъектов, и операций с идентичным (или почти идентичными) правилами в политики функции безопасности. Каждой политике функции безопасности присваивается имя, которое позволит ее идентифицировать.

Далее необходимо определить правила создания и удаления субъектов и объектов. Эти правила могут быть разными для разных типов субъектов и объектов. Правила также должны определять, как инициализируются атрибуты безопасности субъектов и объектов.

А затем в тех случаях, когда эти атрибуты не являются статическими, определяют правила управления атрибутами безопасности субъектов и объектов. Необходимо отметить, что эти правила могут содержать операции, инициированные внешними логическими объектами через ИФБО, а также правила, которые описывают, что модификация атрибутов безопасности является частью операций, выполняемых ФБО.

Потом необходимо будет определить правила регистрации («создание») и дерегистрации («удаление») пользователей, когда пользователи должны быть зарегистрированы в ОО. Правила регистрации пользователей также включают правила инициализации их атрибутов безопасности. Существуют случаи, когда пользователи не должны регистрироваться. Они могут запросить услуги, идентифицировать себя и, возможно, аутентифицировать, предоставляя свои верительные данные. Эти верительные данные могут также включать атрибуты безопасности пользователя. В этих случаях правила должны определять, каким образом определяются принятые верительные данные и каким образом они проверяются.

Далее будет необходимо определить правила идентификации и, при необходимости, правила аутентификации пользователей. Эти правила определяют верительные данные пользователя, которые он должен предоставить (тип, возможные ограничения, например, минимальная и максимальная длина, минимальный и максимальный срок действия и т.д.), а также реакцию ФБО при предоставлении неверных верительных данных.

Затем необходимо определить правила управления атрибутами безопасности пользователей, которые необходимы для определения атрибутов безопасности субъектов и объектов.

Если ОО поддерживает функцию связывания пользователь-субъект, то будет необходимо определить правила включения в это связывание. Эти правила могут содержать:

- необходимые условия, которые должны быть выполнены, чтобы установить связывание;
- назначение субъекту атрибутов безопасности после установления связывания.

После того, как это все будет выполнено, необходимо убедиться в том, не потребуются ли еще какие-либо дополнительные правила управления. Примером такого дополнительного правила является правило, позволяющее создавать новый атрибут безопасности (например, новую роль пользователя) возможно вместе с правилами, определяющими, как управлять этим атрибутом безопасности (например, при определении набора атрибутов безопасности пользователя ему назначается часть роли).

12.2.3 Управление пользователями

12.2.3.1 Пояснение

Согласно парадигме ISO/IEC 15408 пользователь - это логический объект, внешний относительно ОО, который запрашивает услуги от ОО, используя его интерфейсы. Прежде, чем использовать услуги ОО, пользователи должны зарегистрироваться или ОО может позволить пользователям запрашивать услуги без предварительной регистрации. Во многих случаях решение ОО о предоставлении необходимой услуги зависит от некоторых атрибутов безопасности пользователя. Атрибуты безопасности пользователя или могут быть представлены пользователем вместе с запросом, или могут быть получены из данных, которые ОО хранит о пользователе или группе, к которой принадлежит пользователь.

В первом случае ОО необходима гарантия в том, что представленным пользователем атрибутам безопасности можно доверять. Это означает, что ОО выполняет правила оценки атрибутов безопасности и удостоверяется в том, что пользователь (который может быть неизвестен) использует атрибуты безопасности на законном основании.

Во втором случае ОО должен знать идентификатор пользователя или идентификатор группы, к которой он принадлежит. Также в этом случае ОО должен выполнять правила, определяющие каким образом осуществляется проверка того, что предъявленный идентификатор пользователя или его членство в группе являются верными. Во время этого процесса, называемого аутентификацией, пользователю необходимо предоставить верительные данные, которые используются ОО, чтобы удостовериться в правильности предъявленного идентификатора или членства в группе. Должны быть определены правила выполнения процесса аутентификации и как должно происходить управление параметром процесса аутентификации.

Когда требуется, чтобы пользователи были зарегистрированы, тогда необходимо определить правила, каким образом пользователи могут зарегистрироваться и как управлять их атрибутами безопасности.

В некоторых случаях ОО использует один из своих субъектов, чтобы действовать от имени пользователя. В этом случае субъект «связан с пользователем» ФБО, то есть для ФБО должны быть разработаны правила, определяющие, каким образом можно будет получить атрибуты безопасности субъектов, когда субъект связан с пользователем. Очень часто субъект наследует часть атрибутов безопасности пользователя, позволяющую использовать атрибут безопасности пользователя, основанный на политике управления доступом, даже тогда, когда фактический доступ выполняется субъектом.

12.2.3.2 Применение

Чтобы определить функции управления пользователями, необходимо выполнить следующее:

- идентифицировать и определить типы пользователей, которые могут получить доступ к ОО (вместе с набором атрибутов безопасности, который имеет каждый тип пользователя);
- идентифицировать каждый тип пользователя, если он должен быть зарегистрирован прежде использования функций ОО;
- для каждого типа пользователя, который должен быть зарегистрирован, определить правила регистрации пользователя (как это сделать) и атрибуты безопасности пользователя, которые должны быть ему присвоены после регистрации;
- идентифицировать все типы пользователей, если идентификация пользователя необходима, а затем определить правила выполнения идентификации пользователя;
- идентифицировать все типы пользователей, если аутентификация пользователя необходима, а затем определить правила выполнения аутентификации пользователя. Определить условия, при которых пользователь должен быть аутентифицирован;
- определить правила управления процессом аутентификации (включая управление верительными данными, используемыми при аутентификации);
- определить для каждого типа пользователей правила управления атрибутами безопасности пользователя;
- определить правила связывания пользователь-субъект, когда это связывание возможно или необходимо. В первую очередь определить правила присвоения атрибутов безопасности субъектов во время процесса связывания.

12.2.4 Собственная защита объекта оценки

12.2.4.1 Пояснение

Собственная защита функций безопасности требуется всякий раз, когда выполняется одно из следующих условий:

- наличие возможности для агента угроз атаковать функции безопасности в пределах предполагаемой среды ОО таким образом, чтобы цель безопасности не могла быть достигнута;
- наличие вероятности того, что цель безопасности не может быть достигнута из-за сбоя элемента среды ОО;
- наличие вероятности того, что цель безопасности не может быть достигнута из-за сбоя элемента ФБО.

В этих случаях должны быть определены, как часть ФБО, функции собственной защиты, которые будут обнаруживать эти условия и реагировать на них тем способом, которым даже в этих условиях цели безопасности достигаются.

При определении собственной защиты ОО в функциональной модели необходимы:

- идентификация возможных сценариев атак и сбоев, которые могут нарушить цель безопасности;
- идентификация функции, которая способна предотвратить атаку или сбой. Примером такой функции является усиленная физическая защита ОО, которая сможет предотвратить специфические физические атаки;
- идентификация функций, которые обнаруживают атаку или сбой и реагируют должным образом в тех случаях, когда их невозможно предотвратить (в большинстве случаев).

Для обнаружения атак извне или сбоев системы в среде ОО могут потребоваться мониторинг использования ИФБО и проверка режимов работы после атаки, мониторинг режимов каналов связи после атаки или мониторинг датчиков ОО, предназначенных для обнаружения атак.

12.2.4.2 Применение

При определении функций собственной защиты ОО необходимо при постановке задачи безопасности идентифицировать те функции, которые необходимы для достижения целей безопасности. В этом случае, если необходимо предотвращать внешние атаки, нужно будет, например, несколько усилить физическую защиту или, если необходимо обнаруживать атаки или сбои, нужно будет на них соответствующим образом реагировать.

Начать необходимо с составления списка атак или сбоев, с которыми может быть и не приходилось ранее сталкиваться, но которые могут произойти в предполагаемой среде ОО и возможно нарушить цели безопасности. В начале составления каждого списка нужно определить, каким образом предполагается обрабатывать атаку или сбой, то есть будут ли им противодействовать функциональные возможности безопасности, реализованные в ОО, или будет необходимо для ОО определить

функциональные возможности безопасности, которые обнаружат атаку или сбой и среагируют должным образом.

При наличии функции предотвращения атаки ее описание должно содержать некоторое пояснение о том, каким типам атак она может противостоять.

В отношении атак и сбоев должны быть определены критерии и правила обнаружения (на абстрактном уровне) и реагирования (такие же абстрактные правила, формулирующие предположительные действия ОО в таких случаях).

Обнаружение сбоев ФБО может выполняться посредством мониторинга внутренних переменных состояния, внутренних функций тестирования или при наличии функций или избыточных данных и проверки на несогласованность.

Реагирование может закончиться:

- корректирующим действием, которое устранит последствия атаки или сбоя. Примером являются функции, которые могут обнаружить и автоматически скорректировать отказы, и которые основаны на дублировании данных или функциональных возможностях;

- корректирующим действием, которое частично устранит последствия атаки или сбоя, но закончится некоторым уменьшением функциональных возможностей ОО (которые должны соответствовать целям безопасности). Примером являются функции восстановления после отказа или атаки, но восстановление может занять некоторое время и оно может быть неполным. В этих случаях должна быть гарантия того, что ни задержка, ни потеря функциональных возможностей или данных в результате неполного восстановления, не нарушат какую-либо цель безопасности;

- подготовкой ОО для ручного корректирующего воздействия (например, остановка поврежденных при атаке или сбое некоторых частей ОО или всего ОО, восстановление отключенных частей или всего ОО и перезапуск его в безопасном режиме);

- остановкой поврежденных частей ОО или всего ОО при отсутствии в ФБО метода безопасного перезапуска. Примером является ОО, который уничтожает важные функции или данные при обнаружении атаки или сбоя и при этом гарантирует, что ОО не нарушает свои цели безопасности.

Список вышеперечисленных корректирующих воздействий составлен с учетом возрастания воздействия на все функциональные возможности ОО.

12.2.5 Обеспечение безопасной связи

12.2.5.1 Пояснение

Функции, которые защищают данные, передаваемые к внешнему логическому объекту или передаваемые между различными частями распределенного ОО при использовании ненадежного или не доверенного канала связи, являются еще одним примером функций, которым требуется дополнительное моделирование. Для моделирования связи должны быть

определены характеристики безопасности канала связи. Эти характеристики могут включать следующее:

- аутентификацию участников связи;
- защиту целостности данных, передаваемых по каналу (который может включить защиту от повторного использования сообщений и/или от изменения последовательности сообщений);
- защиту конфиденциальности данных, передаваемых по каналу;
- защиту от потери данных;
- обеспечение неотказуемости при передаче и/или получении сообщений.

При моделировании канала связи должны быть определены его пользователи, а также характеристики безопасности канала. Это относится к каналам связи, работающим как в режиме on-line, так и в режиме off-line.

12.2.5.2 Применение

При идентификации функций, для которых необходима безопасная связь, необходимо выполнить следующие шаги:

- идентифицировать каналы связи;
- определить для каждого канала связи необходимые характеристики безопасности. Примерами таких характеристик безопасности являются:

a) аутентификация пользователей связи;

b) защита целостности (возможно включение защиты от повторного использования, защиты от изменения последовательности сообщения и т.д.);

c) защита конфиденциальности (возможно включение защиты от анализа потока трафика);

d) обеспечение неотказуемости (при передаче, получении или в обоих случаях);

e) обеспечение сохранности передаваемых данных.

