ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК ТО 19791— 2008

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Оценка безопасности автоматизированных систем

ISO/IEC TR 19791:2006
Information technology — Security techniques — Security assessment of operational systems
(IDT)

Издание официальное

БЗ 1—2009/599

Москва
Стандартинформ
2010

Предисловие

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

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФГУ «ГНИИИ ПТЗИ ФСТЭК России»), Обществом с ограниченной ответственностью «Центр безопасности информации» (ООО «ЦБИ») на основе собственного аутентичного перевода стандарта, указанного в пункте 5

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. № 525-ст.

4 ВВЕДЕН ВПЕРВЫЕ

5 Настоящий стандарт идентичен международному стандарту ИСО/МЭК/ТО 19791:2006 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем» (ISO/IEC/TR 19791:2006 «Information technology — Security techniques —Security assessment of operational systems»).

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

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

© Стандартинформ, 2010

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

Введение

Настоящий стандарт содержит дополнительные правила (процедуры) к международным стандартам ИСО/МЭК 15408-1, ИСО/МЭК 15408-2, ИСО/МЭК 15408-3 (далее — стандарты серии ИСО/МЭК 15408) в интересах оценки (оценивания) безопасности автоматизированных систем. Требования, установленные в стандартах серии ИСО/МЭК 15408, обеспечивают задание и определение функциональных возможностей безопасности продуктов и систем, входящих в состав информационных технологий. Однако стандарты серии ИСО/МЭК 15408 не рассматривают некоторые критические (важные) аспекты безопасности автоматизированной системы, которые должны быть четко специфицированы для их эффективного оценивания.

Настоящий стандарт содержит дополнительные критерии оценки и рекомендации по оценке аспектов безопасности, связанных как с информационными технологиями, так и с применением их в автоматизированных системах. Настоящий стандарт прежде всего предназначен для тех, кто связан с разработкой, интеграцией, развертыванием и управлением безопасностью автоматизированных систем, а также для организаций, оказывающих услуги по оценке, пытающихся применить требования стандартов серии ИСО/МЭК 15408 к подобным системам. Настоящий стандарт будет также необходим органам, осуществляющим оценку соответствия, ответственным за утверждение и подтверждение правильности действий организаций, оказывающих услуги по оценке. Заказчики оценки безопасности и другие стороны, заинтересованные в безопасности автоматизированных систем, будут дополнительными пользователями сведений общего характера в области безопасности информации.

Относительно определения и использования термина «система» существуют фундаментальные проблемы. В стандартах серии ИСО/МЭК 15408, целью которых является оценка продуктов информационных технологий, термин «система» используется для учета только аспектов информационных технологий конкретной системы. Определение термина «автоматизированная система», используемого в настоящем стандарте, включает в себя совокупность персонала, процедур и процессов, интегрированных с функциями и механизмами информационных технологий, применяемых совместно, чтобы установить приемлемый уровень остаточного риска в установленной среде функционирования автоматизированной системы.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Оценка безопасности автоматизированных систем

Information technology. Security techniques. Security assessment of operational systems

Дата введения — 2009 — 10— 01

1 Область применения

Настоящий стандарт содержит рекомендации и критерии оценки безопасности автоматизированных систем (далее — АС), а также обеспечивает расширение области применения стандартов серии ИСО/МЭК 15408, включая ряд критических аспектов, касающихся оценки среды эксплуатации объекта оценки и декомпозиции составных АС на домены безопасности, которые должны оцениваться отдельно.

Настоящий стандарт устанавливает:

a) определение и модель АС;

b) описание расширений концепции оценки безопасности с помощью стандартов серии ИСО/МЭК 15408, необходимых для оценки АС;

c) методологию и процесс выполнения оценки безопасности АС;

d) дополнительные критерии оценки безопасности, охватывающие те аспекты АС, которые не были охвачены критериями оценки безопасности в стандартах серии ИСО/МЭК 15408.

Настоящий стандарт дает возможность включать продукты безопасности, оцененные в соответствии с требованиями стандартов серии ИСО/МЭК 15408, в автоматизированные системы и проводить оценку как единого целого с использованием настоящего стандарта.

Настоящий стандарт ограничивается оценкой безопасности автоматизированных систем и не распространяется на другие формы оценки систем. Настоящий стандарт не определяет методы и средства идентификации, оценки и принятия эксплуатационного риска.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ИСО/МЭК 15408-1:2005 Информационная технология. Методы и средства обеспечения безопасности информации. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

ИСО/МЭК 15408-2:2005 Информационная технология. Методы и средства обеспечения безопасности информации. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

ИСО/МЭК 15408-3:2005 Информационная технология. Методы и средства обеспечения безопасности информации. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте национального органа Российской Федерации по стандартизации в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по

Издание официальное

соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный стандарт заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **компонент** (component): Поддающаяся идентификации отдельная часть (элемент) автоматизированной системы, которая реализует часть функциональных возможностей системы.

3.2 **внешняя автоматизированная система** (external operational system): Отдельная автоматизированная система, которая имеет связи с автоматизированной системой, являющейся объектом оценки.

3.3 **управленческие меры безопасности** (management controls): Меры безопасности информационной системы, направленные на менеджмент рисков и менеджмент информационной безопасности информационных систем.

Примечание — Меры безопасности — меры защиты и контрмеры.

3.4 **организационные меры безопасности** (operational controls): Меры безопасности информационной системы, которые, главным образом, реализуются и выполняются операторами, а не системами.

[НИСТ СП 800-53]

Примечание — Меры безопасности — меры защиты и контрмеры.

3.5 **автоматизированная система** (operational system): Информационная система, включая элементы, не связанные с информационной технологией, рассматриваемые с учетом условий ее эксплуатации.

3.6 **остаточный риск** (residual risk): Риск, который остается после обработки рисков.

[ИСО/МЭК 13335-1:2004]

3.7 **риск** (risk): Потенциальная возможность нанесения ущерба организации в результате реализации некоторой угрозы с использованием уязвимостей активов или группы активов организаций.

Примечание — Риск измеряется в терминах сочетания вероятности события и его последствий.

[ИСО/МЭК 13335-1:2004]

3.8 **анализ рисков** (risk analysis): Системный подход к определению величины риска.

[ИСО/МЭК 13335-1:2004]

3.9 **оценка рисков** (risk assessment): Процесс, включающий в себя идентификацию рисков, анализ рисков и оценивание рисков.

[ИСО/МЭК 13335-1:2004]

3.10 **менеджмент рисков** (risk management): Весь процесс идентификации, контроля и управления или минимизации подозрительных (неопределенных) событий, которые могут оказать негативное воздействие на ресурсы системы.

Примечание — Адаптированный термин из ИСО/МЭК 13335-1 [1]. Менеджмент рисков обычно включает в себя анализ рисков, обработку рисков, принятие рисков, распространение информации о рисках (обмен или предоставление в совместное пользование информации о рисках между лицом, принимающим решение, и другими заинтересованными лицами).

3.11 **обработка рисков** (risk treatment): Процесс выбора и реализации мер обеспечения безопасности (security controls) для изменения рисков.

Примечание — Адаптированный термин из ИСО/МЭК 13335-1 [1].

3.12 **меры обеспечения безопасности** (security controls): Управленческие, организационные и технические меры обеспечения безопасности, применяемые в информационной системе для защиты и доступности системы и ее информации.

[НИСТ СП 800-53]

Примечания

1 Данное определение распространяется также на меры обеспечения безопасности, связанные с обеспечением подотчетности, аутентичности, неотказуемости, приватности и надежности, которые иногда рассматриваются отдельно от конфиденциальности, целостности и доступности.

2 Меры безопасности — меры защиты и контрмеры.

3.13 **домен безопасности** (security domain): Часть автоматизированной системы, которая реализует одни и те же политики безопасности.

3.14 **подсистема** (subsystem): Один или более компонентов автоматизированной системы, которые допускают их выполнение отдельно от остальной системы.

3.15 **система как объект оценки** (system target of evaluation): Автоматизированная система, которая эксплуатируется в соответствии с рекомендациями по эксплуатации, включая технические и организационные меры обеспечения безопасности, и является предметом оценки.

Примечание — Организционные меры обеспечения безопасности образуют часть эксплуатационной среды. Они не оцениваются по критериям оценки в соответствии со стандартами серии ИСО/МЭК 15408.

3.16 **технические меры безопасности** (technical controls): Меры безопасности информационной системы, которые реализуются и выполняются самой информационной системой через механизмы, содержащиеся в аппаратных, программных или программно-аппаратных компонентах системы.

[НИСТ СП 800-53]

Примечание — Меры безопасности — меры защиты и контрмеры.

3.17 **верификация** (verification): Процессы оценки, используемые для подтверждения того, что меры обеспечения безопасности для автоматизированной системы реализованы корректно, и их применение является эффективным.

3.18 **уязвимость** (vulnerability): Недостатки или слабости в проекте или реализации информационной системы, включая меры обеспечения безопасности, которые могут быть преднамеренно или непреднамеренно использованы для оказания неблагоприятного воздействия на активы организации или ее функционирование.

4 Сокращения

В настоящем стандарте используют следующие сокращения:

ТОО (ETR) — технический отчет об оценке;
СМИБ (ISMS) — система менеджмента информационной безопасности;
ОФБ (OSF) — организационные функциональные требования безопасности;
СП (SP) — специальная публикация;
ПЗС (SPP) — профиль защиты системы;
ДБС (SSA) — доверие к безопасности системы;
ФБС (SSF) — функции безопасности системы;
ЗБС (SST) — задание по безопасности для автоматизированной системы;
СОО (STOE) — система как объект оценки;
ИТ (IT) — информационная технология;
ОО (TOE) — объект оценки;
ТФБ (TSF) — технические функции безопасности;
ОФБ (OSF) — функции безопасности, реализуемые организационными мерами;
ЗБ (ST) — задание по безопасности;
ПЗ (SP) — профиль защиты.

5 Методологический подход к решению проблемы безопасности

5.1 Сущность автоматизированных систем

В целях настоящего стандарта автоматизированная система определена как информационная система, включая ее аспекты, не связанные с ИТ, рассматриваемая в контексте среды ее эксплуатации.

Многие автоматизированные системы являются по своему характеру составными, состоят из совокупности подсистем, которые по своей природе являются отчасти оригинальными и уникальными, а частично построены с использованием покупных широко распространенных продуктов. Автоматизированные системы взаимодействуют с другими системами и имеют зависимости от других систем. Автоматизированная система обычно строится с использованием компонентов от разных поставщиков. Для создания автоматизированной системы эти компоненты могут быть объединены интегратором, который не выполняет каких-либо функций по разработке, а только функции конфигурирования и подключения.

Автоматизированные системы обычно:

- находятся под управлением некоторого одного логического объекта — владельца автоматизированной системы;
- создаются, исходя из специфических потребностей, для выполнения конкретного типа действий;
- часто претерпевают изменения, касающиеся технической структуры и/или организационых требований;
- состоят из значительного (даже большого) числа компонентов;
- содержат покупные компоненты, которые дают большое число возможных вариантов конфигураций;
- дают возможность владельцу автоматизированной системы сочетать технические (а именно ИТ) и нетехнические меры безопасности;
- содержат компоненты с различными уровнями и типами доверия к безопасности.

5.2 Обеспечение безопасности автоматизированных систем

Безопасные продукты вносят важный вклад в обеспечение безопасности автоматизированных систем и, несомненно, использование продуктов, оцененных в соответствии со стандартами серии ИСО/МЭК 15408, может быть предпочтительным при построении безопасной автоматизированной системы. Однако проблемы безопасности в автоматизированных системах порождаются не только из-за проблем с продуктами, а также из-за проблем в самой автоматизированной системе в реальной среде эксплуатации, таких, например, как ненадлежащее применение исправлений безопасности («заплаток»), неправильная настройка параметров управления доступом или правил фильтрации межсетевого экрана, плохая организация каталогов файлов и др. Кроме того, в случае использования сети уровень безопасности автоматизированной системы, подключенной к этой сети, может затрагивать другие автоматизированные системы, которые должны взаимодействовать с ней.

Требования настоящего стандарта базируются на трехэтапном подходе к обеспечению необходимого уровня безопасности автоматизированной системы:

a) оценивание рисков безопасности применименительно к рассматриваемой системе;

b) уменьшение рисков для противодействия или устранения рисков безопасности посредством выбора обеспечения безопасности;

c) аттестация для подтверждения того, что остаточные риски, остающиеся в системе после применения мер обеспечения безопасности, являются приемлемыми для системы, чтобы ее эксплуатировать.

Концептуально этот трехэтапный процесс показан на рисунке 1.

В настоящем стандарте рассматривается только второй этап процесса, а именно – уменьшение рисков посредством выбора, применения и оценки мер обеспечения безопасности. Для этого в нем используется подход к оценке безопасности, основанный на модели оценки безопасности для ИТ-мер обеспечения безопасности, определенной в стандартах серии ИСО/МЭК 15408, но распространенный на все типы мер обеспечения безопасности.

Способы и методы оценки рисков находятся вне области действия настоящего стандарта. Для получения большей информации по оценке рисков см. часть 3 ИСО/МЭК 13335 [1].

Примечание — ИСО/МЭК 13335-3 [2] является техническим отчетом. После опубликования международного стандарта ИСО/МЭК 27005 [5] он заменит ИСО/МЭК 13335 [1], [2], [3], [4].

Способы и модели атестациии являются прерогативой менеджмента и находятся вне области действия настоящего стандарта. Для получения большей информации об одном возможном из подходов см. [6].

Модель оценки безопасности, описанная в ИСО/МЭК 15408-1, исключает рассмотрение среды функционирования (эксплуатации), окружающей часть информационной систем, связанной с ИТ. Среда эксплуатации рассматривается (учитывается) (при оценке в соответствии со стандартами серии ИСО/МЭК 15408) в качестве предположений, но не может не приниматься во внимание для автоматизированных систем. Обычно автоматизированные системы используют меры обеспечения безопасности, не связанные с ИТ, например, организационные меры или меры физической защиты. Следовательно, существует потребность в определении путей выражения и оценки таких требований и мер обеспечения безопасности в виде расширения спецификации критериев стандартов серии ИСО/МЭК 15408. В этих целях настоящий стандарт расширяет критерии оценки безопасности стандартов серии ИСО/МЭК 15408.

В целом расширения стандартов серии ИСО/МЭК 15408 в рамках настоящего стандарта включают в себя (но не ограничиваются):

a) оценку рисков в общую методологию оценки безопасности автоматизированных систем с учетом условий их эксплуатации;

b) методологию определения внутренней структуры автоматизированных систем, в том числе подробности о внутренних и внешних интерфейсах в объеме, необходимом для понимания, каким образом взаимодействуют различные части автоматизированной системы;

c) каталог критериев доверия для выражения расширений области оценки (см. приложение А);

d) каталог функциональных критериев для выражения дополнительных мер обеспечения безопасности при эксплуатации (см. приложение В);

e) каталог критериев доверия для выражения дополнительных задач по оценке, необходимых для оценки автоматизированных систем (см. приложение С).

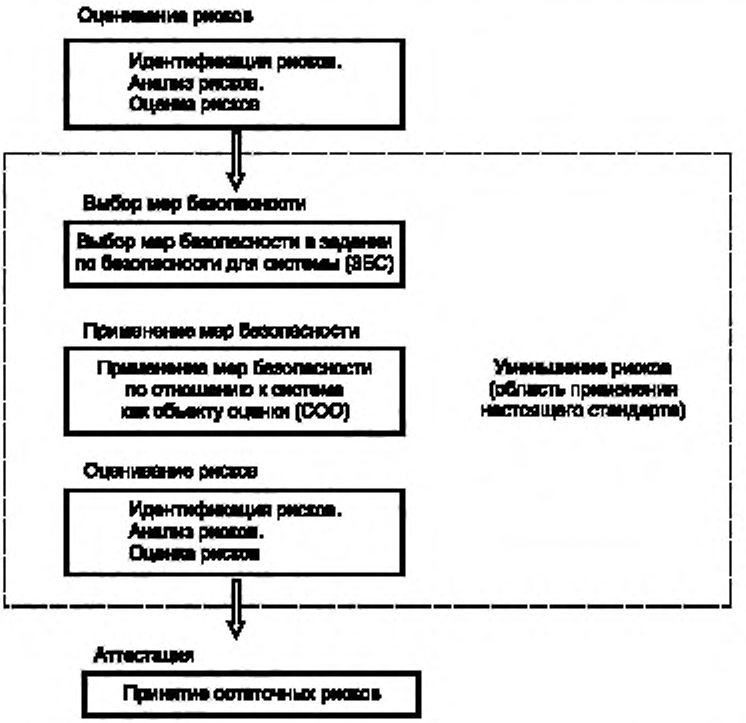

Рисунок 1 — Трехэтапный процесс обеспечения безопасности автоматизированных систем

Распространение подхода стандартов серии ИСО/МЭК 15408 к оценке законченных автоматизированных систем обладает тем преимуществом, что использование некоторого существующего показателя облегчает общее и взаимное понимание результатов оценки. Для конкретной автоматизированной системы представление результата оценки способом, соответствующим стандартам серии ИСО/МЭК 15408, может принести деловую выгоду клиентам, не только предоставляющим услуги таких систем, как банковские системы в Интернете, но и с точки зрения социальной ответственности.