Для каждого канала связи должны быть определены характеристики безопасности. В ЗБ также должны быть определены механизмы, используемые при реализации этих характеристик безопасности (главным образом криптографические механизмы). В ПЗ эти механизмы должны быть определены только до верхнего уровня требуемой детализации. Необходимо отметить, что этот уровень детализации может быть весьма высок в том случае, когда для любого ОО соответствующего ПЗ также предполагается, что он будет удовлетворять требованиям интероперабельности. В этих случаях даже в ПЗ может быть определен механизм до нижнего уровня специфического протокола вместе с опциями протокола (например, криптографических алгоритмов), которые должны гарантировать интероперабельность.

При идентификации списка каналов связи в него необходимо включить не только физические каналы связи, но также и виртуальные каналы (например, на уровне прикладного протокола), которым нужна специфическая защита. Виртуальные каналы связи вполне могут быть

расположены на разных уровнях протокола, в этих случаях на разных уровнях обеспечиваются разные типы защиты. Например, IPsec на IP-уровне может обеспечить аутентификацию равноправных логических объектов (в этом случае системы), а также целостность и защиту конфиденциальности. Прикладной протокол (который может представить другой виртуальный канал связи) поверх IPsec затем может обеспечить дополнительную аутентификацию (например, человека-пользователя или приложения), а также функции неотказуемости. В этом случае IPsec и прикладной протокол должны быть внесены в список как разные каналы связи со своими собственными специфическими характеристиками безопасности.

Следует отметить, что при организации защищенных каналов связи большинство функций обеспечивает защиту целостности и защиту от потери данных при обнаружении таких условий. Подобно функциям обнаружения, описанным в 12.2.4 «Собственная защита объекта оценки», должны быть определены средства реагирования ОО при обнаружении этих условий. Также должны быть определены средства реагирования на неудавшиеся попытки аутентификации и необоснованную неотказуемость.

Следует отметить, что экспорт ФБО или данных пользователя за пределы действия ОО и импорт ФБО или данные пользователя в ОО, когда неизвестен равноправный пользователь связи, могут быть рассмотрены как специальный случай связи. В случае экспорта и импорта должны быть рассмотрены следующие характеристики:

- защита целостности (с возможностью включения защиты от повторного использования и т.п. оригинальной защиты);
- защита конфиденциальности;
- обеспечение неотказуемости (для экспорта и/или импорта).

12.2.6 Аудит безопасности

12.2.6.1 Пояснение

Мониторинг определения критических событий безопасности и ведение учета этих событий для последующего анализа или для оценки, автоматическое реагирование на такие события – это другая функция безопасности, которая может быть необходима ОО для удовлетворения его целей безопасности. Критические события безопасности могут быть непосредственно связаны с запросами на использование услуг ОО действующего логического объекта, а также с обнаружением критического состояния или события безопасности, которое не может быть непосредственно связано с таким запросом.

К критическим событиям безопасности относятся:

- успешные и/или отклоненные попытки использования предоставляемых ФБО услуг;
- неожиданное возникновение неработоспособного состояния;
- непредвиденный или неправильный режим работы удаленного доверенного продукта ИТ;
- отказ, обнаруженный функцией самотестирования;

- превышение заданных критических порогов безопасности;
- изменения критических данных ФБО;
- сбор событий, когда каждое отдельное событие не считается достаточно критическим для аудита.

12.2.6.2 Применение

Для разработки модели аудита безопасности требуются:

- список событий, которые должны быть подвергнуты аудиту;
- определение правил, регулирующих проведение аудита события (например, только тогда, когда будет отклонен запрос);
- определение данных, которые должны быть собраны для каждого события;
- определение правил обработки и анализа собранных данных для аудита.

Рекомендуется проводить анализ каждой отдельной функциональной возможности безопасности, если возникают связанные с ней события, которые должны быть подвергнуты аудиту. Кроме того, должен быть выполнен анализ модели функций безопасности для критических внутренних состояний, при возникновении которых должны создаваться записи аудита.

12.2.7 Требования к архитектуре

12.2.7.1 Пояснение

В дополнение к вышеупомянутым требованиям может возникнуть необходимость в определении требований к архитектуре ОО. Такие требования могут быть необходимы, чтобы гарантировать возможность выполнения анализа архитектуры, а также, чтобы помочь потребителям понять архитектуру ОО. Архитектура ОО обычно обуславливается специфическими характеристиками, которые непременно должен обеспечивать ОО. Типичными примерами таких характеристик являются:

- отказоустойчивость;
- управление информационными потоками;
- приватность;
- режим реального времени.

Требования к архитектуре часто усиливаются требованиями из предыдущих подразделов. Например, управление информационными потоками и приватность обычно сопровождаются специфическими правилами, регулирующими доступ к объектам, а отказоустойчивость обычно сопровождается требованиями аудита безопасности, используемыми для обнаружения отказов. Эти правила управления доступом и особенно правила аудита безопасности необходимы, но их обычно не достаточно для реализации требования относительно характеристик ОО.

Выполнить идентификацию и спецификацию требований к архитектуре гораздо труднее, чем других функциональных требований безопасности. Однако они могут содержать требования, полностью удовлетворяющие некоторым целям безопасности, и поэтому они должны

быть определены в ПЗ или ЗБ как часть функциональных требований безопасности.

12.2.7.2 Применение

Для идентификации и моделирования требований к архитектуре выполняются следующие шаги:

- идентификация целей безопасности, которые не были адресованы или были частично адресованы требованиям, определенным в предыдущих шагах;
- идентификация архитектурной поддержки, необходимой для удовлетворения целей;
- определение правил, которые обеспечивают эту архитектурную поддержку.

Настоящий стандарт может оказать некоторую помощь в выборе требований к архитектуре. В случае ЗБ эти требования, вероятнее всего, будут предопределены архитектурой ОО, для которого разрабатывается это ЗБ. Например, если известно, что ОО будет распределенным, то для достижения определенных целей безопасности будет необходимо определить требования по поддержанию согласованности данных между частями распределенного ОО или требования по защите данных от несанкционированного доступа при передаче их между частями распределенного ОО. Также можно утверждать, что поддерживающие внутренние функции ФБО в пределах ОО должны дублироваться до тех пор, пока ОО удовлетворяет своим целям безопасности в своем ИФБО, определяющим обязательные внутренние функции, которые поддерживают цели безопасности, способствуя их пониманию и помогая анализировать ОО во время оценки.

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

12.3.1 Выбор функциональных требований безопасности

После определения целей безопасности для ОО, являющегося частью ПЗБ, будет необходимо тщательно обдумать, как эти цели безопасности должны быть выполнены. Это делается посредством выбора соответствующего набора ФТБ, которые выполнены на уровне *компонентов*. При этом процесс выбора ФТБ значительно упрощается, если доступны заранее определенные функциональные пакеты, соответствующие целям безопасности для ОО.

Выбор ФТБ основан на модели общих функциональных возможностей ОО. Эта функциональная модель определяет ресурсы, пользователей, субъекты, объекты и операции. ФТБ определяют функциональные возможности безопасности так, что цели безопасности выполняются в пределах функциональной модели ОО. Как и любая другая модель, эта модель - абстракция реальных функциональных возможностей ОО, но уровень абстракции должен быть достаточен для того, чтобы

понять принцип функций ОО. При определении ФТБ можно пренебречь ресурсами, пользователями, субъектами, объектами и операциями, которыми не нужно управлять для достижения целей безопасности. Например, если единственная цель безопасности для ОО заключается в управлении доступом к данным, то при определении ФТБ ресурс «время центрального процессора» можно не учитывать.

В процессе выбора ФТБ для ПЗ или ЗБ существует несколько этапов. В рассматриваемом процессе выбора различают два типа ФТБ:

a) *основные* ФТБ, которые *полностью* удовлетворяют конкретным целям безопасности для ОО;

b) *поддерживающие* ФТБ, которые не предназначены для непосредственного удовлетворения целей безопасности для ОО, но которые тем не менее обеспечивают поддержку основных ФТБ, и, следовательно, косвенно помогают удовлетворению соответствующих целей безопасности для ОО.

В ISO/IEC 15408 отсутствует *явное* различие между этими двумя типами ФТБ, но это различие *подразумевается* при рассмотрении зависимостей между функциональными компонентами и демонстрацией взаимной поддержки между ФТБ. Следовательно, пока нет никакой необходимости в том, чтобы ФТБ в ПЗ или ЗБ явно подразделялись на основные или поддерживающие, но при этом необходимо иметь в виду, что разделение ФТБ на два этих типа очень полезно при написании логического обоснования ПЗ или ЗБ.

Первым этапом в процессе выбора ФТБ для каждой цели безопасности для ОО является идентификация основных ФТБ для функциональной модели, которая непосредственно им удовлетворяет. Как только полный набор основных ФТБ будет установлен, тогда последует итерационный процесс формирования полного набора поддерживающих ФТБ. Как уже было указано выше, все ФТБ (основные или поддерживающие), когда это возможно, должны быть сформулированы с использованием соответствующих функциональных компонентов ISO/IEC 15408-2. В 12.3.2 представлены рекомендации по идентификации тех функциональных компонентов, которые необходимо использовать для формулировки общих функциональных требований безопасности. При выборе функциональных компонентов из ISO/IEC 15408-2 необходимо учитывать рекомендации, содержащиеся в приложениях к ISO/IEC 15408-2, относительно того, как выбрать соответствующий компонент и как он должен был интерпретирован.

Взаимосвязь между основными и поддерживающими ФТБ показана на рисунке 4. Эта взаимосвязь является важной для логического обоснования ПЗ или ЗБ, в котором требуется продемонстрировать взаимную поддержку ФТБ. При этом требуется раскрыть характер поддержки, выполняемой *поддерживающими* ФТБ для достижения целей безопасности ОО.

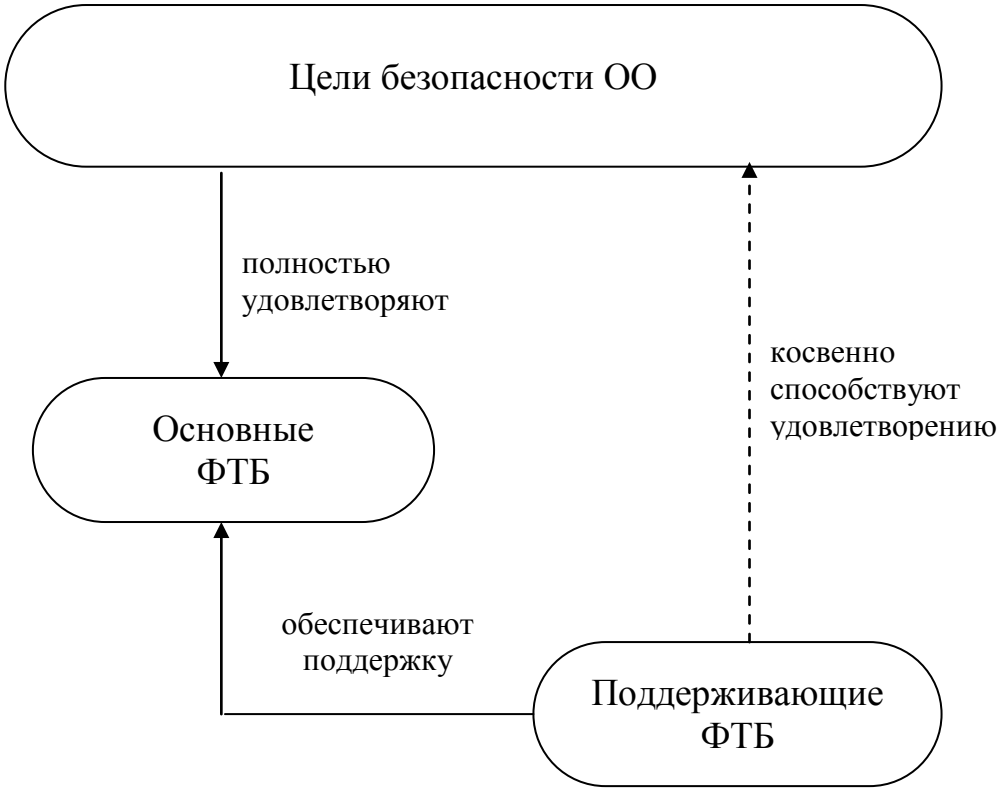

Рисунок 4 – Взаимосвязь между основными и поддерживающими ФТБ

Определение полной совокупности *поддерживающих* ФТБ подразделяется на три этапа:

a) идентификация дополнительных ФТБ, необходимых (с точки зрения разработчика ПЗ) для удовлетворения зависимостей всех основных ФТБ. Она включает любые зависимости *поддерживающих* ФТБ, идентифицированных на этом этапе;

b) идентификация дополнительных ФТБ, которые необходимы для предоставления гарантий того, что цели безопасности для ОО достигнуты. Она включает ФТБ, необходимые для защиты основных ФТБ от многоходовых атак, направленных на преодоление механизмов защиты, реализующих определенную функцию безопасности, затем - на реализацию угрозы, для противодействия которой данная функция безопасности предназначена;

c) идентификация дополнительных ФТБ, необходимых для удовлетворения (с точки зрения разработчика ПЗ) зависимостей тех *поддерживающих* ФТБ, которые были выбраны на втором и третьем этапах.

Идентификация *поддерживающих* ФТБ для удовлетворения зависимостей вероятно будет итеративным процессом, например:

a) предположим, что ПЗ или ЗБ включают в себя цель безопасности,

требующую, чтобы ОО определенным образом реагировал на события, являющиеся показателем предстоящего нарушения безопасности. Это предполагает идентификацию *основного* ФТБ на основе компонента FAU_ARP.1 («Сигналы нарушения безопасности»);

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

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

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

e) компонент FPT_STM.1 не требует предъявления каких-либо требований для дополнительных функциональных компонентов.

Необходимо отметить, что некоторые зависимости могут быть оставлены неудовлетворенными, при этом необходимо пояснить, почему соответствующие ФТБ не нужны для удовлетворения целей безопасности (и, следовательно, обратиться к проблемам безопасности).

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

Обеспечение согласованности для других компонентов может быть более проблематичным. Например, при включении в ПЗ или ЗБ компонента FDP_ACC1 одновременно идентифицируется конкретная ПФБ управления доступом, с которой он связан. При удовлетворении зависимости FDP_ACC1 от компонента FDP_ACF1 необходимо обеспечить применение FDP_ACF.1 к той же ПФБ управления доступом, которая используется для компонента FDP_ACC1. Если к компоненту FDP_ACC1 применяется операция «итерация» для разных ПФБ управления доступом, то зависимость от компонента FDP_ACF.1 должна удовлетворяться для каждой ПФБ управления доступом.

Идентификация дополнительных *поддерживающих* ФТБ (то есть тех, которые согласно ISO/IEC 15408-2 не требуются для удовлетворения зависимостей) включает в себя идентификацию любых других ФТБ, которые считаются необходимыми для обеспечения достижения целей безопасности для ОО. Такие ФТБ обычно должны обеспечивать поддержку путем сокращения вариантов или возможностей, доступных нарушителю, или потребовать от нарушителя более высокого уровня подготовки и значительных ресурсов для проведения успешной атаки. С учетом проблем безопасности и целей безопасности должны быть рассмотрены следующие дополнительные ФТБ:

a) ФТБ, основанные на соответствующих компонентах одного класса ISO/IEC 15408-2 с основными ФТБ. Например, если компонент FAU_GEN.1 («Генерация данных аудита») включен в ПЗ, то может

возникнуть необходимость создания и ведения журнала аудита безопасности для хранения сгенерированных данных (для формулирования подобного требования необходим один или несколько функциональных компонентов из семейства FAU_STG), а также потребность в инструментальных средствах просмотра сгенерированных данных аудита (для формулирования подобного требования необходим один или несколько функциональных компонентов из семейства FAU_SAR). Кроме того, сгенерированные данные аудита безопасности могут быть экспортированы в другую систему для просмотра;

b) ФТБ, основанные на соответствующих компонентах класса FPT («Защита функции безопасности ОО»). Такие ФТБ обычно направлены на защиту целостности и/или доступности ФБО или данных ФБО, на которые полагаются другие ФТБ, хотя они также могут защищать свою конфиденциальность. Например, для защиты ФБО от нарушений, повреждений и модификаций в ПЗ могут быть включены ФТБ на основе компонента FPT_TEE.1 («Тестирование внешних логических объектов») и на основе компонентов семейства FPT_PHP («Физическая защита»), которым при необходимости может потребоваться поддержка целей безопасности для защиты ФБО от отказа, искажения или модификация (возможно с помощью злонамеренных средств);

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

Выбор *поддерживающих* ФТБ должен всегда выполняться в соответствии с целями безопасности и функциональной моделью для того, чтобы сформировать целостный набор поддерживающих друг друга ФТБ. Таким образом, на выбор поддерживающих ФТБ существенное влияние может оказывать процесс создания логического обоснования ПЗ или ЗБ. Необходимо избегать включения в ПЗ или ЗБ *поддерживающих* ФТБ, которые не нужны для достижения целей безопасности, так как включение подобных ФТБ приведет к ограничению сферы применения ПЗ вследствие следующих обстоятельств:

a) возможно, что некоторые ОО не смогут удовлетворить такие ФТБ;

b) увеличение числа ФТБ увеличивает стоимость оценки и количество выполняемых работ при оценке ненужных требований.

Если ПЗ или ЗБ создается на основе другого (базового) ПЗ, то процесс выбора ФТБ значительно упрощается. Однако, принимая во внимание любые различия между постановкой задачи безопасности и/или целями безопасности ОО, в новый ПЗ или ЗБ должны быть включены (где это необходимо) другие ФТБ, отличные от ФТБ базового ПЗ.

12.3.2 Выбор функциональных требований безопасности из ISO/IEC 15408-2

В нижеприведенных таблицах показано соответствие между объясненными парадигмами и компонентами ФТБ, определенными в ISO/IEC 15408-2. Некоторые компоненты охватывают несколько аспектов парадигмы и поэтому они приведены в таблицах 1-6 неоднократно.

Таблица 1 – Управление доступом

Требования	Применимый компонент
Определение субъектов, объектов и операций	FDP_ACC1, FDP_ACC.2, FDP_IFC.1, FDP_IFC.2, FMT_SMF.1
Определение атрибутов безопасности	FDP_DAU.1, FDP_DAU.2, FDP_IFF.1, FDP_IFF.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA.2
Создание субъектов, объектов	FDP_ITC.1, FDP_ITC.2, FMT_SMF.1
Экспорт объектов	FDP_ETC1, FDP_ETC.2
Контроль атрибутов безопасности	FDP_ITC.2, FIA_USB.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FTA_LSA.1
Определение правил доступа	FDP_ACF.1, FDP_IFF.1, FDP_IFF.2, FDP_ROL.1, FDP_ROL.2, FRU_PRS.1, FRU_PRS.2, FRU_RSA.1, FRU_RSA2
Контроль правил управления доступом	FMT_MOF.1, FMT_SMF.1

Таблица 2 – Управление пользователями

Требования	Применимый компонент
1	2
Определение типов пользователей	FMT_SMF.1
Определение атрибутов безопасности	FIA_ATD.1
Правила идентификации пользователя	FIA_UID.1, FIA_UID.2
Правила аутентификации пользователя	FIA_AFL.1, FIA_SOS.1, FIA_SOS2, FIA_UAU.1, FIA_UAU.2, FIA_UAU.3, FIA_UAU.4, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7
Управление верительными данными пользователя и атрибутами безопасности	FMT_MSA.1, FMT_MSA.2, FMT_MSA3, FMT_MSA.4, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1, FMT_SMR.1, FMT_SMR.2, FMT_SMR.3, FTA_LSA.1, FTA MCS.1, FTA_MCS.2
Контроль правил идентификации и аутентификации	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1
Управление связыванием пользователь-субъект	FIA_USB.1

Таблица 3 – Собственная защита ОО

Требования	Применимый компонент
Обнаружение сбоя	FPT_TEE.1, FPT_ITI.2, FPT_ITT.3, FPT_PHP.1, FPT_PHP.2, FPT_PHP.3, FPT_RPL.1, FPT_TST.1, FRU_FLT.1, FRU_FLT.2
Реагирование на сбой	FPT_ITT.3, FPT_PHP.2, FPT_PHP.3, FPT_RCV.1, FPT_RCV.2, FPT_RCV.3, FPT_RSV.4, FPT_RPL.1, FRU_FLT.1, FRU_FLT.2
Контроль правил обнаружения и реагирования	FMT_MCF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1

Таблица 4 – Обеспечение безопасной связи

Требования	Применимый компонент
Установление канала связи	FMT_SMF.1, FTP_ITC.1, FTP_TRP1
Определение характеристик канала связи (атрибутов безопасности)	FCO_NRO.1, FCO_NRO.2, FCO_NRR.1, FCO_NRR.2, FDP_UTC.1, FDP_UIT.1, FDP_UIT.2, FDP_UIT.3, FPT_ITC.1, FPT_ITI.1, FPT_ITI.2, FPT_RPL.1, FTP_ITC.1, FTP_TRP.1
Контроль характеристик канала связи	FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_REV.1, FMT_REV.2, FMT_SAE.1
Контроль правил установления связи	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3, FMT_SMF.1, FTA_SSL.1, FTA_SSL.2, FTA_SSL.3. FTA_SSL.4, FTA_TAB.1, FTA_TAH.1.FTA TSE.1

Таблица 5 – Аудит

Требования	Применимый компонент
Определение событий, подлежащих аудиту	FAU_GEN.1, FAU_GEN.2, FAU_SEL.1
Определение реагирования на события	FAU_ARP.1, FAU_SAA.1, FAU_SAA.2, FAU_SAA3, FAU_SAA.4
Определение управления событиями	FAU_SAR.1, FAU_SAR.2, FAU_SAR.3
Определение управления журналом аудита	FAU_STG.1
Контроль правил аудита	FMT_MOF.1, FMT_MTD.1, FMT_MTD.2, FMT_MTD.3

Таблица 6 – Требования к архитектуре

Требования	Применимый компонент
Защита журнала аудита	FAU_STG.2, FAU_STG.3, FAU_STG.4
Криптографические функции	FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4, FCS_COP.1
Управление потоками информации	FDP_IFF.3, FDP_IFF.4, FDP_IFF.5, FDP_IFF.6
Передача в пределах ОО	FDP_ITT.1, FDP_ITT.2, FDP_ITT.3, FDP_ITT.4
Защита остаточной информации	FDP_RIP.1, FDP_RIP.2
Целостность хранимых данных	FDP_SDI.1, FDP_SDI.2
Управление	FMT_MTD.1
Защита приватности	FPR_ANO.1, FPR_ANO.2, FPR_PSE.1, FPR_PSE2, FPR_PSE.3, FPR_UNL.1, FPR_UNO.1, FPR_UNO.2, FPR_UNO.3, FPR_UNO.4
Безопасность при сбое	FPT_FLS.1
Доступность	FPT_ITA.1, FPT_ITT.1, FPT_ITT.2
Синхронизация состояния	FPT_SSP.1,FPT_SSP.2
Безопасность меток времени	FPT_STM.1
Согласованность данных	FPT_TDC.1,FPT_TRC.1

После того, как в соответствии с 12.2 и 12.3.1 будет определена функциональная модель безопасности, с помощью этих таблиц можно будет определить соответствующие компоненты ФТБ. Таблицы позволят разработчику ЗБ или ПЗ принять решение, какой компонент он выберет и как он сформулирует аспект функциональной модели безопасности, используя компонент и разрешенные операции.