При оценке автоматизированных систем требуется идентификация рисков безопасности, применимых для автоматизированной системы, во время предшествующей оценки риска и определение рисков, которые являются неприемлемыми и должны быть уменьшены или устранены посредством технических и организационных мер безопасности. Тогда оценка автоматизированных систем состоит из следующих этапов:

a) определение целей безопасности для автоматизированной системы, которые уменьшат неприемлемые риски до приемлемого уровня;

b) выбор и спецификация технических и организационных мер безопасности, которые соответствуют целям безопасности автоматизированной системы, принимая во внимание уже реализованные меры обеспечения безопасности;

c) определение конкретных измеримых требований доверия как к техническим, так и организационным мерам обеспечения безопасности для достижения необходимого уровня уверенности в том, что автоматизированная система соответствует целям безопасности;

d) фиксирование принятых решений в ЗБС;

e) оценка конкретной автоматизированной системы с тем, чтобы сделать вывод о ее соответствии ЗБС;

f) периодическая переоценка рисков безопасности автоматизированной системы, так и способности автоматизированной системы противостоять этим рискам.

Хотя эта модель является расширением модели в соответствии со стандартами серии ИСО/МЭК 15408, она совместима с этой моделью и, таким образом, результаты оценки по стандартам серии ИСО/МЭК 15408 могут быть использованы повторно.

5.3 Безопасность в жизненном цикле автоматизированных систем

5.3.1 Общие положения

Считается, что жизненный цикл автоматизированной системы состоит из следующих стадий: разработка/интеграция, установка, эксплуатация системы и модификация. Меры обеспечения безопасности автоматизированной системы должны подвергаться оценке в течение всего жизненного цикла системы.

5.3.2 Стадия разработки/интеграции

На стадии разработки/интеграции первым действием по обеспечению безопасности должна быть идентификация рисков для автоматизированной системы. Риски, считающиеся неприемлемыми, должны уменьшаться или устраняться мерами обеспечения безопасности, интегрированными в систему. Следом за оценкой риска и идентификацией рисков, которые должны быть устранены, доверенное должностное лицо организации (аттестующее лицо) должно рассмотреть предполагаемые остаточные риски, общее число имеющихся остаточных рисков и подтвердить, что они являются приемлемыми.

После этого проектируется автоматизированная система с помощью программных и аппаратных изделий, физических мер, коммерческих программ и технических мер безопасности. Проект автоматизированной системы должен быть записан в ЗБС. В ЗБС содержится описание требований по безопасности, включая риски, которым надо противодействовать, и цели безопасности, которые необходимо реализовать с помощью технических и организационных мер безопасности. Цели безопасности системы конкретизируются в перечне технических и организационных мер безопасности.

Для корректности в ЗБС необходимо обозначать цели безопасности, которые определяют риски, идентифицированные как неприемлемые. В ЗБС должны обозначаться требования по безопасности, полностью соответствующие целям безопасности без каких-либо дополнений или пропусков. В проектной документации автоматизированной системы должны быть определены конкретные контрмеры обеспечения безопасности самой автоматизированной системы, соответствующие всем требованиям безопасности, определенным в ЗБС. Этими контрмерами могут быть: функции безопасности, оборудование, процедуры или правила. Контрмеры обеспечения безопасности в системе должны адекватно контролироваться, управляться и использоваться. Контрмеры обеспечения безопасности нельзя реализовывать с какими-либо несанкционированными дополнениями, удалениями или изменениями. Реализация должна контролироваться посредством тестирования системы или проверки документации. Функционирование контрмер обеспечения безопасности должно быть адекватно описано в руководящей документации.

В целях повышения эффективности риски безопасности, идентифицированные при оценке рисков как неприемлемые, должны быть уменьшены в соответствии с выбранными требованиями по безопасности до приемлемого уровня остаточных рисков. Каждая контрмера безопасности должна эффективно функционировать совместно с другими контрмерами для удовлетворения общих требований по безопасности автоматизированной системы. Стойкость механизмов безопасности должна быть достаточной, чтобы соответствовать предполагаемому потенциалу нападения на систему. При наличии потенциала нападения может потребоваться анализ уязвимости и испытание на проникновение.

Оценщики должны быть задействованы в начале жизненного цикла системы на стадии разработки/интеграции для упрощения их ознакомления с системой и ее предполагаемой средой, получения исходных данных путем просмотра проектной документации и составления руководства по оценке и руководящей документации, которые будут использоваться как часть свидетельств доверия. В идеальном случае полное ЗБС должно оцениваться на стадии предварительной оценки для подтверждения отсутствия каких-либо несоответствий или пробелов в требованиях по безопасности и предлагаемых мерах обеспечения безопасности.

Затем создается или приобретается программное обеспечение для систем и бизнес-приложения, включая технические меры безопасности, и система интегрируется, конфигурируется и испытывается разработ-

чиком. Одновременно создается организационная структура безопасности, формируются политики, правила и процедуры безопасности, которые интегрируются в систему. Должны быть определены и внедрены соответствующие параметры конфигурации безопасности.

После тестирования интеграции автоматизированная система должна проверяться разработчиком как часть проверочных испытаний. Обычно специфические для системы меры обеспечения безопасности, такие как управлеческие меры доступом, могут проверяться разработчиком перед их развертыванием на рабочем месте. Тестирование специфических для рабочего места мер обеспечения безопасности (технических и организационных) откладывается до завершения установки системы в ее предполагаемой эксплуатационной среде. Проверочные испытания должны подтвердить стабильность механизмов безопасности, а также правильное функционирование мер обеспечения безопасности.

Затем осуществляется оценка автоматизированной системы. Оценка должна подтвердить, что все риски, детализированные в ЗБС, которым должны противодействовать меры обеспечения безопасности, определены как приемлемые для системы. Результат оценки является независимым подтверждением для владельца системы приемлемости мер обеспечения безопасности.

В отчете о сертификации указывают все подтвержденные уязвимости, обнаруженные при оценке, и, при необходимости, определяются любые рекомендованные корректирующие действия. Затем владелец системы подготавливает план корректирующих действий по уменьшению или устранению выявленных уязвимостей, если это необходимо. Результат сертификации системы представляется аттестующему лицу для определения приемлемости фактических остаточных рисков для функционирования системы и ее активов. Выходные данные на стадии сертификации будут разрешением на эксплуатацию системы.

5.3.3 Стадия установки (внедрения)

На стадии установки (внедрения) для использования в среде эксплуатации внедряют и подготавливают технические и организационные меры безопасности. Испытывают специфические для рабочего места меры обеспечения безопасности, а остальные меры обеспечения безопасности проверяют повторно для подтверждения их правильного функционирования в конкретной рабочей среде.

Для соблюдения корректности меры обеспечения безопасности должны соответствовать требованиям безопасности, документированным в ЗБС, и должны быть санкционированы для применения компетентным лицом. Для повышения эффективности мер обеспечения безопасности все задействованные в этом обеспечении лица должны быть обучены использованию мер и процедур обеспечения безопасности в среде эксплуатации.

5.3.4 Стадия эксплуатации системы

На стадии эксплуатации системы необходимо собирать и оценивать записи об эксплуатации технических и организационных мер безопасности. Журналы аудита и записи мониторинга всего доступа к активам должны регистрироваться. Необходимо подтвердить правильность функционирования мер обеспечения безопасности. Необходимо также проверять отсутствие несанкционированных операций и неприемлемых рисков. Состояния незащищенности должны быть переведены в состояния защищенности в назначенный срок. Необходимо контролировать и оценивать на наличие проблем с безопасностью изменения, внесенные в ходе регламентного обслуживания. Записи о фактическом доступе и использовании активов должны проверяться. О проблемах с безопасностью необходимо сообщать, они должны быть проверены и проанализированы.

Целью сбора и оценивания записей об эксплуатации технических и организационных мер безопасности является установление обратной связи системы с аттестующим лицом при внесении изменений, которые могут повлиять на безопасность автоматизированной системы. Обычно при эксплуатации системы необходимо определить ряд критически важных мер обеспечения безопасности автоматизированной системы с целью непрерывного мониторинга для проверки их постоянной эффективности. Кроме того, владелец системы должен иметь систему конфигурационного управления, контроля и отчетности, которая документирует текущие активы автоматизированной системы, ее конфигурацию и представляет эту информацию ответственным сторонам.

5.3.5 Стадия модификации

На стадии модификации любые предполагаемые или фактические изменения автоматизированной системы, выходящие за рамки регламентного обслуживания, должны изучаться, анализироваться, и при необходимости, тестироваться для определения их воздействия на безопасность автоматизированной системы перед внедрением в процесс эксплуатации. Эти изменения включают в себя изменения в политиках и процедурах. Для проверки эффективного функционирования модифицированных мер обеспечения безопасности необходимо проводить испытание на проникновение.

Для определения необходимости повторной оценки безопасности результаты анализа воздействия и испытаний должны представляться аттестующему лицу. Если допустить, что модификации незначительно увеличили остаточные риски (возможно, потому, что они уже были оценены как часть процесса поддержания доверия к продукту), то повторное санкционирование может осуществляться без повторной оценки. Однако если результаты оценки были признаны недействительными, может потребоваться повторная оценка.

Конечным действием по модификации системы является прекращение ее эксплуатации после выключения системы, при этом данные системы архивируются, уничтожаются или передаются другим системам. От аттестующего лица требуется подтверждение успешной остановки системы.

5.4 Взаимосвязь с другими системами

Автоматизированная система может взаимодействовать с другими родственными системами и являться частью единого целого. СОО оцененной автоматизированной системы определяется как часть группы систем, которая оценивается с включением как систем ИТ, так и среды их эксплуатации. Остальная часть группы систем считается внешними автоматизированными системами. Автоматизированная система может иметь цели безопасности, которым соответствуют внешние автоматизированные системы, но они не анализируются и не оцениваются.

6 Распространение принципов оценки безопасности автоматизированных систем, установленных в стандартах серии ИСО/МЭК 15408

6.1 Общие положения

Целью настоящего раздела является документирование основных принципов, которые подкрепляют метод оценки безопасности по стандартам серии ИСО/МЭК 15408, и последующее его распространение на автоматизированные системы. В стандартах серии ИСО/МЭК 15408 рассматриваются только технические меры безопасности и родственные им управленческие меры; в автоматизированных системах технические меры безопасности и организационные меры безопасности объединены для защиты информации и других активов организации.

6.2 Основные принципы оценки безопасности

Для многих организаций информация является главным активом и нуждается в защите от угроз несанкционированного разглашения, модификации или уничтожения. Этот актив защищен посредством объединения технических мер безопасности и вспомогательных инфраструктур организационного управления, состоящих из персонала организации, политики организации, процедур и физических мер защиты. Основная концепция стандартов серии ИСО/МЭК 15408 заключается в том, что угрозы активам организации должны быть четко сформулированы, и им должна противодействовать комбинация из инфраструктур технических и организационных мер безопасности. Требования к техническим мерам безопасности по отношению к угрозам включены в стандарты серии ИСО/МЭК 15408. В этих стандартах требования к техническим мерам безопасности рассматривались отдельно как часть процесса аттестации и, следовательно, не учитывались при оценке безопасности автоматизированной системы. В настоящем стандарте делается попытка стандартизировать эти требования с тем, чтобы их можно было оценивать как часть оценки организационных мер безопасности.

В стандартах серии ИСО/МЭК 15408 меры безопасности делятся на предоставляемые, связанные с безопасностью услуги, и меры, предпринимаемые для обеспечения уверенности в том, что эти меры обеспечения безопасности будут реализованы правильно и эффективно. При оценке продукта связанные с безопасностью услуги являются функциями ИТ, реализованными для соответствия целям этой области технологии. В контексте автоматизированных систем можно также оценить процедурное и физическое содействия обеспечению безопасности. Процедурное и физическое содействия обеспечению безопасности аналогичны выполняемым функциям ИТ, поскольку представляют собой потенциальные возможности безопасности автоматизированной системы, которые вместе отвечают целям безопасности. Однако обычно процедурное и физическое содействия обеспечению безопасности не основаны на технологии и больше соответствуют оценки эксплуатационного этапа жизненного цикла автоматизированной системы, чем этапа разработки автоматизированной системы. Поэтому считается, что они должны быть отделены от функциональных требований.

Меры, принятые для должной реализации потенциальных возможностей безопасности и состоящие из сформированного свидетельства и независимой оценки пригодности этих возможностей, в стандартах серии ИСО/МЭК 15408 обозначены термином «доверие». Его можно расширить для включения части орга-

низационных мер безопасности автоматизированной системы с помощью документации, описывающей организационные меры безопасности как реализованные.

Процесс разработки, внедрения и поддержания функционирования самой автоматизированной системы и связанных с безопасностью услуг оказывает значительное влияние на правильность и эффективность связанной с безопасностью услуги и ее общий вклад в общую безопасность автоматизированной системы. Это влияние также содействует уверенности в оказании связанной с безопасностью услуги. Таким образом, процесс разработки, внедрения и поддержания функционирования самой автоматизированной системы и связанных с безопасностью услуг способствует общему доверию к комплексной автоматизированной системе. А именно, чем выше уровень производительности процесса, тем больше уверенность в правильности и эффективности связанной с безопасностью услуги и, следовательно, общее оказываемое доверие.

Функциональные требования обеспечения организационной безопасности реализуются нетехническими средствами, внедренными в автоматизированную систему в интересах обеспечения общих целей безопасности, тогда как требования доверия к ней отражены в свидетельствах соответствия этим требованиям.

Следовательно, оценку безопасности автоматизированной системы можно разделить на несколько этапов:

a) проблема безопасности четко сформулирована как набор рисков, которые должны быть уменьшены или смягчены, и набор политик безопасности организации, которые должны быть реализованы. Для определения цели автоматизированной системы требуется предварительный анализ, а для определения рисков, которым должны противодействовать технические и организационные меры безопасности, требуется оценка рисков. Результаты анализа фиксируются в ЗБС;

b) проблема безопасности делится на высокоуровневое решение по безопасности, представленное совокупностью целей безопасности. Цели безопасности записывают в ЗБС;

c) далее цели безопасности детализируют в требованиях безопасности, которые могут быть оценены независимым оценщиком. Некоторые цели относят к техническим мерам обеспечения безопасности, некоторые — к организационным. Например, контроль за несанкционированным доступом к информационному активу часто осуществляется через обеспечение физической защиты оборудования, содержащего актив (например, замки, охрана), и выполняемые функции ИТ (например, аутентификация пользователя и механизмы управления доступом). Требования безопасности записывают в ЗБС;

d) на основе общих целей и общего доверия к требуемым мерам защиты определяется совокупность действий оценщика во время проведения оценки. Эти требования доверия записаны в ЗБС;

e) оценка независимым оценщиком определяет соответствие автоматизированной системы ее требованиям по безопасности на основе требований, документированных в ЗБС;

f) могут проводиться текущие оценки для обеспечения уверенности в соответствии автоматизированной системы установленным требованиям в ходе эксплуатации. Текущие оценки сосредоточены в основном в области организационных мер безопасности автоматизированной системы, поскольку эти меры зависят от поведения человека, которое является менее контролируемым и последовательным, чем поведение ИТ;

g) периодическая переоценка автоматизированной системы может определить, продолжает ли система соответствовать установленным требованиям, несмотря на изменения в ней или в ее среде. Периодическая переоценка состоит из выявления того, какие изменения имели место, оценки воздействия этих изменений на безопасность, обновления ЗБС, при необходимости, и определения наличия поддержки безопасности в ходе этого процесса.

Данный процесс подобен процессу оценки по стандартам серии ИСО/МЭК 15408. Типичное различие между оценкой автоматизированной системы и оценкой продукта по стандартам серии ИСО/МЭК 15408 заключается в том, что при оценке автоматизированной системы фактическая среда эксплуатации рассматривается полностью, тогда как при оценке продукта среда эксплуатации подробно не рассматривается, а описывается как предположения, которые не подтверждаются во время оценки.

Основной целью оценки автоматизированной системы является получение доверия к правильности и эффективности реализации целей безопасности автоматизированной системы. Однако оценка мер обеспечения безопасности как технических, так и организационных, никогда не сможет обеспечить абсолютного доверия к постоянному должному функционированию в любое время и при всех обстоятельствах. В результате оценки выносится положительное или отрицательное заключение. Даже в случае, если при оценке не обнаруживаются неприемлемые уязвимости, всегда будет остаточный риск того, что меры обеспечения безопасности не функционируют должным образом. Риск можно снизить добавлением дополнительных мер доверия или использованием различных мер доверия, что придает большую уверенность

в безопасности. Остаточный риск неправильного или неэффективного функционирования мер обеспечения безопасности можно выявить только посредством непрерывного мониторинга и оценки. Этот остаточный риск необходимо учитывать при принятии решения об аттестации автоматизированной системы для ее реального функционирования.