Для формулирования требований к архитектуре в соответствующих компонентах ФТБ ISO/IEC 15408-2 подготовлен и отображен список возможных вопросов.

12.3.3 Выполнение операций над функциональными требованиями безопасности

12.3.3.1 Разрешенные операции

Как было установлено в 10.1 (также см. 2.1.4 ISO/IEC 15408-2), над некоторыми функциональными компонентами могут выполняться разрешенные операции, которые необходимы разработчику ПЗ или ЗБ для формулирования соответствующего данному ПЗ или ЗБ требования безопасности. К разрешенным операциям относятся:

a) *назначение* - позволяет специфицировать идентифицированный параметр;

b) *итерация* - позволяет неоднократно использовать один и тот же функциональный компонент для определения различных требований;

c) *выбор* - позволяет специфицировать один или несколько элементов из заданного списка;

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

12.3.3.2 Операция «итерация»

Операция «итерация» часто используется для определения ФТБ на основе компонентов класса FMT («Управление безопасностью»), которые включаются в ПЗ для удовлетворения зависимостей многих других функциональных компонентов ISO/IEC 15408-2. Для удовлетворения таких зависимостей обычно необходимо использовать одни и те же компоненты класса FMT, над которыми иначе выполнены операции «назначение» и «выбор». Например, компонент FMT_MSA.1 может быть использован неоднократно для определения различных ФТБ, которые предназначаются для управления атрибутами безопасности разных типов. Также может потребоваться неоднократное использование компонентов семейств FDP_ACC и FDP_ACF в тех случаях, когда потребуется, чтобы ОО реализовывал различные политики управления доступом, например, дискреционное управление доступом и управление доступом на основе ролей.

Целесообразно использовать операцию «итерация» для внесения дополнительной ясности в ПЗ, например, для того, чтобы разбить сложное и громоздкое ФТБ на отдельные и удобные в управлении ФТБ. Однако, возможно, что при использовании операции «итерация» могут возникнуть другие проблемы при демонстрации ФТБ в ПЗ и ЗБ.

12.3.3.3 Операции «назначение» и «выбор»

При выполнении операции «назначение» существует такая вероятность, когда значение параметра может стать равно нулю, тогда как при выполнении операции «выбор» имеется всегда, по крайней мере, одно значение идентифицированного параметра. В случае завершения операций «назначение» и «выбор» в ПЗ разработчик ЗБ не сможет принять какое-либо решение относительно того, как должен использоваться функциональный компонент для удовлетворения целей безопасности (кроме

операции «уточнение»). Другими словами, снижается ответственность разработчика ЗБ.

Обычно отдельные операции «*назначение*» или «*выбор*» должны быть завершены разработчиком ЗБ. Чрезмерные изменения при выполнении операций или чрезмерная детализация ПЗ могут излишне ограничить количество ОО, которые могли бы соответствовать требованиям данного ПЗ. Для оптимального выполнения операций в ПЗ необходимы:

a) полный набор требований разработчика;

b) независимость от реализации;

c) достаточная детализация, необходимая для демонстрации достижения цели.

Следовательно, операции «назначение» и «выбор» целесообразно выполнять, исходя из необходимости демонстрации достижения целей безопасности. Основным тестом будет являться логическое обоснование требований безопасности: аргументы, представленные для демонстрации пригодности требований безопасности ИТ для удовлетворения целей безопасности, не должны основываться на деталях, которые не были специфицированы в ФТБ. Например, в случае 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 были определены в ПБОр, для удовлетворения которой предназначена соответствующая цель безопасности (управление доступом). В этом случае разработчик ПЗ должен завершить операции «назначение» и «выбор», поскольку необходимо удовлетворить общую цель безопасности, оставляя достаточную свободу разработчику ЗБ, который соблюдая требования ПЗ, определит специфические особенности правил управления доступом, реализованные в ОО.

Один из рекомендуемых методов решения вышеуказанной проблемы - *частичное* выполнение операций. Согласно этому подходу, можно предоставить разработчику ЗБ максимальную свободу действий и в то же самое время предотвратить выполнение операций «назначение» и «выбор», которые не будут соответствовать целям безопасности для ОО.

Например, в ФТБ (основанном на FAU_STG.4.1) операция «выбор» выполнена частично путем предотвращения выбора варианта «игнорирование подвергаемых аудиту событий», который разработчик ПЗ считает противоречащим целям безопасности для ОО. Следовательно, ФТБ предоставляет разработчику ЗБ два (а не три) приемлемых варианта выбора:

*ФБО должна выполнить [выбор: '**предотвращение событий, подвергающихся аудиту, кроме предпринимаемых авторизованным пользователем со специальными правами', 'запись поверх самых старых хранимых записей аудита**'] и [назначение: **другие действия, которые нужно предпринять в случае возможного отказа при сохранении данных аудита**] при переполнении журнала аудита.*

С помощью операций «назначение» разработчик ПЗ может ограничить разработчику ЗБ выбор вариантов, приемлемых для среды. В этом случае, разработчик ПЗ может выполнить операцию «назначение», преобразовав ее в операцию «выбор», содержащую допустимые варианты, и которая, в свою очередь, может быть завершена разработчиком ЗБ.

Общий принцип - *частичное* выполнение операции «выбор» допустимо, если набор полученных вариантов является подмножеством вариантов, разрешенных для исходного функционального компонента. Точно также *частичное* выполнение операции «назначение» допустимо, если разрешенные значения для выполнения операции «назначение» является также 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 логически простым. При выполнении операции «назначение» разработчик должен просто гарантировать, чтобы параметр был определен однозначно. При выполнении операции «выбор» разработчик должен выбрать соответствующие варианты, основанные на анализе целей безопасности для ОО. Кроме того, разработчик, при возникновении сомнений, должен обращаться к рекомендациям, содержащимся в приложениях ISO/IEC 15408-2.

При выполнении операций «назначение» и/или «выбор» в ПЗ необходимо обязательно выделять другим шрифтом специфицированный текст в целях большей наглядности (необходимо для пользователей ПЗ и, особенно, для оценщика ПЗ при проверке соответствия ПЗ требованиям ISO/IEC 15408). Общепринятым способом выделения является использование курсива, но не жирного шрифта, или использование другого набора символов.

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

ФБО должны ограничить возможность назначать ***уполномоченным администратором*** *срок действия* ***паролей пользователей****.*

В этом случае для выделения используется жирный шрифт, так как существующий пример текста уже выделен курсивом.

Если операция остается невыполненной, то необходимо пояснить, что выполнение операции возлагается на разработчика ЗБ.

Любые невыполненные (либо выполненные частично) операции должны, где это необходимо, сопровождаться рекомендациями разработчику ЗБ о том, каким образом следует выполнять операции (например, в виде примечания по применению). Это возможно поможет понять, что ответственность за спецификацию деталей возлагается на разработчика ЗБ.

Например, FDP_RIP.1.1 может быть определен в ПЗ как:

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

Для каждого ФТБ, включенного в ПЗ, необходимо принять решение относительно того, как выполнять каждую операцию «*назначение*» или «*выбор*», включенную в функциональный компонент, используемый при определении ФТБ. В ЗБ все операции «назначение» и «выбор» должны быть выполнены.

12.3.3.4 Операция «уточнение»

Для каждого ФТБ, включенного в ПЗ или ЗБ, необходимо принять решение относительно того, как определить каждое *уточнение* ФТБ.

Операция «уточнение» может быть выполнена для любого элемента любого функционального компонента и заключается в добавлении некоторых технических деталей, которые не выдвигают никаких новых требований, к определенным в тексте, но ограничивают набор допустимых реализаций.

Операция «уточнение» допустима, если выполнение уточненного требования приводит к выполнению не уточненного требования.

Использование операции «уточнение» целесообразно в следующих случаях:

a) когда ПЗ разрабатывается организацией, которая имеет дополнительные технические данные, не включенные в соответствующий компонент ISO/IEC 15408-2, например, информацию о политике организации;

b) когда выбранный функциональный компонент допускает ненадлежащую для рассматриваемого типа ОО реализацию требования безопасности и необходимо исключить такую возможность, например, на основе интероперабельности;

c) когда может быть повышена читабельность ФТБ.

Точно также, как и для операций «назначение» и «выбор», рекомендуется выделять текст уточнения, чтобы помочь пользователю (и, особенно, оценщику ПЗ).

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

ФБО должны обеспечить присвоение данным ФБО только безопасных значений. ***Уточнение: ФБО должны обеспечить, чтобы минимальная длина пароля, требуемого ОО, составляла не менее 6 символов****.*

12.3.4 Спецификация требований аудита

Если в ПЗ или ЗБ включены требования аудита (основанные на компоненте FAU_GEN.1), то при формировании всех остальных функциональных требований, включаемых в ПЗ или ЗБ, необходимо специфицировать минимальные набор событий и объем информации,

подлежащие аудиту.

Выбор подлежащих аудиту событий и информации зависит от множества факторов, включая:

a) любые требования политики безопасности к аудиту безопасности, определенные в ПБОр;

b) значение аудита безопасности для достижения целей безопасности;

c) взаимосвязь некоторых событий и их характеристик с целями безопасности;

d) анализ «стоимость-эффективность».

Например, если ОО предназначен для защиты от действий злоумышленников или хакеров, то аудиту должны подлежать события, связанные с нарушением процедуры доступа в систему или управления доступом, то тогда в ПЗ или ЗБ включают такие ФТБ. В то же время, в состав событий, подлежащих аудиту, можно не включать события, связанные с функциями администрирования, в зависимости от степени доверия, которым администратор обладает (или должен обладать), в этом случае степень доверия к администратору должна быть изложена как предположение.

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

a) является ли полезным сбор информации и влияет ли он на функционирование;

b) имеются ли у администратора необходимые ресурсы (например, соответствующие инструментальные средства) для эффективного анализа собранных данных;

c) величина предполагаемых затрат на управление и хранение собираемых данных.

В 2.1.2.5 ISO/IEC 15408 введены три предопределенных уровня аудита: минимальный, базовый и детализированный: соответственно для каждого предопределенного уровня определен минимальный набор событий, подлежащих аудиту, а также минимальный объем подлежащей регистрации информации с привязкой к функциональным компонентам, содержащихся в ПЗ или ЗБ (ISO/IEC 15408-2, C.2). Эти три уровня могут быть приблизительно охарактеризованы следующим образом:

a) *минимальный* уровень аудита обычно требует, чтобы аудиту подвергалось только определенное подмножество действий или событий, связанных с данным функциональным компонентом. Это подмножество обычно определяется, как наиболее значимые события, представляющие наибольший интерес;

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

c) *детализированный* уровень аудита обычно отличается от *базового* уровня наличием требований регистрации дополнительной информации, представляющей наибольший интерес. Этот уровень необходим в тех случаях, когда объем генерируемых данных аудита недостаточен или анализ данных аудита предполагается проводить с использованием современных инструментальных средств или средств обнаружения вторжения.

Если ни один из перечисленных уровней не является надлежащим, то целесообразно выбрать *неопределенный* уровень аудита и подробно перечислить в списке все подлежащие аудиту события в элементе FAU_GEN.1.1. Например, можно принять за основу *минимальный* уровень аудита, но в некоторых специфических случаях отклониться от *минимальных* требований, поскольку другое подмножество действий или событий является более значимым для достижения целей безопасности, например, если компонент FDP_ACF.1 включен в ПЗ или ЗБ, то может потребоваться более детальный аудит неудачных попыток доступа, а не аудит успешных попыток, который необходим согласно ISO/IEC 15408-2 для *минимального* уровня.

Для того, чтобы сформировать список событий, подлежащих аудиту, необходимо проанализировать поочередно каждый использованный функциональный компонент; если же назначен один из предопределенных уровней аудита - *минимальный*, *базовый* или *детализированный*, то подлежащие аудиту события подробно идентифицируются в подразделе «Аудит» описания семейства компонентов. Следует сформировать таблицу, идентифицирующую события и (при необходимости) дополнительную информацию, подлежащую регистрации, которая может упоминаться в FAU_GEN.1.1 и FAU_GEN.1.2.

12.3.5 Спецификация требований управления

В подразделе «Управление» ISO/IEC 15408-2 для каждого семейства компонентов определен список действий управления применительно к компонентам. Наличие списка действий управления может предполагать необходимость включения специфических компонентов из класса FMT («Управление безопасностью»). Тем не менее, важно обратить внимание на то, что этот подраздел является *справочным*. Следовательно, не требуется обосновывать какое-либо решение не включать в ПЗ или ЗБ специфические компоненты управления (если, конечно, они явно не идентифицированы в подразделе «Зависимости» ISO/IEC 15408-2).

В общем случае, возможные действия управления идентифицируются, когда функциональный компонент ссылается на конфигурируемые данные ФБО (или подразумевает их существование), 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. Следовательно, компоненты класса FMT часто включаются для определения *поддерживающих* ФТБ, способствующих достижению целей

безопасности для ОО, и для того, чтобы ФТБ в целом являлись взаимно поддерживающими.

Действия управления могут быть получены из функциональной модели ОО. Учитываются следующие действия управления:

- регистрация и дерегистрация (удаление) пользователей;
- создание объектов;
- модификации атрибутов безопасности пользователей, объектов, сессий и т.д.;
- изменения в поведении функций безопасности (в том числе включение и выключение всех или части функций ОО);
- модификация параметров аудита;
- изменение внутренних переменных состояния ФБО, которые являются существенными для безопасности (например, изменение режима технического обслуживания).

При выборе функциональных компонентов класса FMT необходимо использовать рекомендации, содержащиеся в ISO/IEC 15408-2 (приложение H).

12.3.6 Спецификация функциональных требований безопасности, позаимствованных из профиля защиты

Если в ЗБ заявлено соответствие ФТБ одному или нескольким ПЗ, то, вероятно, что эти ФТБ уже были определены или во всех, или в большей части ПЗ. В таких случаях разработчик ЗБ должен решить, определить ли функциональные требования ПЗ полностью (чтобы весь текст находился в одном месте) или просто сослаться на ПЗ, а определить только те ФТБ, которые отличаются от ФТБ, определенных в ПЗ.

В последнем случае ЗБ становится более простым, но при этом, для получения полной картины, пользователю будет необходимо ознакомиться как с ПЗ, так и с ЗБ. Очень вероятно, что пользователей ЗБ интересуют больше функции безопасности ИТ, чем ФТБ. Это же относится и к оценщику ОО (так как содержание свидетельств оценки, например, проектной, тестовой документации и руководств в краткой спецификации ОО гораздо проще привязать к функциям безопасности ИТ, чем к ФТБ). Основная цель определения ФТБ в ЗБ - демонстрация соответствия ФТБ ЗБ функциональным требованиям соответствующих ПЗ и функциональным требованиям, определенным в ISO/IEC 15408-2. В некоторых случаях описание ФТБ помещают в приложение, исходя из тех соображений, чтобы не вводить пользователя ЗБ в заблуждение наличием в ЗБ двух спецификаций функциональных возможностей безопасности.

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 определены, операции полностью завершены, а их результат выделен (например, курсивом). Все необходимые пояснения должны быть также выделены. Такой подход облегчает пользователю ЗБ (и, в частности, оценщику ЗБ) понять, какие операции и каким образом были

выполнены, а также облегчает формирование логического обоснования ЗБ.

12.3.7 Спецификация функциональных требований безопасности, отсутствующих в профиле защиты

В некоторых случаях будет необходимо в ЗБ определить ФТБ, которые отсутствуют в соответствующем ПЗ. Это может быть необходимо тогда, когда:

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

b) спонсор считает, что преимущества от включения дополнительных относительно ПЗ функциональных требований или требований доверия оправдывают дополнительные расходы.

В этих случаях используют метод определения ФТБ, аналогичный вышеописанному методу. Если в ЗБ включаются дополнительные относительно ПЗ требования, то разработчик ЗБ должен гарантировать, что они не противоречат ФТБ, включенным в ПЗ (в логическом обосновании ЗБ должно быть продемонстрировано отсутствие противоречия).

12.3.8 Спецификация функциональных требований безопасности, отсутствующих в ISO/IEC 15408-2

Если при разработке ПЗ или ЗБ возникает потребность включить функциональное требование, для которого в ISO/IEC 15408-2 отсутствует соответствующий функциональный компонент, то для вновь полученного ФТБ необходимо использовать модель представления функциональных компонентов ISO/IEC 15408-2.

Принятие решения о наличии соответствующего функционального компонента в ISO/IEC 15408-2 может оказаться сложным для разработчика, т. к. это предполагает хорошее знание ISO/IEC 15408-2. С учетом этого рекомендуется использовать 12.3.2 настоящего стандарта, в котором определены подходящие функциональные компоненты из ISO/IEC 15408-2, соответствующие основным функциональным требованиям безопасности. В большинстве случаев надлежащее ФТБ может быть получено при соответствующем использовании операции «уточнение» или разрешенной операции «назначение» или «выбор». Однако не рекомендуется формулировать ФТБ на основе конкретного функционального компонента, если это сразу не приводит к формированию надлежащего ФТБ, если содержание или назначение полученного ФТБ не могут быть легко поняты пользователем, или если это ФТБ с помощью несоответствующего компонента вводит, например, зависимости, не соответствующие целям безопасности.

Руководство по определению расширенного компонента приведено в разделе 11.

12.3.9 Представление функциональных требований безопасности

Написание набора ФТБ, которые удовлетворяют требованиям ISO/IEC 15408, не является единственной целью разработчика ПЗ или ЗБ. Необходимо лучше всего представить и выразить ФТБ так, чтобы пользователь мог понять, что означают эти требования безопасности.

Существует множество методов, которые можно использовать для повышения читабельности, обеспечивая при этом согласованность с ISO/IEC 15408.

Во-первых, целесообразно объединить ФТБ в группы и озаглавить их в соответствии с контекстом ПЗ или ЗБ. Заголовки групп ФТБ могут отличаться от заголовков классов, семейств и компонентов, используемых в ISO/IEC 15408-2.

Во-вторых, для маркировки ФТБ в ПЗ или ЗБ совсем не обязательно использовать систему маркировки функциональных элементов, принятую в ISO/IEC 15408-2. Для этих целей разработчик ПЗ или ЗБ может использовать свою собственную систему маркировки ФТБ (например, на основе более информативных меток). При использовании собственной системы маркировки ФТБ разработчик ПЗ или ЗБ должен продемонстрировать (например, в приложении) отображение представленных ФТБ на соответствующие функциональные компоненты, определенные в ISO/IEC 15408-2. Такой подход к маркировке ФТБ является более предпочтительным в частности тогда, когда в ПЗ или ЗБ имеются неоднократные ссылки на одни и те же функциональные компоненты. Это является альтернативой для тех ФТБ, которые не имеют собственной маркировки: отсутствие собственной маркировки представляет значительную проблему при формировании логического обоснования 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. Ниже приведен пример ФТБ, сформулированного на основе FMT_MSA.3.1:

ФБО должны осуществлять ***политику дискреционного управления доступом****, чтобы обеспечить* ***ограничительные*** *значения по умолчанию для разрешений на доступ к объекту.*

В этом примере операция «уточнение» использовалась для того, чтобы в формулировке ФТБ заменить выражение более общего характера «атрибуты безопасности, которые используются при выполнении ПФБ» специфическим выражением «разрешения на доступ к объекту».

Результат выполнения операции «уточнение» в формулировке ФТБ должен быть выделен курсивом (или другим способом). Каждое использование операции «уточнение» должно сопровождаться соответствующим пояснением в ПЗ или логическом обосновании ЗБ (для облегчения последующей оценки ПЗ или ЗБ).

12.3.10 Разработка логического обоснования требований безопасности

За исключением тех случаев, когда ЗБ или ПЗ соответствует низкому уровню доверия (см. 15.1), необходимо логическое обоснование, содержащее объяснение, каким образом функциональные требования безопасности удовлетворяют целям безопасности. В логическом обосновании должны быть прослежены все цели безопасности относительно функциональных требований безопасности, которые все вместе взятые должны быть адресованы целям. Это прослеживание должно показать, что каждое ФТБ учитывает, по крайней мере, одну цель безопасности, и каждой цели безопасности соответствует, по крайней мере, одно ФТБ.

В большинстве случаев одна цель безопасности соответствует нескольким ФТБ и часто одно ФТБ учитывает несколько целей безопасности. В большинстве ЗБ и ПЗ количество ФТБ должно превышать количество целей безопасности, поскольку цели безопасности должны иметь более общий характер, чем ФТБ.

Например, цель безопасности «*ОО должен однозначно идентифицировать каждого пользователя и выполнять процедуру аутентификации идентифицированного пользователя до предоставления ему доступа к средствам ОО*» наиболее вероятно будет отображена несколькими ФТБ, определяющими:

- как будет происходить идентификация пользователей;
- как будет происходить аутентификация пользователей;
- что случится при неудачной аутентификации;
- как будет происходить создание пользователей и их аутентификационных данных, а также управление ими;
- как будет осуществляться разграничение доступа пользователей и субъектов.