Факторы среды могут привести к различиям в средах критичности/угроз для различных компонентов автоматизированной системы. Возможно, что для некоторых частей автоматизированной системы может потребоваться большее доверие, тогда как для других частей требуется меньшее доверие. Поскольку при оценке риска можно установить различные уровни его приемлемости, автоматизированную систему можно разделить на домены безопасности с различными требованиями доверия. Оценка риска определяет приемлемость риска для различных частей автоматизированной системы и оказывает содействие при определении соответствующих мер доверия для каждой части автоматизированной системы.

6.3 Доверие к автоматизированным системам

Принцип доверия по стандартам серии ИСО/МЭК 15408 основан на предоставлении свидетельства о существовании правильной и эффективной реализации мер обеспечения безопасности. Более высокие уровни доверия предъявляют более подробные требования к содержанию и способу представления свидетельства. Кроме того, для большего доверия иногда требуется более строгий анализ свидетельства как со стороны разработчика, так и оценщика.

Оценка продукта по стандартам серии ИСО/МЭК 15408 осуществляется способом, который предполагает общую среду эксплуатации, в которой продукт можно использовать. Оценка продукта сконцентрирована на проверке возможностей обеспечения безопасности, реализованных продуктом, независимо от любой конкретной среды эксплуатации. Для обоснования заключения о правильности при оценке применяются различные детализация, конструкция и тестовая документация.

Главной целью оценки продукта является получение уверенности в том, что возможности обеспечения безопасности продукта реализуются корректно. Основу корректности определяют требования безопасности, содержащиеся в ЗБ продукта. ЗБ включает в себя определенную степень прослеживаемости проблемы безопасности, разрешаемой результирующим набором требований безопасности. Предполагается, что проблема безопасности, сформулированная в ЗБ, основана на оценке угрозы для типов сред, пригодных для ввода в действие продукта. Область оценки продукта ограничивается требованиями безопасности ИТ, определенными для продукта этой оценкой угрозы. Кроме того, оценка продукта устанавливает границы «безопасных значений» для конфигурируемых аспектов продукта под названием «оцененная конфигурация». Однако подобные конфигурации не учитывают какую-либо конкретную среду, поскольку она неизвестна на момент оценки. После завершения оценки продукта остается необходимость должным образом интегрировать оцененный продукт с другими продуктами для создания автоматизированной системы и, наконец, проверить, обеспечивает ли автоматизированная система нужные характеристики безопасности и поведение в среде, в которой она эксплуатируется, при существующей конфигурации системы.

При оценке используются одинаковые меры доверия, применяемые ко всем выполняемым функциям безопасности. Хотя технически возможно наличие различных доменов безопасности в продуктах, обычно при общих оценках продукта домены безопасности не применяются.

Свидетельства оценки и отчеты об оценке, полученные из оценки продукта, можно использовать для поддержки интеграции автоматизированной системы и проверочных действий.

В принципе, разница между характеристиками продукта ИТ и автоматизированной системы с точки зрения оценки безопасности невелика. Однако оценка автоматизированной системы может быть значительно сложнее оценки продукта по стандартам серии ИСО/МЭК 15408 по следующим причинам:

a) автоматизированная система может состоять из коммерческих продуктов и заказных разработок ИТ, объединенных в доменах безопасности. Состав каждого домена безопасности системы может основываться на нескольких факторах, таких как используемая технология, предоставленные функциональные возможности и критичность защищаемых активов;

b) автоматизированная система может содержать многочисленные примеры одного и того же продукта (например, многочисленные копии автоматизированной системы, предоставляемые одним и тем же продавцом) или различные многочисленные примеры продуктов одинакового типа (например, многочисленные межсетевые экраны, поставляемые различными продавцами);

c) автоматизированная система может иметь политики безопасности, применимые к одним доменам безопасности и не применимые к другим;

d) различные остаточные риски могут быть приемлемыми в различных доменах, тогда как продукт противостоит конкретным угрозам для конкретных типов актива без учета риска.

Основное различие между оценками продукта по стандартам серии ИСО/МЭК15408 и оценками автоматизированной системы заключается в том, что при оценке автоматизированной системы должны рас-

сматриваться все меры обеспечения безопасности, включая меры, реализованные в среде эксплуатации, которые при оценке продукта считаются предположениями. Вообще тип требований доверия для технических мер безопасности, документированных в ИСО/МЭК 15408-3, можно применить непосредственно или легко расширить для применения к организационным мерам безопасности. Например, концепция оценки проектной документации по техническим мерам безопасности становится оценкой описания способов функционирования организационных мер безопасности. Действия лиц, реализующих организационные меры безопасности, можно проверить способом, аналогичным способу проверки действия программ, реализующих технические меры безопасности.

Особым вопросом является доверие к эффективности мер обеспечения безопасности, реализующих функции безопасности системы. Доверие в данном аспекте технических мер безопасности достигается методами архитектурного проектирования, такими как разделение доменов безопасности, невмешательство и отсутствие возможности обхода мер обеспечения безопасности. Что касается организационных мер безопасности, применяются методы, аналогичные методам, используемым для достижения технических мер безопасности, такие как разделение обязанностей, проверка и мониторинг.

Областями, для которых требуются дополнительные компоненты доверия к управлению автоматизированными системами, являются:

a) общая структура безопасности и размещение компонентов в структуре;

b) конфигурация компонентов, составляющих автоматизированную систему;

c) политики, правила и процедуры менеджмента, управляющие функционированием автоматизированной системы;

d) требования и правила взаимодействия с другими доверенными и недоверенными автоматизированными системами;

e) мониторинг не связанных с ИТ мер обеспечения безопасности во время стадии эксплуатации жизненного цикла системы.

Из-за своей направленности на продукт стандарты серии ИСО/МЭК 15408 предполагают, что ОО будет разрабатываться в единой среде разработки, которая отличается от предполагаемой среды эксплуатации системы. Это предположение вряд ли является справедливым для большинства автоматизированных систем. Даже если автоматизированная система разрабатывается в отдельной среде испытаний, конечной стадией разработки является интегрирование в среду эксплуатации, в которой автоматизированная система дополнена организационными мерами безопасности. Некоторые подсистемы или компоненты, особенно коммерческие продукты, могут также разрабатываться в особых отдельных от основной среды средах разработки.

Это означает, что некоторые требования доверия к среде разработки по ИСО/МЭК15408-3 нельзя выполнить при разработке некоторых автоматизированных систем, или их применение должно быть отложено до стадии установки жизненного цикла системы. Уверенность в организационных мерах по обеспечению безопасности полностью достижима только в среде эксплуатации.

6.4 Комбинированные автоматизированные системы

Многие автоматизированные системы являются большими и сложными, обладают многочисленными функциями и сложной внутренней структурой. Часто они состоят из многих отличных друг от друга компонентов и подсистем. Каждый компонент может содержать одну функцию, предоставленную одним продуктом, один продукт с многочисленными функциями или множество функций, выполняемых с помощью изготовленного по заказу программного обеспечения и эксплуатационных процедур. Некоторые компоненты можно сгруппировать в подсистемы, способные к самостоятельному расширению. Такие подсистемы могут содержать одного клиента или сервер, состоящий из многочисленных продуктов, многочисленные серверы и/или клиенты и сети или неоднородные клиенты и/или серверы. Некоторые компоненты и подсистемы могут быть подвергнуты безопасной оценке, другие нет.

При вводе в действие новых составных автоматизированных систем у владельцев систем могут возникнуть определенные временные и стоимостные ограничения. Таким образом, процессы, осуществляющиеся во время выполнения технической части разрешения на эксплуатацию (иногда называемые сертификацией сайта или частью аттестации автоматизированной системы), должны быть адаптируемыми для фактических потребностей.

Обычно составные автоматизированные системы:

a) состоят из нескольких подсистем или компонентов с различными степенями и типами доверия;

b) имеют хорошо определенные структуры управления. Примером хорошо определенной структуры управления может быть единоличный «владелец» автоматизированной системы или определенный набор взаимоотношений во время управления различными частями автоматизированной системы;

c) созданы для конкретных потребностей конкретной операции;

d) отдельные компоненты обладают большим числом возможных вариантов конфигураций, некоторые из которых не соответствуют политикам безопасности автоматизированной системы;

e) используют владельца для использования различного соотношения технических и организационных мер безопасности в различных частях автоматизированной системы.

Для различных вышеупомянутых комбинаций политика безопасности может быть различной за исключением тех редких случаев, когда автоматизированная система выполняет одну единственную функцию. Логически все части автоматизированной системы с одним набором политик безопасности можно обозначить как домены безопасности. Декомпозиция подсистем и компонентов автоматизированной системы, управляемых одной политикой (политиками) безопасности, затем характеризуется политикой безопасности согласно соответствующим для этого домена рискам. В каждом домене безопасности можно определить функциональные требования безопасности и требования доверия к безопасности. В этом случае каждый домен безопасности будет обладать собственной политикой безопасности, определением проблем безопасности, целями безопасности, требованиями безопасности и документацией по безопасности. Однако у каждого домена безопасности могут быть собственные требования доверия, основанные на степени уверенности, необходимой в этом домене безопасности, и ее общее участие в автоматизированной системе. В задании по безопасности обозначают требования безопасности автоматизированной системы, которые являются представительной компиляцией доменов безопасности, создающих автоматизированную систему из общего контекста автоматизированной системы. Концепция домена безопасности показана на рисунке 2.

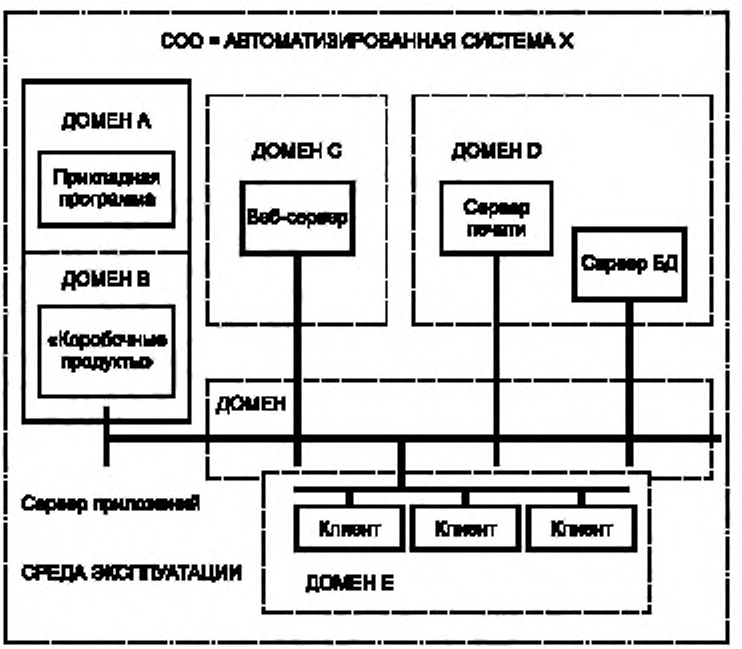

Рисунок 2 — Пример концепции доменов безопасности

При создании составной автоматизированной системы существует необходимость идентификации и описания границ системы, описания интерфейсов и зависимостей между компонентами системы и изложения интерфейсов и зависимостей между компонентами системы и ее средой (например, пользователи, внешние автоматизированные системы). Необходимо определить все интерфейсы между компонентами и между автоматизированной системой и окружающей ее средой. Спецификации интерфейса должны включать в себя любые требования безопасности для интерфейса или линий связи, реализующих интерфейс.

Кроме того, в спецификациях должны определяться любые доверительные отношения или инвариантные характеристики безопасности интерфейса.

Одним из преимуществ концепции домена безопасности является то, что концепция позволяет применять различные требования доверия к различным частям автоматизированной системы.

Рассмотрим типичную серверную систему. Серверная система состоит из различных компонентов, таких как прикладные программы, продукты промежуточного программного обеспечения и базовое программное обеспечение, такое как операционная система. Базовое и промежуточное программное обеспечение может быть предметом оценки продуктов, но может также и не оцениваться.

В отношении неоцениваемых продуктов продавец может оказать содействие в предоставлении свидетельства, необходимого для оценки, но также может отказать в предоставлении необходимого свидетельства.

Для оцененных продуктов может быть в наличии ТОО для содействия повторному использованию результатов оценки, но в доступе к ТОО может быть отказано.

Рассмотрим построение системы, приведенной на рисунке 3. В отношении домена безопасности А, который создан из собственного программного обеспечения, можно, вероятно, предоставить свидетельства, необходимые для оценки по стандартам серии ИСО/МЭК 15408. Что касается домена безопасности В, то можно получить свидетельства для удовлетворения некоторых критериев по стандартам серии ИСО/МЭК 15408 (например, классы ADO и AGD и ATE_FUN), но доступность других критериев (например, классы ADV и AVA и FNT_COV/DPT) маловероятна, поскольку необходимые свидетельства были уничтожены или вообще не существовали. Необходимо получить альтернативное доверие или принять остаточные риски.

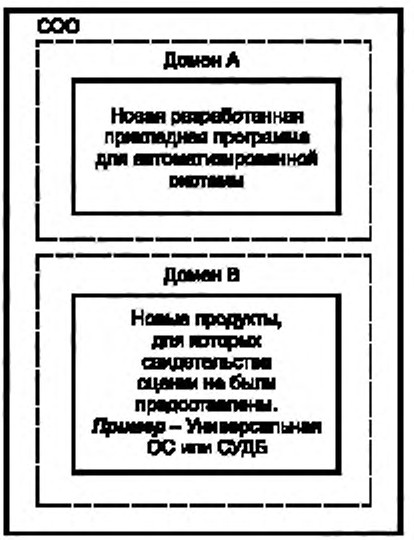

Рисунок 3 — Гетерогенное построение системы

С другой стороны, построение системы, показанное на рисунке 4, полностью составлено из компонентов, для которых можно получить свидетельство, необходимое для оценки по стандартам серии ИСО/МЭК 15408. Следовательно, можно рассматривать как отдельный домен безопасности X с однородными требованиями доверия.

Для достижения соответствия своим требованиям безопасности один домен внутри составной автоматизированной системы может зависеть от характеристик безопасности других доменов. Домен безопасности может предлагать услуги по безопасности, которые могут использоваться другими доменами через средства связи или интерфейсы прикладного программирования, или может задавать характеристики безопасности другим доменам. Это должно быть отражено в ЗБС автоматизированной системы.

Услуги по обеспечению безопасности и характеристики безопасности, заданные или ставшие доступными для других доменов, должны определяться как таковые посредством формулировки целей

безопасности для домена безопасности. Аналогично, если домен безопасности имеет цели безопасности, соответствующие другим доменам, эти цели должны определяться как таковые в формулировке целей безопасности.

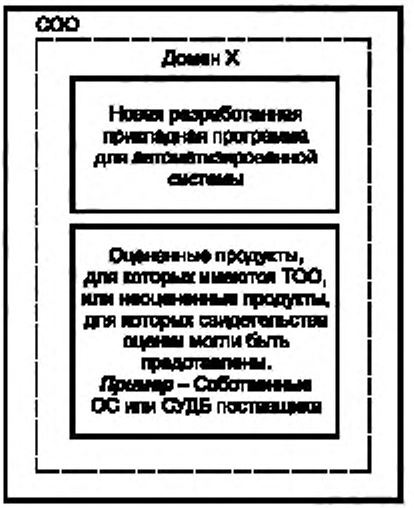

Рисунок 4 — Гомогенное построение системы

6.5 Типы мер обеспечения безопасности

В стандартах серии ИСО/МЭК 15408 в основном излагаются технические меры безопасности, т.е. меры обеспечения безопасности, осуществляемые ИТ-компонентами системы. Кроме того, необходимо определить управленческие меры и процедуры, требуемые для их реализации и мониторинга технических мер безопасности.

В автоматизированных системах также необходимо установить организационные меры безопасности. Так же, как и технические меры, они включают в себя аналогичные управленческие меры и процедуры в интересах обеспечения правильного и рационального их использования и предотвращения неправильного использования.

Поскольку большинство организационных мер безопасности зависят от действий человека, которые часто являются непредсказуемыми или воспроизводимыми, управление и мониторинг приобретают для организационных мер еще большее значение, чем для технических мер безопасности. Кроме того, имеются средства, реализуемые системой и комплексным управлением, предназначенные для обеспечения безопасного функционирования системы. Эти средства обеспечения безопасности можно категорировать как эксплуатационные (поскольку они являются частью процесса эксплуатации системы) или как самостоятельные управленческие (поскольку они относятся именно к управлению).

В настоящем стандарте используется тот же подход к управленческим мерам безопасности, что и в стандартах серии ИСО/МЭК 15408, т.е. управленческие меры являются частью технических или организационных мер безопасности, которые они поддерживают.

Пример мер обеспечения безопасности приведен на рисунке 5. В этом примере функции управления доступом, выполняемые сервером, являются технической мерой безопасности. Регистрация атрибутов пользователя является управленческой мерой безопасности, которая поддерживает функции управления доступом. Однако правила назначения ролей пользователей (например, распределение обязанностей) является организационной мерой безопасности. Процедуры управления ролями пользователей являются управленческой мерой, которая поддерживает организационную меру безопасности.

Организационные меры безопасности автоматизированных систем могут включать в себя как правила и процедуры, так и физическую защиту. Примером организационной меры безопасности, в которой затрагивается только управленческая деятельность, является отчетность об инцидентах безопасности.

Для обеспечения защиты автоматизированной системы организационые и технические меры безопасности должны интегрироваться и функционировать совместно с целью охвата всех угроз. Практически

доля участия технических мер безопасности в обеспечении безопасности системы испытывает влияние организационных мер безопасности, которые обеспечивают среду эксплуатации и зависят от них. В качестве примера, ценность «актива ИТ» системы для организации определяет тип организационных мер безопасности, таких как физическая защита, которую организация может себе позволить, а также какому персоналу организация может предоставить доступ к этому активу, и при каких условиях этот доступ поддерживается для оказания содействия непрерывности функционирования. Кроме того, для обеспечения безопасности огранизационные и технические меры допускается объединять. Например, организационные меры безопасности физического доступа к активу могут использовать технические меры безопасности в целях аутентификации, а организационные меры безопасности могут предоставлять техническим мерам информацию о физическом присутствии или отсутствии персонала на рабочем месте.

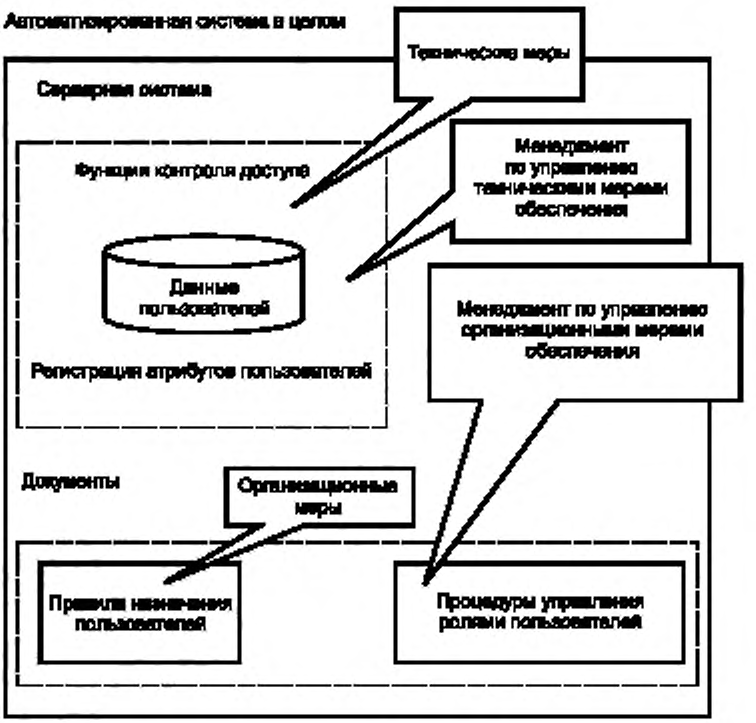

Рисунок 5 – Пример мер обеспечения безопасности

Многие технические меры безопасности автоматизированной системы можно представить непосредственно с помощью функциональных компонентов по стандартам серии ИСО/МЭК 15408. Однако вследствие сложности автоматизированной системы может потребоваться дополнительное обновление компонентов, обычно необязательное при оценке по стандартам серии ИСО/МЭК 15408.

Примеры

1 Администратору может потребоваться определить правильность конфигурации автоматизированной системы. Требованием для получения этой возможности является включение уточнения самотестирования функции технической безопасности (FPT_TST) в определение «правильное функционирование ОО».

2 Для ЗБС может потребоваться специфическое распределение функциональных возможностей безопасности конкретным компонентам в пределах доменов безопасности. Это будет означать, что потребуется уточнение для конкретных частей функций безопасности ОО, например, «Домен безопасности с межсетевым экраном должен обеспечить механизм для…».

3 Может возникнуть необходимость определения функций технических мер безопасности, касающихся возможности взаимодействия с другими системами или между различными компонентами или подсистемами автоматизированной системы.

Если для технических мер безопасности в автоматизированной системе уже имеется ЗБ, например, если меры обеспечения безопасности предоставляются коммерческим и оцененным продуктом, ЗБ может применяться как образец для формирования требований безопасности автоматизированной системы. Однако, поскольку оценка автоматизированной системы основана на рисках, угрозы и предположения ЗБ продукта и связанные с ними логические обоснования ЗБ придется оценить заново и, возможно, внести в них поправки.

Большинство организационых мер безопасности используют способы управления, процессы и процедуры эксплуатации, находящиеся за пределами области оценки по стандартам серии ИСО/МЭК 15408, и, следовательно, их нельзя выразить с помощью функциональных компонентов стандартов серии ИСО/МЭК 15408. Для оперирования этими требованиями нужны дополнительные определеные в настоящем стандарте функциональные компоненты.

6.6 Функциональные возможности обеспечения безопасности систем

Принцип функций безопасности по стандартам серии ИСО/МЭК 15408 построен на ОО, который связан только с функциями безопасности ИТ. В автоматизированной системе конкретный ОО обобщается в СОО, который включает в себя как организационные, так и технические меры безопасности.

ФБС объединяют части СОО (и, следовательно, автоматизированной системы), предназначенные для поддержания политик безопасности этой системы. В ЗБС содержатся как технические, так и организационные меры безопасности.

После определения требований безопасности владелец системы может решить, как распределить требования для удовлетворения целей технических или организационных мер безопасности или их комбинации.

Следовательно, при определении требований организационной безопасности применяют три формулировки требований. При потребности в технических мерах безопасности требование должно быть представлено следующей формулировкой «ФБО должны…». Эта формулировка используется, так как в стандартах серии ИСО/МЭК 15408 уже применяется термин «ФБО (функции безопасности ОО)» для технических мер безопасности. Если требуются организационные меры безопасности, требование должно быть представлено следующей формулировкой «ОФБ должны…», указывающее, что мера безопасности должна быть физической и основываться на использовании персонала или процедур. Если выполнение может быть осуществлено техническим или организационным путем или их комбинацией, требование должно быть представлено следующей формулировкой «ФБС должны…».

Важно отметить, что только связанные с безопасностью части СОО включены в оцененную ФБС и СОО, не надо представлять всю автоматизированную систему. Меры обеспечения безопасности системы представлены на рисунке 6.

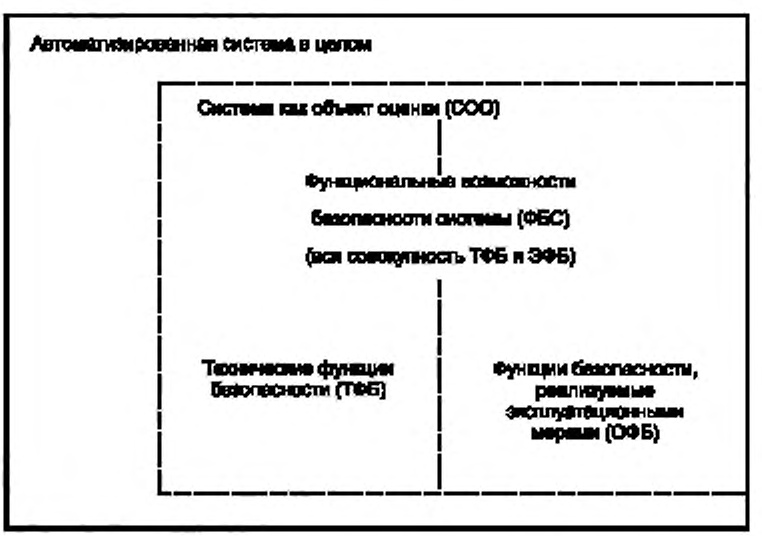

Рисунок 6 — Меры обеспечения безопасности системы

При оценке по стандартам серии ИСО/МЭК 15408 функции технической безопасности часто зависят от аспектов организационной безопасности. Примером такой зависимости является элемент управления доступом FDP_ACC по ИСО/МЭК 15408-2:

FDP_ACC.1.1 ФБО должны осуществлять [назначение: ПФБ управления доступом] для [назначение: список субъектов, объектов и операций субъектов на объектах, на которые распространяется ПФБ].

При оценке по стандартам серии ИСО/МЭК 15408 политика управления доступом и список субъектов, объектов и операций должны документироваться и только в этом случае считаются правильными. При оценке автоматизированных систем политика управления доступом и список оцениваются как часть оценки защиты данных и ролей и обязанностей персонала (см. приложение В, пункт В.4.2.4, FOA_INF.1.7; и приложение В, пункт В.2.2.4, FOD_PSN.1.19). В основном правила и процедуры функции технической безопасности, которые должны считаться правильными и применимыми для оценки по стандартам серии ИСО/МЭК 15408, оценивают как часть оценки автоматизированной системы.

6.7 Определение времени оценки

При оценке в данный момент времени определяют, соответствуют ли меры обеспечения безопасности предъявляемым им требованиям. Оценка может происходить в любое время жизненного цикла продукта или системы, но для стандартов серии ИСО/МЭК 15408 оценка продукта происходит по завершении разработки, но до начала эксплуатации продукта.

Вполне вероятно, что техническая мера безопасности, успешно испытанная в среде разработки, будет также функционировать и в среде эксплуатации. Вероятность того, что организационная мера безопасности, успешно испытанная в среде разработки, будет также функционировать и в среде эксплуатации меньше, чем в случае с технической мерой безопасности. В рабочих условиях при постоянной эксплуатации системы могут использоваться люди менее надежные, опытные, компетентные и/или мотивированные, чем во время испытаний в среде разработки. Таким образом, доверие к организационным мерам безопасности в среде разработки передается в среду эксплуатации гораздо труднее, чем доверие к техническим мерам безопасности, а, следовательно, более вероятно, что начальная оценка перейдет на стадию эксплуатации или будет проводиться на уже работающей системе.

В идеальном случае автоматизированная система должна переоцениваться (перепроверяться) после крупных изменений в характеристиках системы или рисках. Однако необходимо также периодически переоценивать автоматизированную систему для подтверждения ее эффективного соответствия своим целям и определения необходимости каких-либо корректировок с тем, чтобы оставаться в допустимых пределах риска.

В первом случае при оценке на стадии разработки предоставляется достаточно свидетельств о том, что автоматизированная система способна отвечать изменившимся целям, но мало свидетельств, что это справедливо также и для условий фактической эксплуатации. Руководству организации остается обеспечивать эффективное применение мер обеспечения безопасности. Во втором случае оценщик может подтвердить соответствие мер обеспечения безопасности предъявляемым им требованиям и их эффективное функционирование путем изучения записей об использовании этих мер.

6.8 Использование оцененных продуктов

После оценки продукта могут появиться свидетельства, которые допускаются повторно использовать при оценке автоматизированной системы. Однако подробные свидетельства могут и не быть общедоступными. В некоторых случаях их можно получить непосредственно по соглашению с разработчиком продукта или непосредственно из реестра проверенных продуктов. В других случаях невозможно получить значимые подробности, необходимые для определения, применимо ли свидетельство к функции, которое оно выполняет в автоматизированной системе, и тогда владелец системы должен определить, может ли он принять результаты оценки без доступа к свидетельствам, которые способствовали получению этих результатов.

Результаты оценки продукта необязательно применимы к оценке автоматизированной системы. Некоторыми причинами этого являются:

a) конфигурация продукта во время его оценки и при его интегрировании в автоматизированную систему могут быть различными;

b) доверие, при котором оценивался продукт, является неадекватным по сравнению с доверием, которое требуется для продукта при его интегрировании в автоматизированную систему в качестве компонента. В этом случае может существовать свидетельство, которое можно использовать повторно, помимо нового свидетельства, которое еще предстоит создать.

На этих примерах при оценке автоматизированной системы необходимо определить степень, с которой можно использовать имеющиеся результаты, и необходимые меры доверия. В худшем случае эти компоненты придется рассматривать как неоцененные.

Если оценка продукта не завершена, неизвестно, какой объем информации будет доступен для поддержки оценки автоматизированной системы, и будет ли подтверждена имеющаяся информация о продукте его оценкой. Если продукт не был оценен, информация, обычно необходимая для оценки продукта, может быть недоступна для поддержки оценки автоматизированной системы. Эти соображения надо учитывать при оценке автоматизированной системы.

Важно также наличие информации о характеристиках безопасности интерфейсов между продуктами, т.е. какие функции безопасности одного продукта зависят от функций безопасности другого продукта. При оценке системы необходимо подтвердить, что все продукты, зависящие от функций безопасности других продуктов, используют эти продукты безопасным образом. Часто необходимая информация документируется в ТОО другого продукта, но не может быть представлена как совместимая. В этом случае необходимо просмотреть другую документацию, такую как спецификации интерфейсов, и документацию проектирования архитектуры как часть оценки системы и подтвердить наличие требуемых характеристик безопасности. Подтверждение наличия требуемых характкристик безопасности справедливо и при использовании неоцененных продуктов.

Многообразие и разная степень качества оцененных имеющихся в продаже продуктов, доступных для интегрирования в автоматизированную систему, ограничивают максимальное доверие, которого можно достичь только при использовании оцененных продуктов. Вообще нецелесообразно оценивать заново оцененные продукты при более высоком уровне доверия, поскольку отсутствие дополнительных свидетельств и поддержки разработчика очевидно. Необходимо также получить дополнительное доверие посредством альтернативных мер обеспечения безопасности или архитектурных мер, например, добавлением межсетевых экранов или других специфических для обеспечения безопасности компонентов архитектуры.

В качестве альтернативы при оценке автоматизированной системы существует возможность распределения различных уровней доверия по различным доменам безопасности автоматизированной системы. Там, где доверие к определенному домену ограничено использованием оцененных продуктов, аккредитующее лицо может попросить принять побочный повышенный остаточный риск для этого единственного домена безопасности.

6.9 Требования к документации

При оценке продукта по стандартам серии ИСО/МЭК 15408 большинство требований к документации используется оценщиками для подтверждения правильности опытно-конструкторских работ и обеспечения пользователей необходимой информацией с целью конфигурирования и безопасной эксплуатации ОО.

В случае с автоматизированной системой необходимо предоставлять информацию, определяющую организационные меры безопасности с тем, чтобы:

a) оценщики могли подтвердить, что организационные меры при правильном их применении соответствуют поставленным целям безопасности;

b) можно было провести на стадии эксплуатации жизненного цикла системы проверки выполнения соответствующих процедур и эффективности процедурных и физических мер безопасности.

Необходимо также представлять информацию, относящуюся к характеристикам безопасности интерфейсов между различными компонентами автоматизированной системы и между компонентами автоматизированной системы и другими системами в окружающей ее среде так, чтобы в случае зависимости какого-либо компонента от характеристик безопасности другого компонента или системы оценщики могли бы подтверждать, что эти характеристики являются действительными в соответствии со спецификацией этого компонента или системы.

6.10 Действия по тестированию

Требования к действиям по тестированию, выполняемым как часть оценки автоматизированной системы, отсутствуют в оценке продукта по стандартам серии ИСО/МЭК 15408.

При тестировании автоматизированной системы оценивают эффективность функций технических и организационных мер безопасности, противодействущих известным неприемлемым рискам и обеспечивающих реализацию определенных политик безопасности. Эффективность функций технических и организационных мер безопасности определяется частично по выполняемым функциям безопасности автоматизированной системы и частично при проведении испытания на проникновение. Проведение тестирования имеет смысл только после размещения автоматизированной системы в проверенной безопасной конфигурации. Существуют два типа конфигурации продуктов: конфигурация продуктов для взаимодействия в качестве компонентов автоматизированной системы и конфигурация продуктов для обеспечения режима безопасности, необходимого для повседневных операций, связанных с деловой деятельностью или задача-

ми, выполняемыми автоматизированной системой. Технические меры безопасности автоматизированной системы могут и должны быть протестированы до ввода в действие системы ее разработчиком/интегратором. Тестирование обеспечивает уверенность в правильности работы функций технических мер безопасности и их эффективном противодействии риску на уровне, определенном оценкой риска. Тестирование также должно выявлять любые непреднамеренные дефекты и обеспечивать разработчику возможность устранения этих дефектов до проведения оценки. Затем организационные меры безопасности интегрируют с техническими мерами безопасности на рабочем месте, на котором можно оценить эффективность интегрированных мер безопасности автоматизированной системы.

Поскольку организационное тестирование не является частью оценки продукта, и для оценки продукта по стандартам серии ИСО/МЭК 15408 не требуется конфигурация продукта для осуществления конкретного набора «реальных» организационных политик, все продукты надо специально тестировать в своей конфигурации автоматизированной системы как часть тестирования общей автоматизированной системы.

Случается также, что продукты или подсистемы внутри автоматизированной системы должным образом не взаимодействуют, то есть при общем тестировании автоматизированной системы необходимо изучить и подтвердить надежное взаимодействие различных компонентов и подсистем.

Внутренняя стратегия испытаний также может отличаться для различных доменов безопасности, входящих в автоматизированную систему, в зависимости от таких характеристик, как:

a) уровень доверия, требуемый для подсистемы;

b) уровень доверия, уже установленный (или не установленный) для продуктов, составляющих подсистему;

c) выбранная архитектура и продукты, составляющие архитектуру;

d) используемая технология;

e) размещение компонентов в физической среде.