Более важным, чем прослеживание целей безопасности относительно ФТБ, является объяснение достаточности ФТБ для удовлетворения каждой цели безопасности. Для вышеприведенного примера это объяснение может быть легко получено, но оно не будет верным для всех целей безопасности. Особенно в случае целей безопасности, которые определяют характеристики ОО, объяснение того, что ФТБ полностью удовлетворяют цели безопасности, может быть нестандартным. Например, для цели безопасности «*ОО должен гарантировать, что к информации субъекта, работающего с определенной меткой безопасности, не сможет получить доступ субъект, работающий с иерархически более низкой или несовместимой меткой безопасности*».

Сложно объяснить, что ФТБ полностью удовлетворяют цели безопасности для структуры, основанной на политике полномочного управления доступом. Например, в архитектуру для обеспечения лучшей поддержки управления потоком информации могут быть добавлены дополнительные ФТБ, но при всем этом будет не возможно доказать, что

совокупность ФТБ полностью удовлетворяет цели безопасности. Например, даже при правильной реализации всех ФТБ могут существовать скрытые каналы, позволяющие передавать информацию способом, который противоречит цели безопасности. В объяснении достаточности, являющемся частью логического обоснования требований безопасности, это должно быть признано и указано, что в пределах модели ОО предусмотренная совокупность ФТБ полностью удовлетворяет цели безопасности, то есть там отсутствуют ФТБ, которые противоречат цели безопасности.

В общем, выполнить прослеживание между целями безопасности и ФТБ, а также объяснить достаточность будет легче, когда цели безопасности будут выражены как функции, а не как характеристики, уровень детализации которых будет максимально приближен к уровню, представленному в ФТБ. Следовательно, цели безопасности должны быть как можно более точными. При написании ЗБ или ПЗ следует повторно рассмотреть цели безопасности и попытаться сформулировать их более точно при наличии проблемы с прослеживанием целей безопасности относительно ФТБ или с объяснением того, что ФТБ полностью удовлетворяют цели безопасности.

12.4 Спецификация требований доверия к безопасности в профилях защиты и заданиях по безопасности

12.4.1 Выбор требований доверия к безопасности

При выборе требований доверия к безопасности требуется сбалансированность нескольких факторов, включая:

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

b) возможность технической реализации;

c) стоимость разработки и оценки;

d) необходимое время для разработки и оценки ОО;

e) требования рынка (для продуктов ИТ);

f) любые определенные зависимости функциональных компонентов и компонентов доверия к безопасности.

Чем выше ценность активов, подлежащих защите, и чем больше риск компрометации этих активов, тем более высокий уровень доверия к безопасности необходим для функций безопасности, используемых для защиты рассматриваемых активов. Это должно быть отражено в формулировке целей безопасности. Организации могут устанавливать собственные политики и правила определения уровня доверия к безопасности, который необходим для снижения риска для этих активов до приемлемого уровня. Это, в свою очередь, определяет необходимый уровень доверия к безопасности продуктов ИТ, которые предполагается использовать в этой организации.

Другие факторы, например, стоимость и затраты времени, как правило, ограничивают уровень доверия к безопасности, который является практически достижимым. Возможность технической реализации рассматривается в том случае, когда считается практически нецелесообразной подготовка свидетельства, требуемого конкретными компонентами доверия к безопасности. Это может быть очень важно для наследуемых систем (при отсутствии полного комплекта конструкторской документации) или когда теоретически требуется высокий уровень доверия к безопасности, но технически невозможно за приемлемое время подготовить требуемое полуформальное либо формальное 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 в формулировке целей безопасности.

Формулировка целей безопасности может также указывать на то, какие специфические требования доверия к безопасности должны быть включены в ТДБ. Например:

a) цели безопасности для ОО могут устанавливать, что ОО должен противодействовать нарушителям с высоким атакующим потенциалом. Очевидно, что будет необходимо включить компонент AVA_VAN.5, который потребует такое противодействие, какое только можно продемонстрировать;

b) в целях безопасности может быть указано, что в тех случаях, когда собственная защита, разделение домена или невозможность обхода являются проблемой, тогда необходимо включить компонент ADV_ARC.1. Следует отметить, что класс ADV_ARC содержит только один компонент, но требуемый уровень архитектурного описания зависит от компонента, выбранного из класса ADV_TDS;

c) при формулировке целей безопасности может быть отмечено, что безопасность ОО очень сильно зависит от безопасности среды разработки. В этом случае настоятельно рекомендуется включить в набор ТДБ компонент из семейства ALC_DVS, гарантирующий, что безопасность среды разработки проанализирована.

Выбор ТДБ сравнительно прост, если необходимо выбрать только подходящий пакет доверия к безопасности, например, ОУД из ISO/IEC 15408. Прежде чем выбрать подходящий с точки зрения сформулированных целей безопасности пакет доверия к безопасности, необходимо изучить его описание (например, в случае выбора ОУД см. раздел 6 ISO/IEC 15408-3). Возможно, что пакет доверия к безопасности соответствует требуемому уровню доверия, но в нем отсутствуют требования, связанные с некоторыми целями безопасности. В этих случаях целесообразно включать расширенные требования доверия к безопасности (то есть требования, которые являются дополнительными по отношению к пакету) для того, чтобы проверить, все ли цели безопасности удовлетворены.

Если в ПЗ или ЗБ определены расширенные требования доверия к безопасности, то разработчик ПЗ или ЗБ должен проверить, удовлетворяет ли расширенное ТДБ этим дополнительным требованиям. Например, если в ПЗ или ЗБ пакет ОУД3 расширен с помощью компонента AVA_VAN.3, то в ПЗ или ЗБ также необходимо включить компоненты ADV_TSD.3 и ADV_IMP.1. Кроме того, также должен быть включен компонент ADV_FSP.4, так как ADV_TDS.3 имеет зависимость от ADV_FSP.4.

12.4.2 Выполнение операций над требованиями доверия к безопасности

Возможны следующие операции:

a) «*итерация*», позволяющая многократно использовать один и тот же компонент доверия к безопасности;

b) «*уточнение*», позволяющая добавлять детали к требованию доверия к безопасности;

c) «*назначение*», позволяющая присваивать значение элементу ТДБ вместе с присвоением значения параметру.

На практике выполнение операции «итерация» должно использоваться только в тех случаях, когда для одного и того же компонента доверия к безопасности нужны разные «уточнения», которые относятся к разным частям ОО, либо когда в ПЗ или ЗБ определены разные наборы ТДБ для разных компонентов составного ОО (см. 14.1). В последнем случае операция «итерация» требуется для компонентов доверия к безопасности (уточненных или не уточненных), которые используются для нескольких компонентов составного ОО.

Операция «уточнение» может быть использована применительно к ТДБ, чтобы:

a) ограничить действия разработчика путем предписания использовать конкретные инструментальные средства разработки, методологии, модели жизненного цикла, методы анализа, системы обозначений, строгое соблюдение требований определенных стандартов и т.д.;

b) ограничить действия оценщика, например:

- в случае компонента ADV_IMP.1, определяющего какие части представления реализации ОО должны быть включены в оцениваемый поднабор;

- в случае компонента AVA_VAN.1, идентифицирующего специфический минимальный набор публичных доменов источников уязвимостей, которые должны быть учтены, так как они описывают уязвимости, соответствующие контексту ОО.

Существуют только два случая в списках ТДБ ISO/IEC 15408-3, когда разрешается выполнение операций «назначение»: ADV_INT.1.1D и ADV_SPM.1.1D. В первом случае разработчик ПЗ/ЗБ должен определить операцию «назначение» поднабора ФБО, для которого применяется элемент, во втором случае, разработчик ПЗ/ЗБ должен определить операцию «назначение» набора политик безопасности, которые формально оформлены.

12.4.3 Спецификация требований доверия к безопасности, отсутствующих в ISO/IEC 15408-3

Если разработчик ПЗ или ЗБ захочет включить расширенное ТДБ, для которого в ISO/IEC 15408 отсутствует соответствующий компонент доверия к безопасности, то он при получении расширенного ТДБ должен использовать модель представления компонентов ISO/IEC 15408-3. Рекомендации по определению расширенного компонента доверия в ПЗ или ЗБ представлены в разделе 11.

12.4.4 Логическое обоснование требований доверия к безопасности

Структура ПЗ и ЗБ (за исключением низкого уровня доверия, который рассмотрен в 15.1) также должна содержать логическое обоснование выбора этого набора ТДБ. ТДБ могут быть получены из ПЗБ, целей безопасности, а также из других источников. ISO/IEC 15408-1 позволяет не предоставлять каких-либо объяснений относительно того, каким образом были получены ТДБ или ссылаться на конкретные нормативные документы, которые требуют использовать определенный набор ТДБ.

Во многих случаях ТДБ получают на основе анализа угроз и агентов угроз, идентифицированных при ПЗБ с целью выбрать такие ТДБ, чтобы ОО мог противостоять атакам, инициируемых агентами угроз, содержащимися в постановке задачи безопасности. В этом случае все это необходимо отразить в логическом обосновании выбора ТДБ.

13 Краткая спецификация объекта оценки

Краткая спецификация ОО необходима только для ЗБ, для ПЗ она не нужна. Назначение краткой спецификации ОО заключается в том, чтобы обеспечить пользователей описанием функций безопасности ОО, объясняющим как были выполнены ФТБ. Следовательно, краткая спецификация ОО должна содержать описание функции безопасности в контексте общих функциональных возможностей и архитектуры ОО, обеспечивающее достаточную детализацию для получения абстрактного представления об ОО и о способах реализации ФТБ в ОО.

Краткая спецификация ОО представляет собой абстрактную модель всего ОО, ориентированную на безопасность, где субъекты, объекты, атрибуты безопасности и правила, определенные в ФТБ, помещены в контекст архитектуры ОО и ее общие функциональные возможности. Тем не менее эта модель может быть абстрагирована от целого ряда функций, которые обеспечивает ОО и которые не являются функциями безопасности, до тех пор, пока эти функции не связаны с функциональными возможностями безопасности, реализованными в ОО. Уровень детализации, представленный в краткой спецификации ОО, должен быть выше, чем уровень детализации в описании ОО, и сфокусирован на объяснении, как обеспечивается выполнение ФТБ. Необходимо

отобразить, каким образом функциональные возможности безопасности, описанные в краткой спецификации ОО, выполняют ФТБ.

Как правило, краткая спецификация ОО должна начинаться с общего обзора, в котором представлена архитектура абстрактного ОО, содержащая ограничения ФБО. Будет полезно также описать, как ФБО защищает себя от взлома и обхода, даже если не требуется соответствие ASE_TSS.2. Затем на основе функциональной модели, которая использовалась для получения ФТБ, должны быть описаны функции безопасности. Параллельно следует писать краткую спецификацию ОО и раздел с описанием ФТБ, это обеспечит согласованность каждого ФТБ с функциональной моделью и при этом разработку отображения ФТБ на функции безопасности, описанные в краткой спецификации ОО. Краткая спецификация ОО должна в основном содержать функциональную модель (см. 12.2), дополненную текстом, который помещает эту модель в контекст целого ОО со всеми его функциями и архитектурой. Ознакомившись с краткой спецификацией ОО, читатель поймет, почему определенные функции безопасности или их части были выбраны и как они поддерживают общие функциональные возможности ОО. Кроме того, преобразование краткой спецификации ОО в ФТБ обеспечивается автоматически, так как они получены из одной вышеупомянутой модели.