6.11 Управление конфигурацией

Для оценки автоматизированной системы предъявляются требования к конфигурационному управлению, которые обычно отсутствуют для оценки продуктов по стандартам серии ИСО/МЭК 15408.

В стандартах серии ИСО/МЭК 15408 жизненный цикл продуктов ИТ рассматривается с точки зрения разработчика. Жизненный цикл продуктов ИТ начинается с требований к продукту, а затем получает свое развитие на стадиях проектирования, разработки, оценки и производства. В жизненном цикле вопросы эксплуатации рассматриваются только с точки зрения их воздействия на следующую версию продукта. По этой причине конфигурационное управление рассматривается, главным образом, как мера доверия для того, чтобы оценщик мог быть уверен в правильности версии оцениваемого ЗБ и в знании разработчика того, что должно быть включено в оцениваемый ОО, предназначенный для распространения. Процесс конфигурационного управления является не частью ЗБ, а инструментом создания ЗБ.

В случае автоматизированных систем важно знать не только то, что в системе используются правильные компоненты, но и, что конфигурация автоматизированных систем остается известной и понятной во время их эксплуатации. Следовательно, могут существовать две различные системы конфигурационного управления: одна — для среды разработки, в которой создается автоматизированная система, и другая — для среды эксплуатации, в которой она функционирует. Первая рассматривается как доверие к оценке, вторая — характеристика организационных мер безопасности.

Организационная система конфигурационного управления существует, главным образом, для того, чтобы администраторы автоматизированных систем и руководители службы безопасности могли установить, что автоматизированная система продолжает работать в безопасной конфигурации, а также знать о воздействии обновлений, удалении и включениях компонентов автоматизированных систем. Следовательно, автоматизированная система должна иметь возможность (посредством процедурных или технологических мер) управлять конфигурацией и сообщать о текущей конфигурации. Для сравнения фактической конфигурации автоматизированной системы с ее предполагаемой конфигурацией с целью упрощения проверки правильности конфигурирования мер обеспечения безопасности системы и отсутствия изменений в этих мерах, внесенных во время обслуживания и должным образом не документированных, может использоваться возможность отчетности. Отчетность также служит поддержкой доверия к анализу воздействия любого изменения как результат непрерывного мониторинга. Таким образом, конфигурационное управление становится возможностью обеспечения безопасности автоматизированной системы. Конфигурационное управление может использоваться для предоставления свидетельства доверия к правильности и эффективности применения организационных мер безопасности.

7 Взаимосвязь с существующими стандартами безопасности

7.1 Общие положения

Настоящий стандарт дополняет стандарты серии ИСО/МЭК 15408 с целью проведения оценки автоматизированных систем. В соответствии с ранее изложенным для оценки автоматизированных систем требуется расширение модели оценки по стандартам серии ИСО/МЭК 15408 и определение дополнительных критериев оценки.

Большей частью, дополнительные процессы, документация и задания, требуемые для оценки автоматизированных систем, были определены расширением аналогичных концепций в соответствии со стандартами серии ИСО/МЭК 15408. Дополнительные критерии оценки касаются в первую очередь аспектов эксплуатационной интеграции и интеграции системы информационной безопасности и взяты из действующих стандартов по информационной безопасности, не связанных с оценкой. В частности, настоящий стандарт содержит значительные заимствования из двух стандартов безопасности ИСО/МЭК 17799 [8] и НИСТ СП 800-53 [9]. Принимая во внимание наличие и широкое признание этих стандартов, было принято решение считать разработку новых критериев и их структур нецелесообразным.

Взаимосвязь между средой эксплуатации и критериями оценки показана на рисунке 7. Модель политики безопасности системы, оценка риска, анализ уязвимостей, процедуры, руководства и проектная документация разработки – взяты из стандартов серии ИСО/МЭК 15408 и образуют часть документации, предназначенной для оценки системы. Критерии оценки среды эксплуатации и, в частности, организационных мер безопасности были взяты из не относящихся к оценке стандартов и руководств.

Рисунок 7 — Взаимосвязь между средой эксплуатации и критериями оценки

Наряду с ИСО/МЭК 17799 [8] и НИСТ СП 800-53 [9] существует группа других стандартов ПК 27, например, ИСО/МЭК 13335 [1], [2], [3], [4] и ИСО/МЭК 21827 [10], применяемых в качестве источников. Стандарты серии ИСО/МЭК/ТО 15443 [7] предлагают альтернативные потенциальные подходы в отношении

требований доверия. В ИСО/МЭК/ТО 15446 [11] предлагаются руководства по разработке профилей защиты и заданий по безопасности.

Другие относящиеся к данной предметной области документы включают в себя Руководство по оценке средств обеспечения безопасности в федеральных информационных системах [12] и Руководство по защите базы ИТ Германии [13].

По возможности, концепции и специфические меры обеспечения безопасности были заимствованы из указанных документов. Однако критерии оценки не предназначены для определения путей безопасного проектирования и управления автоматизированной системой. Назначением критериев оценки является определение путей оценки защищенных автоматизированных систем с помощью свидетельств, представленных оценщикам владельцами систем, разработчиками, интеграторами, операторами и администраторами автоматизированной системы. Таким образом, критерии оценки охватывают различные аспекты и отличаются от исходного материала этих релевантных документов.

Поскольку процессы, документы и задачи, определенные в данном стандарте, основаны на имеющихся процессах, документах и задачах стандартов серии ИСО/МЭК 15408, заимствования из других релевантных документов были реструктурированы в формат, который является расширением материалов, уже использованных в ИСО/МЭК 15408.

7.2 Взаимосвязь со стандартами серии ИСО/МЭК 15408

В качестве основы и структуры для оценки автоматизированных систем использовались стандарты серии ИСО/МЭК 15408. Они обеспечивают средства определения требований для технических мер безопасности. Например, в стандартах данной серии содержатся критерии детализации политик управления доступом. Стандарты серии ИСО/МЭК 15408 не предоставляют средства определения организационных мер обеспечения безопасности, но такие меры обеспечения безопасности можно получить из структуры, подобной структуре стандартов серии ИСО/МЭК 15408. Схожесть структур настоящего стандарта и стандаров серии ИСО/МЭК 15408 позволяет провести оценку автоматизированной системы с помощью критериев доверия, подобных тем, которые применяются в стандартах серии ИСО/МЭК 15408 и проверяются в ходе оценки.

В ИСО/МЭК 15408-1 определяются концепции заданий по безопасности и профилей защиты. Эти структуры детализации требований служат основой для расширенных заданий и профилей, профилей защиты системы (ПЗС) и заданий по безопасности системы (ЗБС), которые также охватывают область организационных мер безопасности.

В ИСО/МЭК 15408-2 определяются критерии оценки функциональных требований. Эти критерии применяют непосредственно к техническим мерам обеспечения безопасности, требуемым для автоматизированных систем, и как основу для определения новых дополнительных классов, семейств и компонентов, сосредоточенных на организационных мерах безопасности автоматизированной системы в пределах требований настоящего стандарта. Настоящий стандарт также включает в себя аспект «конфигурирование» функций и механизмов внутри автоматизированной системы и требования для политик и процедур, которые должны быть реализованы в среде эксплуатации организационными мерами безопасности.

В ИСО/МЭК 15408-3 определяются критерии оценки требований доверия. Эти критерии доверия используют в качестве основы для новых классов доверия, семейств и компонентов, сосредоточенных на действиях, которые должны выполняться для оценки аспектов мер обеспечения безопасности автоматизированной системы как единой интегрированной единицы. Оценка аспектов мер обеспечения безопасности автоматизированной системы как единой интегрированной единицы включает в себя требования к свидетельствам политик и процедур, которые будут реализовываться организационными мерами безопасности в среде эксплуатации.

7.3 Взаимосвязь со стандартами, не связанными с оценкой

Стандарт ИСО/МЭК 17799 [8] является Сводом правил, рекомендующим методы и средства обеспечения безопасности, которые должны рассматриваться организацией для управления безопасностью информационных активов. В стандарте содержатся рекомендации по менеджменту информационной безопасности для инициирования, осуществления и поддержания информационной безопасности.

ИСО/МЭК 17799 [8] предоставляет принятую повсеместно организационную структуру безопасности для руководства. В качестве основного источника идентификации и обозначения аспектов организационной безопасности там, где требуются меры обеспечения безопасности и формулирования конкретных требований организационного управления, принималась редакция 2005 г.

В НИСТ СП 800-53 [9] представлены руководства по выбору и обозначению мер обеспечения безопасности информационных систем, предназначенных для использования в федеральных системах правительства США. Применение этих руководств рекомендуется системам управления штатами и

местным самоуправлениям, а также организациям частного сектора, составляющим критически важную инфраструктуру США. Предполагается их замена федеральным стандартом по обработке информации США, FIPS Publication 200. Меры минимальной безопасности федеральных информационных систем. НИСТ СП 800-53 [9] использует не только определение мер обеспечения безопасности по ИСО/МЭК 17799 [8], но также охватывает другие области, не связанные непосредственно с менеджментом информационной безопасности.

Следовательно, НИСТ СП 800-53 [9] использовался как второй основной источник для организационных мер безопасности, особенно в областях организационной безопасности, которые находятся вне области применения ИСО/МЭК 17799 [8].

В стандартах серии ИСО/МЭК 13335 [1], [2], [3], [4] также используются требования к мерам обеспечения безопасности. Однако в них меры обеспечения безопасности задействованы на слишком высоком уровне, чтобы применяться в качестве источника конкретных требований к организационным мерам безопасности.

7.4 Взаимосвязь с разработкой Общих критериев

Общие критерии являются стандартом, в техническом отношении идентичным стандартам серии ИСО/МЭК 15408, опубликованным Советом по разработке Общих критериев, ассоциации национальных проектов по оценке и сертификации. Версия 2.3 Общих критериев является эквивалентом ИСО/МЭК 15408:2005, который послужил основой для разработки настоящего стандарта.

В данное время Совет по разработке Общих критериев разрабатывает новую версию Общих критериев под названием «Версия 3». Став установившейся, эта версия, по-видимому, будет использоваться в качестве основы для будущего пересмотра стандартов серии ИСО/МЭК 15408. Самым последним проектом на момент подготовки настоящего стандарта была Версия 3.0 [14]. Данная версия была издана только для комментариев, т.е., в качестве рабочего проекта ИСО/МЭК.

Хотя Версия 3.0 [14] предназначена только для комментариев, она включает в себя существенные разработки технологии оценки, основанные на практическом применении Общих критериев и стандартов серии ИСО/МЭК 15408. Таким образом, значительные изменения, внесенные в эту новую версию Общих критериев, и оценка их потенциального влияния на требования настоящего стандарта рассматриваются в приложении D.

8 Оценка автоматизированных систем

8.1 Введение

Автоматизированные системы должны оцениваться с использованием общей модели оценки, определенной в ИСО/МЭК 15408-1, с расширениями (дополнениями), определенными в настоящем разделе.

8.2 Роли оценки и обязанности

Существуют виды деятельности, необходимые для оценки автоматизированной системы. Ими являются:

- разработка свидетельств оценки (включающих в себя оценку рисков, спецификацию ЗБС, свидетельства разработки и интеграции, эксплуатации, модификации);
- оценка (включая сертификацию результатов оценки);
- аттестация.

Для каждого из перечисленных видов деятельности должен быть назначен соответствующий персонал, его полномочия должны быть согласованы и необходимые задачи должны быть выполнены. Эти виды деятельности и связанные с ними роли и обязанности персонала представлены в таблице 1. Действия, необходимые в соответствии с требованиями настоящего стандарта, должны легко сопоставляться с ролями и обязанностями, определенными в данной таблице. Все действия следует также сопоставлять с разделами СЗБ, идентифицированными в таблице 1.

Таблица 1 — Роли и обязанности по оценке автоматизированных систем

Вид деятельности	Роль	Обязанность	Разделы ЗБС
Разработка свидетельств для оценки	Высший менеджмент	Общая ответственность за безопасность. Определяет приемлемые риски. Санкционирует действия уполномоченных должностных лиц	Не определено

Окончание таблицы 1

Вид деятельности	Роль	Обязанность	Разделы ЗБС
Разработка свидетельств для оценки	Уполномоченные должностные лица организации	Оценивают и принимают остаточные риски	Определение проблемы безопасности
	Агентство безопасности	Устанавливает политики безопасности всей организации	
	Владелец системы	Проводит оценку рисков. Определяет проблемы безопасности, которые должны быть учтены в системе (включая цели, требования). Подготавливает любой ПЗС (возможно, как представитель консорциума владельцев аналогичных систем). Санкционирует переоценку, связанную с изменениями в системе или ее среде. Анализирует состояние системы на основе отчетов о непрерывном мониторинге	Определение проблемы безопасности. Цели безопасности. Требования безопасности. Описание СОО
	Разработчик/интегратор/проектировщик системы	Разработка или поддержка разработки ЗБС на основе проблемы безопасности, определенной владельцем системы. Разработка свидетельств разработки. Содействие (помощь) владельцу системы в уменьшении или устранении уязвимостей, выявленных во время оценки	Описание СОО. Технические меры безопасности. Требования доверия, относящиеся к разработке. Архитектура и краткая спецификация
	Оператор/администратор/ответственный за сопровождение	Поддержка разработки СЗБ. Разработка эксплуатационных свидетельств. Содействие (помощь) владельцу системы в уменьшении или устранении уязвимостей, выявленных в процессе оценки	Организационные меры. Требования доверия, относящиеся к эксплуатации. Архитектура и краткая спецификация
Оценка	Оценщик/лицо, осуществляющее сертификацию (сертификатор)	Оценивает систему на основе требований безопасности, сформулированных в СЗБ, чтобы сделать заключение о способности системы удовлетворять требованиям безопасности в данный момент времени. Обеспечивает независимую оценку безопасного функционирования системы на этапе ее эксплуатации. Выполняет переоценку, которая требуется, для поддержки изменений системы и ее среды. Сертифицирует результаты оценки. Предоставляет отчет об оценке и отчет о сертификации владельцу системы с рекомендациями, которые требуются для поддержки аттестации /авторизации системы	Все
Аттестация	Аттестующий	Авторизует систему для использования или подтверждает приемлемость прогнозирования остаточных рисков перед уполномоченным должностным лицом	Определение проблемы безопасности

8.3 Оценка риска и определение неприемлемых рисков

Перед оценкой автоматизированной системы владелец системы должен оценить границы автоматизированной системы, определить активы, требующие защиты, и вместе с уполномоченным должностным лицом или должностным лицом из числа высшего менеджмента определить уровень риска, который организация готова принять, когда некоторый актив может быть потерян, испорчен или скомпрометирован.

Затем владелец системы должен провести оценку рисков, охватывающую все активы автоматизированной системы. При этой оценке должны идентифицироваться все возможные риски этой системы, включая риски, которым противостоят реализованные меры обеспечения безопасности или которые устраняются ими. Эти реализованные меры обеспечения безопасности должны документироваться как часть оценки риска, чтобы их можно было включить в описание целей безопасности в ЗБС.

Примечание — В настоящем стандарте не предписывается какая-либо определенная модель или форма оценки риска. Дальнейшую информацию относительно риска для систем информационных и телекоммуникационных технологий можно найти в ИСО/МЭК 13335-1[1].

При наличии рисков, превышающих уровень, который организация готова допустить, владелец системы должен определить предполагаемое направление действий по уменьшению рисков до приемлемого уровня. Предполагаемое направление действий по уменьшению рисков может принять форму:

- принятия риска;
- принятие повышенного риска и осознание ответственности за последствия, если риск будет реализован;
- переноса рисков; перенос рисков или ответственности за их последствия на другую сторону;
- избежания риска; отказ от деятельности, которая приводит к риску;
- уменьшения или устранения рисков; уменьшение рисков до приемлемого уровня путем применения в рамках автоматизированной системы оцененных контрмер для уменьшения вероятности и/или последствий риска.

После этого анализа необходимо категорировать каждый риск как «приемлемый» или «неприемлемый» по отношению к автоматизированной системе. Приемлемые риски должны быть допустимыми, принятыми, перенесенными или рисками, которых избежали. Неприемлемыми рисками являются те, которые должны быть снижены или устранены.

При неприемлемости рисков владелец системы вместе с разработчиком системы должен идентифицировать и специфицировать технические меры и организационные меры безопасности, которые должны быть применены в качестве контрмер. Владелец системы совместно с ее разработчиком должны также определить и обозначить меры доверия для подтверждения того, что риск неспособности технических и организационных мер безопасности выполнять их цели безопасности в качестве мер противодействия снижен до допустимого для организации уровня.

Как часть стадии эксплуатации жизненного цикла системы владелец системы должен периодически повторять оценку рисков, чтобы определить:

- имеются ли изменения в бизнес-активах;
- имеются ли новые риски или изменения в рисках для активов;
- остаются ли надлежащими реализованные контрмеры.

Затем владелец должен определить, имеется ли необходимость в переоценке системы для подтверждения адекватности и эффективности мер обеспечения безопасности АС с учетом повторной оценки рисков.

8.4 Определение проблемы безопасности

Владелец системы должен определить проблему безопасности, стоящую перед автоматизированной системой, подвергающейся оценке. Описание проблемы безопасности должно включать в себя:

- результаты оценки риска;
- политики безопасности организации, применимые к системе.

8.5 Цели безопасности

Владелец системы должен подготовить формулировки целей безопасности для автоматизированной системы. Цели безопасности должны содержать четкую формулировку предполагаемого реагирования на проблемы безопасности, стоящие перед автоматизированной системой.

В целях оценки автоматизированных систем необходимо различать два типа целей безопасности:

а) функциональные цели безопасности, которые достигаются техническими и организационными мерами безопасности, используемыми в автоматизированной системе;

b) цели доверия к безопасности, которые достигаются мерами доверия (например, деятельностью по верификации).

При оценке по стандартам серии ИСО/МЭК 15408 функциональные цели безопасности обычно достигаются исключительно техническими мерами безопасности, поскольку среда эксплуатации не оценивается, а рассматривается в рамках определения проблемы безопасности в качестве предположений. В целях оценки автоматизированных систем среда эксплуатации включена в область оценки, и функциональные цели безопасности могут быть реализованы техническими, организационными мерами безопасности или сочетанием этих мер. Как технические, так и организационные меры могут повлечь за собой меры или действия по управлению.

Формулировка целей безопасности должна покрывать все требуемые меры обеспечения безопасности, включая как уже реализованные, так и те, которые необходимо применить как часть реализации автоматизированной системы.

При оценке по стандартам ИСО/МЭК 15408 требования доверия обычно не следуют из проблемы безопасности. Они выбираются аксиоматически или путем принятия «политического» решения. В рамках автоматизированной системы для различных компонентов или подсистем могут потребоваться различные формы мер доверия в зависимости от различных типов доступной информации, а также разработки или формы доверия могут также зависеть от типов выбранных функциональных мер (организационные меры могут быть наилучшим образом обеспечены различными техническими мерами). Исходя из вышесказанного, следует, что цели доверия должны рассматриваться как часть решения проблемы безопасности.

8.6 Требования безопасности

8.6.1 Введение

Владелец системы должен подготовить набор требований безопасности для автоматизированной системы. Требования безопасности должны определить набор мер обеспечения безопасности, которые должны быть реализованы в автоматизированной системе (функциональные требования безопасности), и способы оценки того, что эти меры реализованы корректно и эффективно (требования доверия к безопасности).

8.6.2 Функциональные требования безопасности

Технические меры безопасности должны выбираться из функциональных классов, определенных в ИСО/МЭК 15408-2. Если в ИСО/МЭК 15408-2 нет подходящих функциональных компонентов, тогда в соответствии с процедурой, определенной в ИСО/МЭК 15408-1, в приложении В, должны быть самостоятельно разработаны и определены дополнительные компоненты.

Организационные меры безопасности должны выбираться из функциональных классов, в соответствии с приложением В. Если в приложении В нет подходящих функциональных компонентов, тогда в соответствии с процедурой, определенной в ИСО/МЭК 15408-1, в приложении В, должны быть самостоятельно разработаны и определены дополнительные компоненты.

Сравнение функциональных классов, определенных в стандартах серии ИСО/МЭК 15408 и настоящем стандарте, а также их применимость при оценке автоматизированных систем приведены в таблице 2.

Таблица 2 — Сравнение функциональных классов

Стандарты серии ИСО/МЭК 15408	Автоматизированная система: ИСО/МЭК ТО 19791	Применимость и область применения
Аудит безопасности (FAU)	Аудит безопасности (FAU)	Применимо
Связь (FCO)	Связь (FCO)	
Криптография (FCS)	Криптография (FCS)	
Защита данных пользователя (FDP)	Защита данных пользователя (FDP)	
Идентификация и аутентификация (FIA)	Идентификация и аутентификация (FIA)	
Управление безопасностью (FMT)	Управление безопасностью (FMT)	
Приватность (FPR)	Приватность (FPR)	

Окончание таблицы 2

Стандарты серии ИСО/МЭК 15408	Автоматизированная система: ИСО/МЭК ТО 19791	Применимость и область применения
Защита ФБО (FPT)	Защита ФБО (FPT)	Применимо
Доступ к ОО (FTA)	Доступ к ОО (FTA)	
Доверенный маршрут/канал (FTP)	Доверенный маршрут/канал (FTP)	
Аудит безопасности (FAU)	Аудит безопасности (FAU)	
—	Организационные меры безопасности (FOD)	Политика, персонал, менеджмент рисков, менеджмент инцидентов, организация безопасности, соглашение об услугах
—	Меры обеспечения безопасности систем ИТ (FOS)	Политика, конфигурация, сетевая безопасность, мониторинг, управление персоналом, активы автоматизированных систем, регистрация и запись
—	Меры обеспечения безопасности активов пользователей (FOA)	Защита приватности данных, активы пользователей
—	Меры обеспечения безопасности бизнес-процессов (FOB)	Политика, непрерывность
—	Меры обеспечения безопасности аппаратуры и оборудования (FOP)	Мобильное оборудование, съемное оборудование, удаленное оборудование, система, аппаратура
—	Меры обеспечения безопасности по отношению к третьей стороне (FOT)	Управление
—	Управление (FOM)	Параметры безопасности, классификация активов, обязанности персонала, организация безопасности, отчеты о безопасности

8.6.3 Требования доверия к безопасности

Требования доверия должны выбираться в соответствии с ИСО/МЭК 15408-3 и приложением С настоящего стандарта. Если в ИСО/МЭК 15408-3 и приложении С настоящего стандарта нет подходящих компонентов доверия, то в соответствии с процедурой, определенной в ИСО/МЭК 15408-1, приложение В, должны быть самостоятельно разработаны и определены дополнительные компоненты.

Сравнение классов доверия, определенных в стандартах серии ИСО/МЭК 15408 и настоящем стандарте, а также их применимость при оценке автоматизированных систем приведено в таблице 3.

Таблица 3 — Сравнение классов доверия

Стандарты серии ИСО/МЭК 15408	Автоматизированная система. ИСО/МЭК ТО 19791	Применимость
APE: оценка профиля защиты	Оценка профиля защиты для системы (ASP)	Зависит от отличий ПЗС
ASE: оценка задания по безопасности	Оценка задания по безопасности для системы (ASS)	Зависит от отличий ЗБС

Окончание таблицы 3

Стандарты серии ИСО/МЭК 15408	Автоматизированная система: ИСО/МЭК ТО 19791	Применимость
ACM: управление конфигурацией	Управление конфигурацией автоматизированных систем (AOC)	Композиционные требования для составных продуктов. Управление конфигурацией (изменение, отслеживание, сопровождение). Подтверждение и верификация (во время эксплуатации)
ADO: поставка и эксплуатация	Безопасная установка системы (ASI)	Информирование и связь ФБС. Подтверждение и верификация (во время эксплуатации)
ADV: разработка	Документация по проектированию архитектуры автоматизированных систем и конфигурационная	Интерфейсы и конфигурация компонентов. Внешние интерфейсы. Архитектура, информационные потоки, доступ к СОО. Режим эксплуатации/условия развития
AGD: руководства	Руководства для автоматизированных систем (AOD)	Правила и процедуры для пользователя и администратора. Конфигурация. Подтверждение и верификация (во время эксплуатации)
ALC: поддержка жизненного цикла	Поддержка жизненного цикла автоматизированных систем (AOL)	Аналогично мерам обеспечения безопасности для среды разработки/интеграции. Подтверждение и верификация (во время эксплуатации)
ATE: тестирование	Тестирование автоматизированных систем (AOT)	Функциональное тестирование, глубина тестирования и покрытие тестами ФБС. Независимое тестирование ФБС. Регрессивное тестирование на этапе поддержки (сопровождения)/модификации
AVA: Оценка уязвимостей	—	Анализ уязвимостей автоматизированных систем (AOV)
—	Регистрация и запись в автоматизированных системах (ASO)	Записи в журналы ФБС. Административный анализ ФБС. Независимая верификация ФБС. Подтверждение и верификация записей

8.7 Задание по безопасности для системы

Владелец системы должен зафиксировать определение проблемы безопасности, цели безопасности и требования безопасности для автоматизированной системы в ЗБС. Владелец также должен получать и документировать другую информацию, необходимую для завершения ЗБС, которая определена в приложении А.

Если владелец автоматизированной системы хочет определить требования для автоматизированной системы независимым от реализации способом, он может сначала разработать или заимствовать ПЗС. Обязательное и необязательное содержание ПЗС определено в приложении А.

ЗБС служит основой как для документирования возможностей обеспечения безопасности автоматизированной системы, так и для оценки этих возможностей в СОО. Оно обеспечивает свидетельство и информацию, необходимые для проведения оценки.

ЗБС отличается от ЗБ своей направленностью как на технические, так и на организационные меры безопасности автоматизированной системы. ЗБС можно подразделить на несколько отдельных доменов безопасности с различными функциональными мерами и мерами доверия. Однако, как и ЗБ, ЗБС может оцениваться на согласованность (непротиворечивость) независимо от самого СОО.

Впоследствии при оценке СОО могут быть идентифицированы несоответствия между ЗБС и СОО. Типы расхождений могут включать в себя:

a) аспекты реализованной среды автоматизированной системы, не согласующиеся со средой АС, которая специфицирована в ЗБС;

b) аспекты реализованных функциональных возможностей безопасности автоматизированной системы, отличающиеся от функциональных возможностей безопасности, которые специфицированы в ЗБС;

c) аспекты реализованных интерфейсов и соединений автоматизированной системы и их режимы работы, не согласующиеся с интерфейсами автоматизированной системы, которые специфицированы в ЗБС.

Владелец системы должен определить, реализованы ли среда, функциональные возможности или интерфейсы/соединения требуемым образом, а описание в ЗБС является неправильным, или среда, функциональные возможности или интерфейсы/соединения должны быть такими, как специфицировано в ЗБС. После завершения оценки необходимо внести соответствующие изменения. Эти изменения могут привести к изменениям в ЗБС и/или автоматизированной системе. По этим причинам после оценки ЗБС невозможно вынести окончательный вердикт, является ли ЗБС корректным представлением автоматизированной системы. Только после того, как оценка СОО будет завершена и несоответствия будут разрешены (устранены), можно будет подтвердить, что ЗБС является корректным представлением.

Сравнение элементов ЗБ, определенного в стандартах серии ИСО/МЭК 15408, и ЗБС, определенного в настоящем стандарте, а также их применимость для оценки автоматизированных систем приведены в таблице 4.

Таблица 4 — Сравнение элементов заданий по безопасности

Стандарты серии ИСО/МЭК 15408	Автоматизированная система: ИСО/МЭК ТО 19791	Применимость к автоматизированным системам
Введение	Введение	Должны быть определены ИТ/эксплуатационные части СОО и интерфейсы с внешними автоматизированными системами. Может быть определена доменная организация
Описание ОО		
Среда безопасности ОО	Проблемы безопасности	Вместо угроз следует определить риски. Предположения не должны быть определены, так как среда является реальной
Цели безопасности	Цели безопасности	Должны быть определены цели безопасности для ИТ-частей и эксплуатационных частей СОО, а также для внешних автоматизированных систем
Требования безопасности ИТ	Требования безопасности	Функциональные требования для ИТ-частей СОО. Эксплуатационные требования для эксплуатационных частей СОО. Должны быть определены требования доверия

Окончание таблицы 4

Стандарты серии ИСО/МЭК 15408	Автоматизированная система: ИСО/МЭК ТО 19791	Применимость к автоматизированным системам
Краткая спецификация ОО	Краткая спецификация СОО	Должна быть описана функциональная, эксплуатационная спецификация и спецификации доверия
Утверждения о соответствии ПЗ	Утверждение о соответствии	Могут быть определены утверждения о соответствии ПЗС, ПЗ и/или ЗБ
—	Введение (доменная часть)	Должны быть определены ИТ/эксплуатационные части домена
—	Проблемы безопасности (доменная часть)	Должны быть определены риски и ПБОр
—	Цели безопасности (доменная часть)	Должны быть определены цели безопасности для ИТ- и эксплуатационных частей домена
—	Требования безопасности (доменная часть)	Должны быть определены функциональные требования для ИТ- и эксплуатационных частей домена. Должны быть определены требования доверия для домена
—	Краткая спецификация (доменная часть)	Должна быть описана функциональная, эксплуатационная спецификация и спецификации доверия для домена
—	Утверждение о соответствии (доменная часть)	Могут быть определены утверждения о соответствии ПЗС, ПЗ и/или ЗБ для домена

8.8 Периодическая переоценка

Владелец системы должен специфицировать меры обеспечения безопасности для обеспечения того, чтобы результаты оценки автоматизированной системы оставались действительными во время эксплуатации системы.

Спецификация может быть выполнена следующими способами:

- могут быть специфицированы управленческие меры безопасности для периодической проверки того, что конфигурация технических мер поддерживается, а организационные меры правильно применяются. Для этого должен быть разработан набор процессов и процедур с тем, чтобы управлять влиянием на безопасность изменений, которые происходят в среде системы. Спецификация управленческих мер может включать в себя регрессионное тестирование всех изменений системы для того, чтобы удостовериться, что меры обеспечения безопасности системы не модифицированы и не отключены;

- оценщик может периодически переоценивать СОО (автоматизированную систему), уделяя особое внимание тому, необходима ли корректировка совокупности технических и организационных мер для удовлетворения изменяющихся требований безопасности организации, а также с тем, чтобы подтвердить, что эксплуатационные процессы и процедуры применяются эффективно.

Приложение А
(обязательное)

Профили защиты и задания по безопасности для автоматизированных систем

А.1 Спецификация заданий по безопасности для систем

А.1.1 Краткий обзор

В данном подразделе определяется концепция и содержание задания по безопасности для системы (ЗБС).

ЗБС обеспечивает спецификацию реализованных возможностей обеспечения безопасности автоматизированной системы при ее использовании в среде эксплуатации для противодействия оцененным рискам и/или осуществления политик безопасности организации для достижения приемлемого уровня остаточного риска. Автоматизированная система состоит из интегрированной комбинации функций технических и организационных мер безопасности. В ЗБС излагаются требования и режим функций, реализующие цели безопасности посредством основанных на технологиях и эксплуатации механизмах. Кроме того, в ЗБС описываются меры, обеспечивающие доверие, исходя из способности автоматизированной системы соответствовать своим функциональным целям при работе на приемлемом уровне остаточного риска.

ЗБС служит основанием для проведения оценки автоматизированной системы. Следовательно, в ЗБС должно содержаться описание автоматизированной системы, которое является:

a) достаточно полным. Каждому риску оказывается достаточное противодействие, и каждая политика безопасности организации в достаточной степени осуществляется комбинацией функций технических и организационных мер безопасности;

b) соответствующим и необходимым решением заявленной проблемы. Комбинация функций технических и организационных мер безопасности эффективна при противодействии неприемлемым рискам, а меры доверия обеспечивают достаточное доверие к правильности и эффективности осуществляемых функций безопасности;

c) точной реализацией любых ПЗС, ПЗ или ЗБ, соответствие которым оно утверждает полностью или частично.

Концепция и структура ЗБС основана на расширении концепции и структуры стандартов серии ИСО/МЭК 15408 для ЗБ. Краткое изложение концептуальных различий между ЗБ и ЗБС приведено в таблице А.1.

Таблица А.1 — Краткое изложение различий между ЗБ и ЗБС

	ЗБ «для продукта»	ЗБС
Структура детализации	Сосредоточение на одном «блоке»	Усиление внимания к рассмотрению больших и более сложных группирований компонентов систем, которые можно разделить на домены безопасности
Цели безопасности	Специально для ИТ и отсутствие прямого соответствия целей безопасности требованиям доверия	Конкретные цели, сопоставимые с конкретными требованиями доверия. Взаимосвязь организационных мер безопасности (физических, процедурных и политики) и их вклад в документированное обеспечение безопасности системы и выбранные меры доверия
Документирование среды	Рассматривается в минимальной степени за пределами области оценки риска в виде предположений	Должно быть четко определено и документировано без предположений
Оценка риска	Определяет не связанные с ИТ процедуры как предположения и связанное с ними соответствие продукта	Определяет риски как «известные», и для организационных мер безопасности может потребоваться оценка в отношении их адекватности в интегрированной среде системы
Описание ОО	Сосредоточение на ИТ	Определяет среду технических и организационных мер безопасности, их интерфейсы и взаимоотношения

Окончание таблицы А.1

	ЗБ «для продукта»	ЗБС
Требования соотвествия	Строго выполняемые функции ИТ	Может перераспределять выполняемые функции (например, технические и организационные меры безопасности)
Структура системы	Основано на «автономном» продукте	Обычно разделяется на четкие домены безопасности с различными мерами обеспечения безопасности

А.1.2 Содержание ЗБС

ЗБС должно соответствовать требованиям к содержанию, изложенным в настоящем приложении. ЗБС должно быть представлено как ориентированный на пользователя документ, минимизирующий ссылки на другие материалы, которые могут не быть доступными пользователю ЗБС. При необходимости обоснование может предоставляться отдельно.