В краткой спецификации составного ОО должны быть описаны отдельные компоненты и их взаимодействие при выполнении ФТБ. Из описания должно быть понятно, как ФТБ для составного ОО могут быть отображены в компонентах ФТБ и как эти ФТБ взаимодействуют. В 14.1 приведены рекомендации относительно ЗБ для составного ОО.

14 Профили защиты и задания по безопасности для составных объектов оценки и компонентов объектов оценки

14.1 Составные объекты оценки

В рамках операционной среды большинство ОО взаимодействует с другими продуктами или системами ИТ. Во многих случаях им для удовлетворения функциональных требований безопасности необходима поддержка таких продуктов или систем ИТ. Например, ОО, являющийся системной базой данных, взаимодействует с операционной системой, обеспечивающей защиту файла, разделение адресного пространства и функцию аутентификации пользователя. Другим примером является операционная система, зависящая от внешнего LDAP-сервера, на котором хранятся цифровые сертификаты и списки аннулированных сертификатов, используемые для аутентификации. Операционная система также зависит от внешней PKI, которая генерирует эти сертификаты, списки аннулированных сертификатов и своевременно публикует их на LDAP-сервере. Объединив оба этих примера, можно увидеть, что СУБД (зависящая от аутентификации пользователя в операционной системе)

также зависит от аутентификации пользователя в LDAP-сервере и PKI-системе. Этот пример можно легко расширить, если для аутентификации пользователя используются смарт-карты. В этом случае существуют зависимости непосредственно как от самих смарт-карт, но так и от системы их персонализации.

Эти примеры показывают, что на первый взгляд простое функциональное требование безопасности (аутентификация пользователя) может потребовать корректного и безопасного взаимодействия множества продуктов ИТ, каждый из которых может быть оценен отдельно. В этом подразделе рассматривается задача определения функциональных требований безопасности ОО в соответствии с целями безопасности среды ОО, чтобы сформулировать эту задачу как функциональные требования безопасности, выполняемые совокупностью продуктов ИТ.

В вышеизложенных примерах выявлены следующие зависимости:

- СУБД зависит от операционной системы, выполняющей аутентификацию пользователя, защиту файла и разделение адресного пространства;

- операционная система зависит от используемых аппаратных средств разделения адресного пространства и защиты от прямого доступа непривилегированных программ, прилагаемых к устройствам ввода/вывода и предназначенных для регистров конфигурации процессора;

- операционная система зависит от LDAP-сервера, защищающего информацию аутентификации пользователя от несанкционированного доступа. Она также зависит от LDAP-сервера, оперативно предоставляющего по запросу информацию, который также защищает информацию от необнаруженной модификации во время передачи между LDAP-сервером и операционной системой;

- операционная система зависит от PKI, предназначенной для генерации цифровых сертификатов с достоверной информацией о пользователях сертификатов и для корректного управления этими сертификатами (включая своевременную публикацию сертификатов, а также списков аннулированных сертификатов на LDAP-сервере);

- операционная система зависит от смарт-карты, которая защищает личный ключ пользователя и использует его только после получения точной информации аутентификации (например, ПИН);

- смарт-карты зависят от операционной системы хоста, которая защищает ПИН пользователя с того момента времени, когда пользователь ввел его при использовании смарт-карты, и до того момента, когда ПИН был надежно удален из памяти операционной системы хоста. Смарт-карты зависят от операционной системы хоста, которая не должна злоупотреблять ПИН пользователей, например, без авторизации пользователя активировать смарт-карту.

Только этот список зависимостей будет использован для демонстрации того, что они были рассмотрены в ПЗ или ЗБ.

При анализе зависимостей можно легко определить следующее:

- база данных зависит от операционной системы, обеспечивающей ее функциональные возможности безопасности;
- операционная система зависит от аппаратных средств;
- операционная система зависит от LDAP-сервера;
- операционная система зависит от PKI;
- операционная система зависит от смарт-карт;
- смарт-карты зависят от операционной системы хоста.

В том случае, когда один компонент зависит от другого, в ISO/IEC 15408 они называются «зависимым» и «основным» компонентами. Например, в совокупности базы данных и операционной системы база данных - зависимый компонент, а операционная система - базовый компонент. Аналогично, в совокупности операционной системы и аппаратных средств, операционная система – зависимый компонент, а аппаратные средства – основной компонент. В случае смарт-карты и операционной системы оба компонента зависят друг от друга и, следовательно, они оба являются и зависимыми, и основными компонентами.

При разработке ЗБ или ПЗ для зависимого компонента, зависимость от основного компонента должна быть сформулирована как предположения, а цели безопасности для операционной среды должны быть получены из тех предположений. Например, для СУБД могут быть сформулированы следующие предположения.

Предположение 1

Операционная среда будет защищать ПО СУБД от воздействия и искажения любым другим выполняемым прикладным ПО той же СУБД.

Предположение 2

Операционная среда будет защищать файлы, используемые СУБД, чтобы сохранить данные ее пользователей и ФБО от несанкционированного доступа.

Предположение 3

Операционная среда будет идентифицировать и аутентифицировать отдельных пользователей и обеспечивать путь для СУБД для получения идентификатора пользователя, от имени которого будет выполняться запрос к СУБД.

Эти предположения могут быть использованы для весьма точного определения целей для операционной системы, как части операционной среды. Уровень детализации этих целей сильно зависит от специфических требований к СУБД. Например, если аудит является функциональным требованием безопасности для СУБД, то возможно, что будет полезно потребовать также некоторый уровень аудита для операционной системы, чтобы обнаружить попытки обхода или искажения с помощью функциональных возможностей безопасности операционной системы, от которой

зависит СУБД.

Примеры

1 Операционная система должна обеспечить механизм, который позволит СУБД действовать в ее рабочей области, защищенной от воздействия и искажения со стороны других прикладных программ, выполняемых под управлением этой операционной системы.

2 Операционная система должна защищать от несанкционированного доступа выполняемые СУБД программы.

3 Операционная система должна обеспечить механизм, который позволит обнаруживать нарушения целостности программного обеспечения СУБД и запрещать запуск СУБД, когда обнаружено нарушение целостности, которое не может быть устранено.

4 Операционная система должна обеспечить механизм управления доступом к файлам, доступ к которым подразделяется, по крайней мере, на доступ на чтение и доступ на запись/выполнение, и позволять индивидуально определять уровень доступа (включая «доступ запрещен») вплоть до степени детализации отдельного пользователя.

5 Операционная система должна позволять ограничивать управление правами доступа к файлам отдельным пользователям или определенным группам пользователей.

6 Операционная система должна идентифицировать и аутентифицировать отдельных пользователей до того, как они смогут вызвать функции СУБД.

7 Операционная система должна использовать защищенный механизм аутентификации, который ограничит вероятность ложной аутентификации пользователя до вероятности, не превышающей 1:1 000 000.

8 Операционная система должна иметь возможность аудита успешных и неудачных попыток аутентификации, причем запись аудита должна содержать предъявленный идентификатор пользователя, время и дату попытки аутентификации.

9 Операционная система должна обеспечить интерфейс, который сможет использоваться СУБД для безошибочного получения предъявленного идентификатора пользователя, с помощью которого будут вызваны функции базы данных.

Большинство целей безопасности может быть легко отображено в соответствии с функциональными требованиями безопасности, определенными в ISO/IEC 15408-2. Только первая цель безопасности отличается,

поскольку она адресована характеристике архитектуры - разделению домена. В документации на архитектуру безопасности должно быть описано, как эта характеристика реализована в операционной системе. Наличие описания архитектуры безопасности обязательно для оценочных уровней доверия, начиная с ОУД2 и выше.

В том случае, когда СУБД выступает как зависимый компонент, а операционная система как базовый компонент, можно определить цели безопасности для операционной системы с весьма высоким уровнем детализации, очень близким к уровню детализации функциональных требований безопасности. Всякий раз, когда это возможно, следует обеспечивать такой же уровень детализации.

Существуют другие ситуации, когда предположения, а также цели безопасности для операционной среды, полученные из этих предположений, должны быть более универсальны. Например, в том случае, когда операционная система является зависимым компонентом, а LDAP-сервер - базовым компонентом, тогда необходимо сделать следующее предположение:

Операционная среда должна защищать цифровые сертификаты и списки аннулирования сертификатов, необходимые операционной системе для аутентификации пользователей, от несанкционированной модификации и от несанкционированного добавления сертификатов и списков аннулирования сертификатов.

В этом случае ЗБ или ПЗ вполне может оставить некоторые детали этой защиты открытыми, позволяя удовлетворить это предположение другими способами. Из этого предположения могут быть получены следующие цели безопасности для операционной среды:

- *LDAP-сервер должен идентифицировать и аутентифицировать пользователей до получения разрешения на модификацию и/или добавление сертификатов и списков аннулированных сертификатов, используемых для аутентификации пользователей операционной системы;*

- *операционная среда должна защищать данные, передаваемые между LDAP-сервером и операционной системой, от необнаруженной модификации (включая добавление и повторное использование).*

Для этого примера не требуется определение более детального способа достижения целей безопасности для операционной среды, поскольку существует множество различных способов выполнения этих требований. В данном примере этот вопрос преднамеренно оставляют открытым, если вторая цель безопасности была достигнута путем использования протокола криптографически защищенной связи или физической защиты сети.

При разработке ЗБ или ПЗ для зависимого компонента возможно существование двух разных случаев: первый - это когда основной

компонент был оценен и результаты его оценки доступны при оценке зависимого компонента; и второй – это когда основной компонент или не был оценен, или результаты его оценки не доступны.

Для первого случая в ISO/IEC 15408-3 существует класс ACO, в котором определены критерии оценки для составных оцененных компонентов. Разработчик ЗБ или ПЗ для составного ОО должен включить компоненты класса ACO, которые он считает подходящими для соответствующего уровня доверия. Этому способствует ISO/IEC 15408-3, в котором определены три «пакета компонентов доверия», которые могут быть включены в ЗБ или ПЗ для составного ОО. Если разработчику будет необходимо выбрать компоненты класса ACO, отличающиеся от этих предварительно определенных пакетов, то он должен будет гарантировать, что зависимости были проанализированы.

14.2 Компоненты объектов оценки

Существуют ОО, которые являются самостоятельными, явно не зависимыми от других компонентов ИТ в своей среде, а также множество других ОО, для которых это не характерно. Эти ОО определяются в ЗБ или ПЗ как «компоненты ОО». Типичными примерами компонентов ОО являются:

- пакет ПО, который обеспечивает определенные функции безопасности, но предназначенный, чтобы интегрироваться со множеством других продуктов. Защита ФБО пакета ПО и данных его ФБО, а также управление некоторыми данными этих ФБО зависит от продуктов, с которыми пакет ПО интегрирован;
- приложение, которое осуществляет управление доступом на принадлежащих ему объектах, но полагается на идентификацию и аутентификацию пользователя, которую необходимо предусмотреть в среде;
- приложение или операционная система, которая зависит от криптографического сопроцессора для реализации криптографических функций и управления их ключами.

Во всех этих случаях одна или несколько целей безопасности только частично отображены в функциональных требованиях безопасности ОО и частично отображены в среде. Следовательно, ОО может быть оценен только при предположении, что в среде правильно реализованы функциональные требования безопасности, которым всецело адресована та часть целей безопасности, которую ОО не способен адресовать себе.