ЗБС должно включать в себя:

a) общую часть, применимую ко всему СОО;

b) части домена безопасности, одну для каждого домена, определенного в СОО, и описывающую уникальные аспекты этого домена.

Общая часть должна содержать:

a) введение ЗБС;

b) требования соответствия;

c) определение проблем безопасности;

d) цели безопасности;

e) расширенное определение компонентов;

f) требования безопасности;

g) краткую спецификацию СОО.

Для каждого домена безопасности, образующего часть автоматизированной системы, необходимо включать:

a) введение доменов безопасности;

b) требования соответствия доменов безопасности;

c) определение проблем доменов безопасности;

d) цели безопасности доменов безопасности;

e) требования безопасности доменов безопасности;

f) краткую спецификацию доменов безопасности.

Некоторые разделы ЗБС могут быть незаполненными из-за отсутствия релевантной информации. Требования соответствия появляются только в случае утверждения соответствия ЗБС одному или нескольким ПЗС, ПЗ или ЗБ. Некоторые подразделы информации из домена безопасности являются необязательными. Их необходимо обозначать только в случае наличия у доменов безопасности уникальных проблем, целей или требований безопасности, которые не относятся к СОО в целом.

Спецификации, представленные в данном разделе, взяты частично из спецификаций ЗБ, содержащихся в приложении А к ИСО/МЭК 15408-1 и, частично, из дополнительных требований ЗБС, определенных в настоящем стандарте.

А.1.3 Введение задание по безопасности системы

Во введении ЗБС должны идентифицироваться ЗБС и СОО и обеспечиваться обзор СОО, описание СОО и организация доменов. Введение ЗБС должно содержать информацию об управлении документами и обзорную информацию с учетом того, что:

a) идентификация ЗБС и СОО должна обеспечить информацию о маркировке и описательную информацию, необходимую для контроля и идентификации ЗБС и СОО, к которым относится информация;

b) цели СОО должны резюмироваться в кратком обзоре СОО и представляться в форме отчета. Обзор должен быть достаточно подробным, чтобы потенциальный пользователь мог определить, представляет ли для пользователя интерес ЗБС;

c) в описании СОО должны быть намечены функции и границы СОО в форме отчета;

d) в спецификации структуры доменов должно быть изложено разделение СОО на домены с уникальными требованиями безопасности.

Для краткого обзора СОО установленные содержание или план отсутствуют, но в обзоре должны отражаться цель или задача автоматизированной системы, обзор системы в контексте среды ее эксплуатации и описание системы в отношении деловой деятельности, руководства и технической архитектуры. Необходимо определить взаимосвязь между СОО и внешними автоматизированными системами, а также интерфейсы между СОО и этими системами.

Для описания СОО отсутствует какое-либо заданное содержание или план, но в нем должны излагаться область применения и границы СОО (как логические, так и физические границы). В области применения должны также указываться организация и место разработки СОО, включая любые уникальные характеристики отдельных доменов, например, доменов, основанных на серийно выпускаемых продуктах.

Автоматизированная система состоит из одного или нескольких доменов безопасности. Каждый домен безопасности включает в себя несколько компонентов, и к нему могут предъявляться собственные требования доверия к безопасности. Спецификация структуры доменов должна подробно документировать структуру доменов безопасности, границы доменов и их интерфейсы.

В лучшем случае СОО будет состоять из компонентов, полностью определяющих автоматизированную систему как закрытый объект, в силу чего отсутствуют какие-либо интерфейсы с внешними автоматизированными системами, не включеные в оценку. С практической точки зрения данный наилучший случай иногда невозможен, и необходимо определить четкое разделение частей автоматизированной системы, которые подвергнутся оценке в качестве интегрированной единицы, и частей, не входящих в область действия оценки. Компоненты, не входящие в область действия оценки, рассматриваются как часть внешних автоматизированных систем.

Концепция автоматизированной системы основана на интерфейсах между ее компонентами. Без интерфейсов автоматизированной системы не существует. Следовательно, интерфейсы критически важны для определения автоматизированной системы и равно важны для способности автоматизированной системы осуществлять политику безопасности через ее интерфейсы. Спецификация структур доменов обеспечивает обзор различных компонентов автоматизированной системы, включая способ их соединения. Детали интерфейсов оставлены в спецификациях интерфейсов для проектирования и интеграции. Однако спецификация структур доменов должна определять характеристики безопасности отдельных доменов, которые задаются другим доменам, а также услуги по обеспечению безопасности, предлагаемые отдельными доменами, недоступные другим доменам.

А.1.4 Утверждения о соответствии

Настоящий подраздел применим только в случае утверждения соответствия ЗБС одному или нескольким ПЗС, ПЗ, ЗБ или пакетам требований безопасности. Настоящий подраздел также представляет свидетельство того, что ЗБС является приемлемой реализацией любого ПЗС, ПЗ, ЗБ или пакета требований, соответствие которым утверждается. Обоснование утверждений соответствия должно демонстрировать согласованность между целями и требованиями безопасности ЗБС и целями и требованиями ПЗС, ПЗ, ЗБ или пакетов требований, соответствие которым утверждается.

Основное внимание утверждения соответствия уделяется «эквивалентности» с точки зрения соответствия основному набору критериев, изложенному в ПЗС, ПЗ, ЗБ или пакетах требований. ЗБС может быть функциональным надмножеством пакета или профиля, но оно не должно быть подмножеством.

Основным различием между утверждениями соответствия автоматизированной системы и продукта заключается в том, что для автоматизированной системы можно перераспределять выполняемые функции между частями технических и организационных мер безопасности системы, поскольку они все считаются частью СОО. При оценке продукта распределение выполняемых функций ИТ в среду, не связанную с ИТ, изменяет всю концепцию продукта и аннулирует цель деятельности по оценке продукта.

А.1.5 Определение проблемы безопасности

А.1.5.1 Краткий обзор

Подраздел определения проблем безопасности в ЗБС должен предоставлять когерентное, последовательное и достаточно полное определения проблем безопасности, которые могут стоять перед автоматизированной системой. Проблемы безопасности сформулированы в рисках, которым противодействует автоматизированная система, и политиках безопасности организации, поддерживающих использование автоматизированной системы и управляющих ею для снижения риска этой системы до приемлемого уровня.

Определение проблем безопасности должно определять:

a) риски, применимые к СОО;

b) политики безопасности организации, применимые к СОО.

В настоящем пункте должны идентифицироваться проблемы безопасности, относящиеся ко всему СОО. Возможно, что различные домены безопасности СОО будут реализовываться в различных средах эксплуатации, и результатом этого могут стать различные или специфические риски или политики, которые должны независимо рассматриваться разными доменами безопасности автоматизированной системы. Для каждого домена безопасности должны быть определены дополнительные проблемы безопасности, присущие только этому домену.

Зная, что настоящему подразделу предшествует «введение СОО», важно, чтобы любой материал, представленный в настоящем пункте по СОО, согласовывался с информацией, представленной во «введении СОО».

А.1.5.2 Идентификация рисков

В настоящем пункте все риски, применимые к СОО, должны описываться на основе оценки риска автоматизированной системы. Каждый риск должен категоризироваться как «приемлемый» или «неприемлемый», т.е. требующий снижения или устранения посредством технических или организационных мер в пределах СОО. Принятые риски тем не менее должны идентифицироваться, поскольку приемлемость рисков может со временем измениться.

Перечень рисков должен включать в себя риски, связанные с разработкой автоматизированной системы. Описание каждого риска должно быть достаточно подробным, чтобы идентифицировать активы, которые могут

быть повреждены или скомпрометированы, угрозы и уязвимости, применимые для каждого актива, и воздействия успешной атаки. Угрозы должны характеризоваться, исходя из ассоциированных источников угроз и их потенциально враждебных действий, направленных против активов. При оценке рисков должны идентифицироваться все возможные риски для автоматизированной системы, включая риски, которым противодействуют, или которые устраняются имеющимися мерами обеспечения безопасности.

Примечание — Источники угроз могут включать в себя природные явления, такие как катастрофы, а также человека и созданные им специальные компьютерные программы.

Со временем могут идентифицироваться дополнительные риски или изменяться последствия нарушения безопасности. В течение жизненного цикла системы оценка риска должна повторяться, ЗБС обновляться и, если это необходимо, автоматизированная система оцениваться повторно.

В настоящем подразделе должны идентифицироваться и категорироваться риски, связанные с эксплуатацией системы в целом, например, риски, связанные со служащими или деловыми активами. Некоторые риски, например, риски, связанные с обработкой приложений, могут относиться только к определенному домену безопасности и, следовательно, должны идентифицироваться и анализироваться только для этого домена.

А.1.5.3 Политики безопасности организации (ПБОр)

В автоматизированных системах область применения ПБОр расширена для включения в нее проблем управления процессами жизненного цикла и эксплуатации, которые не рассматриваются во время оценки по стандартам серии ИСО/МЭК 15408. Политики управления процессами жизненного цикла и эксплуатации включают в себя:

a) основные законы и директивы;

b) непрерывность деловой деятельности;

c) соглашения по применениям внутри организации (т.е. внутрислужебное соглашение или меморандум о взаимопонимании).

А.1.6 Цели безопасности

Цели безопасности, содержащиеся в подразделе «цели безопасности» ЗБС, должны обеспечивать когерентное, последовательное и достаточно полное высокоуровневое описание решения безопасности, основанного на определении неприемлемых рисков и политик безопасности организации в разделе определения проблем безопасности. Высокоуровневое описание осуществляется, исходя из функциональных целей безопасности, которые впоследствии распределяются между техническими и организационными мерами безопасности автоматизированных систем или другими автоматизированными системами, сопряженными с данной системой. Обоснование должно демонстрировать, что установленные цели безопасности прослеживаются до всех аспектов, указанных в определении проблем безопасности ЗБС и пригодных для их обеспечения. Обоснование должно обеспечивать полную прослеживаемость между заявленными целями безопасности и всеми аспектами формулировки проблемы безопасности и иметь достаточно информации для определения эффективности противодействия целей безопасности установленным неприемлемым рискам и осуществления установленных политик безопасности организации.

Существует другой тип цели безопасности, управляющий проверочными действиями по созданию и анализу свидетельства и наблюдению и испытанию реализации на соответствие требованиям. Обоснование этому типу цели безопасности обычно не приводится при оценке по стандартам серии ИСО/МЭК 15408 (т.е. конкретные цели безопасности не сопоставляются с конкретными требованиями доверия). В результате этого в документах ПЗ/ЗБ продукта мало информации, обосновывающей выбранные меры доверия, если таковая вообще имеется. Однако для автоматизированной системы необходима четкая формулировка целей доверия, выведенная из аспектов доверия проблемы безопасности для обоснования мер доверия, применимых к автоматизированной системе в целом. Эти меры доверия можно применить к среде разработки ОО или среде эксплуатации.

Формулировка целей безопасности должна охватывать все необходимые меры обеспечения безопасности, включая оба типа уже имеющихся мер обеспечения безопасности, а также меры, которые должны быть приняты как часть реализации автоматизированной системы.

Цели безопасности, выбранные для реализации одного аспекта проблемы безопасности, могут также обеспечивать законченные или частичные решения в других областях. В частности, цели безопасности могут учитывать риски, принятые после их оценки, т.е. категорированные как «допустимые», «приемлемые», «передаваемые» или «риски, которые можно избежать». Подобные случаи должны идентифицироваться и регистрироваться, так как приемлемость рисков может со временем меняться.

Цели безопасности предоставляют на самом высоком уровне формулировку стратегии и философии противодействия определенным рискам для осуществления определенных политик безопасности организации. Для автоматизированных систем критически важна точность целей безопасности. Точность требуется как в отношении того, как цели прослеживают и включают формулировки, принятые при определении проблем безопасности, так и как цели безопасности распределяют решение компонентам автоматизированной системы и физическим процессам.

В отношении установленных рисков и политик безопасности организации цели безопасности должны рассматриваться более подробно, чем в отношении продукта. Более подробное рассмотрение целей безопасности в отношении установленных рисков и политик безопасности организации объясняется воздействием, которое

среда оказывает на оценку автоматизированной системы, и детальной осведомленностью о среде, которая должна быть зарегистрирована в целях безопасности.

Кроме того, цели безопасности автоматизированной системы должны обеспечивать равновесие, достигнутое при менеджменте общего остаточного риска.

Возможно, чтобы разные домены безопасности автоматизированной системы оказывали поддержку и реализовывались в разных средах эксплуатации. Например, возможность мониторинга автоматизированной системой входящего сетевого трафика может конфигурироваться как «выключено», тогда как возможность мониторинга автоматизированной системой сетевого трафика, входящего во внутреннюю сеть, конфигурируется как «включено». В результате для различных доменов безопасности могут существовать различные или уникальные цели безопасности. Для определенных доменов безопасности могут существовать дополнительные цели доверия для выполнения уникальных требований к доверию, применимых только к этим областям.

А.1.7 Определение компонентов расширения

В некоторых случаях подходящие компоненты для описания требований безопасности отсутствуют в стандартах серии ИСО/МЭК 15408 или в настоящем стандарте. В таких случаях в настоящем подразделе ЗБС необходимо определить новые компоненты. Новые расширенные компоненты могут использоваться для определения дополнительных функциональных требований и требований доверия.

А.1.8 Требования безопасности

Настоящий подраздел должен предоставлять полный и последовательный набор требований безопасности для СОО. Настоящий подраздел включает в себя как функциональные требования автоматизированной системы, так и требования доверия к безопасности автоматизированной системы. Он применим как к техническим, так и организационным мерам безопасности, предусмотренным для соответствия целям безопасности автоматизированной системы. Эти требования должны обеспечивать адекватную базу для разработки процессов, процедур, механизмов и услуг безопасности, которые могут быть сконфигурированы для осуществления определенных политик и противодействия идентифицированным рискам. Обоснование требований безопасности должно демонстрировать пригодность набора требований безопасности для выполнения всех целей безопасности ЗБС и их прослеживаемость для достижения этих целей.

В некоторых случаях требования безопасности автоматизированной системы можно сформулировать без обоснования, т.е. они не являются следствием целей безопасности, которые сами выведены из определений проблем безопасности. В этих случаях подразделы «цели безопасности» и «определение проблем безопасности» в ЗБС можно опустить.

В настоящем подразделе должны излагаться функции безопасности системы и меры доверия к безопасности системы, требуемые для автоматизированной системы, исходя из заполненных (завершенных) компонентов безопасности.

Вполне возможно, что различные домены безопасности автоматизированной системы будут реализовываться в различных средах эксплуатации.

В результате могут существовать различные или уникальные функциональные требования для каждого домена безопасности, необходимые для выполнения уникальных целей безопасности этого домена. Аналогично требования доверия к безопасности не следует применять ко всем компонентам автоматизированной системы в одинаковом объеме. Различным доменам безопасности, определенным в ЗБС, необходимо распределять соответствующие уровни и типы доверия.

А.1.9 Краткая спецификация СОО

Краткая спецификация СОО должна предоставлять когерентное, последовательное и достаточно полное описание механизмов безопасности, услуг, интерфейсов, организационных мер безопасности и мер доверия и демонстрировать их соответствие определенным требованиям безопасности автоматизированной системы. Обоснование краткой спецификации СОО должно показывать пригодность функций безопасности и мер доверия СОО для выполнения требований безопасности СОО.

Необходимо, чтобы в ЗБС содержалось достаточно информации о структуре автоматизированной системы с тем, чтобы читатель понял решение, предоставляемое для выполнения требований безопасности. Подробности определения подсистем, интерфейсов и межсоединений и назначение функциональных требований различным подсистемам, которые образуют автоматизированную систему, должны оставляться для использования в последующей проектной документации. В структуре и краткой спецификации ЗБС должны учитываться взаимодействия между доменами безопасности и доменами и их средой.

А.1.10 Информация о доменах безопасности

Настоящий подраздел ЗБС должен предоставлять информацию, относящуюся к каждому домену безопасности, образующему часть полной автоматизированной системы. В информации должна предоставляться точная и корректная идентификация каждого домена безопасности и специфическая для домена информация о безопасности, которая может потребоваться.

Если в СОО имеется только один домен безопасности, его необязательно явно называть или идентифицировать, и настоящий подраздел следует опустить.