Следовательно, ЗБ или ПЗ для компонента незначительно отличаются от ЗБ или ПЗ для отдельного продукта. Единственное различие заключается в том, что цели безопасности для среды ИТ, которые необходимо удовлетворить, чтобы полностью адресовать целям безопасности ОО, обычно определяются весьма точно, упоминая также (где это возможно) тип продукта ИТ в среде, которая предназначена для

удовлетворения цели. В приведенном в 14.1 примере в ЗБ для операционной системы можно четко и по отдельности определить цели безопасности, которые нужно удовлетворить используя аппаратные средства, LDAP-сервер, PKI-систему и смарт-карту. Эти цели безопасности должны быть определены как можно точно, чтобы их можно было легко отобразить на функциональные требования безопасности, как определено в ЗБ этих компонентов. Это во время оценки позволит более просто отобразить совокупность таких компонентов, как составной ОО.

15 Особые случаи

15.1 Профили защиты и задания по безопасности для низкого уровня доверия

В тех случаях, когда в ПЗ или ЗБ требования доверия не выше тех, которые определены для оценочного уровня доверия ОУД1, ISO/IEC 15408 позволяет упростить ПЗ или ЗБ. Тогда в ЗБ или ПЗ можно не включать:

- ПЗБ;
- цели безопасности;
- логическое обоснование целей безопасности;
- логическое обоснование требований безопасности, за исключением обоснования неразрешенных зависимостей между требованиями безопасности.

ЗБ или ПЗ для низкого уровня доверия может потребовать соответствия только ПЗ для низкого уровня доверия, но ПЗ или ЗБ для высокого уровня доверия может потребовать соответствия ПЗ для низкого уровня доверия. ПЗ или ЗБ для высокого уровня доверия должен содержать все разделы, необходимые для ПЗ или ЗБ для высокого уровня доверия. Следовательно, разделы, не включенные в ПЗ для низкого уровня доверия, должны быть включены в ПЗ или ЗБ для высокого уровня доверия.

15.2 Пакеты функциональных требований и требований доверия к безопасности

Дополнительно к ПЗ ISO/IEC 15408 также допускает определение функциональных пакетов и пакетов требований доверия к безопасности. Функциональный пакет содержит набор функциональных требований безопасности, а пакет требований доверия к безопасности содержит набор требований доверия к безопасности. Создание смешанных пакетов, которые содержат как функциональные требования безопасности, так и требования доверия к безопасности, не допустимо.

Пакет должен иметь имя, которое позволит его идентифицировать, и должен содержать набор полезных и эффективных требований. Например, функциональный пакет может содержать функциональные требования

безопасности, указывающие только на специфический аспект безопасности. Типичным примером является функциональный пакет, определяющий функциональные возможности, связанные с аудитом (минимальный набор событий, который подлежит аудиту, защита журнала аудита, обзор требований аудита, управление аудитом) без указания каких-либо других аспектов. Такой функциональный пакет затем может быть многократно использован для других типов продуктов безопасности (например, для операционных систем, систем управления базой данных, межсетевых экранов). При определении такого функционального пакета или пакета требований доверия к безопасности будет наиболее благоразумно, чтобы адресовать зависимости либо непосредственно в пределах пакета, или предоставить рекомендации, каким образом при использовании пакета должны быть адресованы неразрешенные зависимости.

16 Использование автоматических инструментальных средств

Предпосылками использования автоматических инструментальных средств при разработке и оценке ПЗ и ЗБ являются особенности структуры ISO/IEC 15408 и фиксированное содержание ПЗ/ЗБ.

Использование инструментальных средств позволяет разработчику сконцентрироваться на содержании ПЗ/ЗБ, облегчает ему демонстрацию правильности ПЗ/ЗБ, позволяет существенно сократить временные затраты на выполнение таких задач, как разработка логического обоснования и описание взаимосвязей, проверка функциональных возможностей, а оценщикам при оценке ПЗ/ЗБ облегчает выполнение наиболее трудоёмкой и рутинной работы.

Представление ISO/IEC 15408 и «Общих критериев» в формате XML предоставляет разработчикам новые возможности в автоматизации процесса разработки ПЗ/ЗБ, поддержки и интеграции в жизненный цикл их разработки инструментальных средств. Эти новые возможности должны быть доступны разработчику соответствующего ОО.

С помощью инструментальных средств может быть легко получена большая часть содержания ПЗ/ЗБ и предъявлены требования путем копирования текста последней версии ISO/IEC 15408.

Приложение А
(справочное)

Пример определения расширенного компонента

В настоящем приложении представлен пример определения расширенного компонента функциональной безопасности, в котором сделана попытка определить требования по восстановлению данных ФБО. В этом примере также представлены структура и характеристика расширенного компонента, а также логическое обоснование для этого компонента, который предполагается определить для ЗБ и ПЗ.

Восстановление данных ФБО (FPT_REC_EXT)

Характеристика семейства

Восстановление данных ФБО позволяет определять контрольные точки для определенных данных ФБО, а позднее восстановить те данные, которые были на момент установления соответствующей контрольной точки. Это позволяет восстанавливать данные ФБО после их модификации, например, в результате ошибки администратора или после их искажения в результате сбоя какого-либо аппаратного средства или программного обеспечения.

Ранжирование компонента

FPT_REC_EXT.1 «Базовое восстановление данных ФБО» направляет запрос на установление контрольных точек и восстанавливает данные из контрольных точек, задаваемых вручную администратором.

FPT_REC_EXT.2 «Расширенное восстановление данных ФБО» направляет запрос на установление контрольных точек и восстанавливает данные из контрольных точек, задаваемых или автоматически, или вручную администратором.

Управление: FPT_REC_EXT.1, FPT_REC_EXT.2

Для функций управления из класса FMT могут рассматриваться следующие действия:

- управление привилегиями, необходимое для определения контрольной точки и/или инициирования восстановления;
- управление данными ФБО, которые содержатся в сохраненных данных контрольной точки.

Аудит FPT_REC_EXT.1, FPT_REC_EXT.2

Если в ПЗ/ЗБ включено семейство FAU_GEN «Генерация данных аудита безопасности», то следует предусмотреть возможность аудита следующих действий:

- минимальный: все операции восстановления выполнены успешно;
- базовый: все попытки выполнения операции восстановления;
- детализированный: все попытки выполнения операции восстановления, все операции контрольной точки.

FPT_REC_EXT.1 Базовое восстановление данных ФБО

Иерархический для: нет других компонентов.

Зависимости: FMT_SMR.1 «Роли безопасности», FMT_MOF.1 «Управление режимом выполнения функций безопасности».

FPT_REC_EXT.1.1 ФБО должны разрешать пользователю с ролями [назначение: список ролей] определять контрольные точки для [назначение: список данных ФБО]. ФБО должны сохранять эти данные ФБО до тех пор, пока не будет достигнута та позиция контрольной точки, с которой они впоследствии могут быть восстановлены.

FPT_REC_EXT.1.2 ФБО должны разрешать пользователю с ролями [назначение: список ролей] восстанавливать данные ФБО из значений, которые содержатся в контрольной точке.

FPT_REC_EXT.1.3 ФБО должны выполнить следующие действия, чтобы обеспечить согласованность и целостность данных ФБО после восстановления [назначение: список действий для проверок согласованности и целостности].

FPT_REC_EXT.1.4 ФБО должны выполнить следующие действия, когда будут обнаружены несогласованность между данными ФБО или нарушение целостности во время восстановления [назначение: список действий].

FPT_REC_EXT.2 Автоматическое восстановление данных ФБО

Иерархический для: FPT_REC_EXT.1.

Зависимости: FMT_SMR.1 «Роли безопасности», FMT_MOF.1 «Управление режимом выполнения функций безопасности».

FPT_REC_EXT.2.1 ФБО должны определять контрольные точки для [назначение: список данных ФБО] при следующих условиях [выбор: администратор определяет интервалы времени, когда следующие условия выполнены [назначение: список условий], [назначение: другие критерии]]. ФБО должны загружать эти данные ФБО до тех пор, пока не будет достигнута та позиция контрольной точки, с которой они впоследствии могут быть восстановлены.

FPT_REC_EXT.2.2 ФБО должны восстанавливать данные ФБО из значений, которые содержатся в контрольной точке, при следующих условиях [назначение: список условий].

FPT_REC_EXT.2.3 ФБО должны выполнить следующие действия, чтобы обеспечить согласованность и целостность данных ФБО после восстановления [назначение: список действий для проверок согласованности и целостности].

FPT_REC_EXT.2.4 ФБО должны выполнить следующие действия, когда будут обнаружены несогласованность между данными ФБО или нарушение целостности во время восстановления [назначение: список действий].

FPT_REC_EXT.2.5 ФБО должен использовать восстановленные данные ФБО только тогда, когда обеспечена их согласованность и целостность.

Логическое обоснование определения расширенного компонента

В ISO/IEC 15408-2 не определены ФТБ по восстановлению данных ФБО, сохраняемых в определенных контрольных точках. Этот вид восстановления важен для обеспечения безопасной работы ОО. Функциональное требование определяет условия, при которых значения определенных данных ФТБ «сохраняются» как часть операции «контрольная точка» и впоследствии эти значения при определенных условиях восстанавливаются из их сохраненных значений. Вполне возможно, что будет восстановлен только определенный набор данных ФБО, в результате это может привести к несогласованному (и потенциально небезопасному) состояниию ФБО. Также должна быть обеспечена целостность сохраненных данных ФБО. Следовательно, было бы хорошо потребовать выполнение проверки, чтобы обеспечить уверенность в том, что общее состояние ФБО после восстановления будет согласованным и безопасным, а восстановленные данные ФБО не были модифицированы. Вследствие этого ФТБ допускает проверки заданных согласованности и целостности, которые должны быть выполнены после восстановления и до возобновления нормальной работы ОО.

Если в процессе проверок согласованности получен неудовлетворительный результат, то ОО может разрешить выполнить автоматическую коррекцию путем ввода режима «техническое обслуживание», который позволяет администраторам выполнять вручную коррекцию или другие действия, необходимые для предотвращения небезопасного состояния ОО. FPT_REC_EXT.2 не позволяет использовать восстановленные ФБО до тех пор, пока не обеспечены их согласованность и целостность. Этот компонент функционального требования безопасности является расширенным компонентом для функциональных компонентов безопасности класса FPT, определенного в ISO/IEC 15408-2.

Приложение В
(справочное)

Сведения о соответствии государственных стандартов Узбекистана международным стандартам

Таблица В.1

Обозначение и наименование международного стандарта	Степень соответ-ствия	Обозначение и наименование государственного стандарта Узбекистана
ISO/IEC 15408-1:2009 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель	MOD	O‘z DSt ISO/IEC 15408-1:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ISO/IEC 15408-2:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности	MOD	O‘z DSt ISO/IEC 15408-2:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности
ISO/IEC 15408-3:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты	MOD	O‘z DSt ISO/IEC 15408-3:2016 Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
ISO/IEC 18045:2008 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий	IDT	O‘z DSt ISO/IEC 18045:2013 Информационная технология. Методы обеспечения безопасности. Методология оценки безопасности информационных технологий
Примечание – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: IDT - идентичная; MOD - модифицированная.		

(Новая редакция, Изм. № 1)

УДК 351.864.1 ОКС 35.040 Т 55

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