Информация для каждого домена безопасности должна содержать:

а) введение домена безопасности должно предоставлять маркировочную и описательную информацию, необходимую для управления и идентификации домена безопасности и СОО, к которому он относится, резюми-

ровать домен и представлять в форме отчета. Для понимания бизнес-функций домена безопасности и требований безопасности его обзор должен быть достаточно подробным;

b) утверждения соответствия домена безопасности должны определять любые утверждения соответствия, уникальные для домена. Если домен безопасности не имеет утверждений соответствия, настоящий подраздел можно опустить;

c) определение проблем безопасности домена безопасности должно определять любые проблемы безопасности, уникальные для домена. Определение проблем безопасности домена безопасности должно включать в себя политики и риски, уникальные для домена. При отсутствии уникальных проблем безопасности домена настоящий подраздел можно опустить;

d) цели безопасности домена безопасности должны определять любые цели безопасности, уникальные для домена. Цели безопасности домена безопасности должны включать в себя цели безопасности, доступные для других доменов или реализуемые другими областями. При отсутствии уникальных целей безопасности для домена безопасности данный подраздел можно опустить;

e) требования безопасности домена безопасности должны определять любые требования безопасности, уникальные для домена. При отсутствии уникальных требований безопасности для домена безопасности настоящий подраздел можно опустить;

f) краткая спецификация домена безопасности должна определять любые механизмы, услуги, интерфейсы, организационные меры безопасности и меры доверия, уникальные для домена. При отсутствии уникальных механизмов, услуг, интерфейсов, организационных мер безопасности и мер доверия настоящий подраздел можно опустить.

А.2 Спецификация профилей защиты систем

А.2.1 Краткий обзор

В данном подразделе определяется концепция и содержание профиля защиты системы (ПЗС).

Концептуально ПЗС выполняет ту же функцию, что и профиль защиты по стандартам серии ИСО/МЭК 15408; ПЗС предоставляет собой определение характеристик приемлемого решения проблемы безопасности. Однако ПЗС приходится иметь дело с интеграцией технических и организационных мер безопасности, и может потребоваться интегрирование многочисленных компонентов или подсистем с различными политиками безопасности и/или средами эксплуатации.

ПЗС должен быть способен представлять варианты и условные решения. Пример приводится в определении целей безопасности. Могут существовать решения как технических, так организационных мер обеспечения безопасности, относящихся к конкретному риску и приемлемых с точки зрения эксплуатации и стоимости. ПЗС может предлагать автору ЗБС на выбор различные приемлемые и обоснованные решения.

ПЗС должен обладать способностью передавать определенные общие меры обеспечения безопасности. Например, в организации может быть принята политика применения некоторых организационных мер безопасности к информационным системам внутри организации.

Наконец, схема детализации ПЗС должна обладать достаточной гибкостью для повторного использования автоматизированной системы, оцененной на основе ПЗС, в качестве оцененного компонента большей системы.

ПЗС может также использоваться как часть спецификации закупки при приобретении автоматизированной системы. Для этого ПЗС должен содержать описание возможностей безопасности автоматизированной системы, которое должно быть:

a) достаточно полным. К каждому риску применяются достаточные контрмеры, и каждая политика организации в достаточной степени осуществляется предписанной комбинацией функций технических и организационных мер безопасности (или выбранным вариантом, если ПЗС допускает альтернативы);

b) соответственным и необходимым решением заявленной проблемы безопасности. Комбинация функций технических и организационных мер обеспечения безопасности эффективна при противодействии неприемлемым рискам и осуществлении политик безопасности организации, а меры доверия обеспечивают достаточное доверие к правильности и эффективности реализации функций безопасности;

c) точной реализацией (конкретизацией) любого ПЗС или ПЗ, о частичном или полном соответствии которому оно заявляет.

Концепция и структура ПЗС основаны на расширении концепции и структуры профилей защиты по стандартам серии ИСО/МЭК 15408. Краткое изложение различий между ПЗ и ПЗС приведено в таблице А.2.

Таблица А.2 — Краткое изложение различий между ПЗ и ПЗС

	ПЗ продукта	ПЗ системы
Схема детализации	Средоточенность на одном «блоке»	Усиление внимания большим и более сложным группировкам продуктов, составляющим автоматизированную систему с физически разбросанным назначением и интегрированными мерами обеспечения безопасности

Окончание таблицы А.2

	ПЗ продукта	ПЗ системы
Средоточие	Более узкое и специфическое для ИТ	Более широкое, гибкое; включает в себя аспекты мер обеспечения безопасности системы — гибкое с учетом меняющихся обстоятельств деловой деятельности
Организационные меры безопасности	Минимальное рассмотрение внешней стороны оценки риска предполагает участие среды	Рассматривает как полноправного партнера с техническими мерами обеспечения безопасности, содействующего безопасности системы для соответствия организационным потребностям
Оценка риска	Рассматривает процедуры, не связанные с ИТ, как предположения, связанные с соответствием продукта	Идентифицирует риски как «известные», и может потребоваться оценка организационных мер безопасности в отношении их адекватности в среде интегрированной системы
Описание ОО	Узкий и сосредоточенный на ИТ	Более широкое объединение внутренних интерфейсов, а также интерфейсов с «внешними/дистанционными» системами, подсистемами и компонентами

А.2.2 Содержание профиля защиты системы

ПЗС должен соответствовать требованиям к содержанию, изложенным в настоящем приложении. ПЗС должен быть представлен в виде ориентированного на пользователя документа, минимизирующего ссылки на другой материал, который может быть труднодоступен для пользователя ПЗС. Обоснование ПЗС может предоставляться по необходимости отдельно.

ПЗС должен включать в себя:

а) общую часть, применимую ко всему СОО;

в) части домена, одну часть для каждого домена безопасности, определенного в СОО, описывающую уникальные аспекты этого домена.

Общая часть должна содержать:

a) введение ПЗС;

b) утверждения соответствия;

c) определение проблем безопасности;

d) цели безопасности;

e) определение расширенных компонентов;

f) требования безопасности.

Для каждого домена безопасности, образующего часть автоматизированной системы, соответствующей ПЗС, необходимо включить:

a) введение домена безопасности;

b) утверждения соответствия домена безопасности;

c) определение проблем безопасности домена безопасности;

d) цели безопасности домена безопасности;

e) требования безопасности домена безопасности.

При отсутствии релевантной информации некоторые разделы ПЗС могут быть не заполнены. Определенные подразделы информации о доменах безопасности являются произвольными. Их надо обозначать только при наличии у доменов безопасности проблем, целей или требований безопасности, которые не относятся к СОО в целом.

Спецификации, представленные в настоящем подразделе, частично заимствованы из спецификаций ПЗ, содержащихся в приложении В к ИСО/МЭК 15408-1, и, частично, из дополнительных требований ПЗС, определенных в настоящем стандарте.

А.2.3 Введение профиля защиты системы

Введение ПЗС должно идентифицировать ПЗС и обеспечивать обзор СОО и организации доменов. Введение ПЗС должно содержать управление документированием и обзорную информацию с учетом того, что:

а) идентификация ПЗС должна предоставлять собой маркировочную и описательную информацию, необходимую для управления и идентификации ПЗС;

b) краткий обзор СОО должен резюмировать СОО, представленный ПЗС в повествовательной форме. Обзор должен быть достаточно подробным, чтобы пользователь ПЗС мог определить его полезность для себя. Краткий обзор должен также быть пригоден для применения в качестве отдельной аннотации в каталогах и указателях по ПЗС;

c) в детализации организации доменов должно быть описано разделение СОО на домены с уникальными требованиями безопасности.

Не существует установленного содержания или схемы краткого обзора об СОО, но в обзоре должны отражаться назначение или задача автоматизированной системы, обзор системы в контексте среды ее эксплуатации и описание системы с точки зрения бизнеса (деловой деятельности), руководства и технической архитектуры. Необходимо определить взаимосвязь между СОО и внешними автоматизированными системами, а также интерфейсы между СОО и этими системами.

Автоматизированная система состоит из одного или нескольких доменов безопасности. Каждый домен безопасности включает в себя несколько компонентов и к нему могут предъявляться собственные требования доверия к безопасности. Спецификация структуры доменов должна подробно документировать структуру доменов безопасности, границы доменов и их интерфейсы.

В лучшем случае СОО будет состоять из компонентов, полностью определяющих автоматизированную систему как закрытый объект, в силу чего отсутствуют какие-либо интерфейсы с внешними автоматизированными системами, не включеные в оценку. С практической точки зрения данный наилучший случай иногда невозможен, и необходимо определить четкое разделение частей автоматизированной системы, которые подвергнутся оценке в качестве интегрированной единицы, и частей, не входящих в область действия оценки. Компоненты, не входящие в область действия оценки, рассматриваются как часть внешних автоматизированных систем.

Концепция автоматизированной системы основана на интерфейсах между ее компонентами. Без интерфейсов автоматизированной системы не существует. Следовательно, интерфейсы критически важны для определения автоматизированной системы и равно важны для способности автоматизированной системы осуществлять политику безопасности через ее интерфейсы. Спецификация структур доменов обеспечивает обзор различных компонентов автоматизированной системы, включая способ их соединения. Детали интерфейсов оставлены в спецификациях интерфейсов для проектирования и интеграции. Однако спецификация структур доменов должна определять характеристики безопасности отдельных доменов, которые задаются другим доменам, а также услуги по обеспечению безопасности, предлагаемые отдельными доменами, недоступные другим доменам.

А.2.4 Утверждения о соответствии

Настоящий подраздел применим только в случае утверждения соответствия ЗБС одному или нескольким ПЗС, ПЗ или пакетам требований безопасности. Настоящий подраздел также представляет свидетельство того, что ЗБС является приемлемой реализацией любого ПЗС, ПЗ или пакета требований, соответствие которым утверждается. Обоснование утверждений соответствия должно демонстрировать согласованность между целями и требованиями безопасности ЗБС и целями и требованиями ПЗС, ПЗ или пакетов требований, соответствие которым утверждается.

Основное внимание утверждения соответствия уделяется «эквивалентности» с точки зрения соответствия основному набору критериев, изложенному в ПЗС, ПЗ или пакетах требований. ЗБС может быть функциональным надмножеством пакета или профиля, но оно не должно быть подмножеством.

Основным различием между утверждениями соответствия автоматизированной системы и продукта заключается в том, что для автоматизированной системы можно перераспределять выполняемые функции между частями технических и организационных мер безопасности системы, поскольку они все считаются частью СОО. При оценке продукта распределение выполняемых функций ИТ в среду, не связанную с ИТ, изменяет всю концепцию продукта и аннулирует цель деятельности по оценке продукта.

А.2.5 Определение проблемы безопасности

А.2.5.1 Краткий обзор

Подраздел «Определение проблем безопасности» в ЗБС должен предоставлять когерентное, последовательное и достаточно полное определения проблем безопасности, которые, как предполагается, могут стоять перед автоматизированными системами, сответствующими требованиям ПЗС. Проблемы безопасности сформулированы в рисках, которым противодействует автоматизированная система, и политиках безопасности организации, поддерживающих использование автоматизированной системы и управляющих ею, соответствующих требованиям ПЗС, для снижения риска этой системы до приемлемого уровня.

Определение проблемы безопасности должно определять:

a) риски, применимые к СОО;

b) политики безопасности организации, применимые к СОО.

В настоящем пункте должны идентифицироваться проблемы безопасности, которые относятся к автоматизированным системам, соответствующим требованиям ПЗС в целом. Может быть, что различные домены безопасности автоматизированных систем, соответствующих ПЗС, функционируют в разных средах, и в результате могут появиться различные или уникальные политики или риски, которые должны учитываться независимо различными доменами безопасности автоматизированной системы. Для каждого домена безопасности должны быть определены дополнительные проблемы безопасности, присущие только этому домену.

Если оценка риска фактической автоматизированной системы указывает на наличие рисков, не идентифицированных в ПЗС, необходимо изменить границы системы для устранения этих рисков или ввести дополнительные риски в пункт «идентификация риска» ЗБС.

Зная, что настоящему подразделу предшествует «введение СОО», важно, чтобы любой материал, представленный в настоящем пункте ПЗС, соответствовал информации, имеющейся в подразделе «введение СОО».

А.2.5.2 Идентификация рисков

В настоящем пункте все риски, применимые к СОО, должны описываться на основе оценки риска автоматизированной системы или типов автоматизированной системы, охватываемых ПЗС. Каждый риск должен категоризироваться как «приемлемый» или «неприемлемый», т.е. требующий снижения или устранения посредством технических или организационных мер в пределах СОО. Принятые риски тем не менее должны идентифицироваться, поскольку приемлемость рисков может со временем измениться.

Перечень рисков должен включать в себя риски, связанные с разработкой автоматизированной системы. Описание каждого риска должно быть достаточно подробным, чтобы идентифицировать активы или типы актива, которые могут быть повреждены или скомпрометированы, угрозы и уязвимости, относящиеся к каждому активу или типу актива, и воздействие успешной атаки. Угрозы должны характеризоваться, исходя из источников этих угроз и их потенциально негативного воздействия на активы. При оценке рисков должны идентифицироваться все возможные риски для автоматизированных систем, соответствующих требованиям ПЗС.

Примечание — Источники угроз могут включать в себя природные явления, такие как катастрофы, а также человека и созданные им специальные компьютерные программы.

Со временем могут идентифицироваться дополнительные риски или изменяться последствия нарушения безопасности. В течение жизненного цикла системы оценка риска должна повторяться, ПЗС обновляться и, если это необходимо, автоматизированная система — оцениваться повторно.

В настоящем подразделе должны идентифицироваться и категорироваться риски, связанные с эксплуатацией систем, удовлетворяющих в целом требованиям ПЗС, например, риски, связанные с работниками или бизнес-активами. Некоторые риски, например, риски, связанные с обработкой приложений, могут относиться только к определенному домену безопасности и, следовательно, идентифицироваться и анализироваться только для этого домена.

А.2.5.3 Политики безопасности организации (ПБОр)

В автоматизированных системах область применения ПБОр расширена для включения в нее проблем управления процессами жизненного цикла и эксплуатации, которые не рассматриваются во время оценки по стандартам серии ИСО/МЭК 15408. Политики управления процессами жизненного цикла и эксплуатации включают в себя:

a) основные законы и директивы;

b) непрерывность деловой деятельности;

c) соглашения по применениям внутри организации (т.е. внутрислужебное соглашение или меморандум о взаимопонимании).

А.2.6 Цели безопасности

Цели безопасности, содержащиеся в подразделе «цели безопасности» ПЗС, должны обеспечивать когерентное, последовательное и достаточно полное высокоуровневое описание решения безопасности, основанного на определении неприемлемых рисков и политик безопасности организации в разделе определения проблем безопасности. Высокоуровневое описание осуществляется, исходя из функциональных целей безопасности, которые впоследствии распределяются между техническими и организационными мерами безопасности автоматизированных систем, удовлетворяющих требованиям ПЗС, или других автоматизированных систем, сопряженных с данной системой. Обоснование должно демонстрировать, что установленные цели безопасности прослеживаются до всех аспектов, указанных в определении проблем безопасности ЗБС и пригодных для их обеспечения. Обоснование должно обеспечивать полную прослеживаемость между заявленными целями безопасности и всеми аспектами формулировки проблемы безопасности и иметь достаточно информации для определения эффективности противодействия целей безопасности установленным неприемлемым рискам и осуществления установленных политик безопасности организации.

Существует другой тип цели безопасности, управляющий проверочными действиями по созданию и анализу свидетельства и наблюдению и испытанию реализации на соответствие требованиям. Обоснование этому типу цели безопасности обычно не приводится при оценке по стандартам серии ИСО/МЭК 15408 (т.е. конкретные цели безопасности не сопоставляются с конкретными требованиями доверия). В результате имеется мало информации, если таковая вообще имеется, в документах ПЗ/ЗБ продукта, обосновывающего выбранные меры доверия. Однако для автоматизированной системы необходима четкая формулировка целей доверия, выведенная из аспектов доверия проблемы безопасности для обоснования мер доверия, применимых к автоматизированной системе в целом. Эти меры доверия можно применить к среде разработки СОО или среде эксплуатации.

Формулировка целей безопасности должна охватывать все требуемые меры обеспечения безопасности, включая обе меры, существование которых предполагается, и меры, которые должны быть приняты как часть реализации автоматизированной системы.

Цели безопасности, выбранные для реализации одного аспекта проблемы безопасности, могут также обеспечивать решения или частичные решения в других областях. В частности, цели безопасности могут адресовать риски, принятые после оценки риска, т.е. категорированные как допустимые, приемлемые, передаваемые или риски, которых надо избегать. Подобные взаимосвязи должны быть идентифицированы и зарегистрированы, так как приемлемость рисков может со временем изменяться.

Цели безопасности предоставляют на самом высоком уровне формулировку стратегии и философии противодействия определенным рискам и для осуществления определенных политик безопасности организации. Для автоматизированных систем критически важной является точность целей безопасности. Точность требуется как в отношении того, как цели прослеживают и включают формулировки, принятые при определении проблем безопасности, так и как цели безопасности распределяют решение компонентам автоматизированной системы и физическим процессам.

В отношении установленных рисков и политик безопасности организации цели безопасности должны рассматриваться более подробно, чем в отношении продукта. Более подробное рассмотрение целей безопасности в отношении установленных рисков и политик безопасности организации объясняется воздействием, которое среда оказывает на оценку автоматизированной системы, и детальной осведомленностью о среде, которая должна быть зарегистрирована в целях безопасности.

Кроме того, цели безопасности автоматизированной системы должны обеспечить равновесие, достигаемое при менеджменте общего остаточного риска.

Возможно, чтобы разные домены безопасности автоматизированной системы оказывали поддержку и реализовывались в разных средах эксплуатации. Например, возможность мониторинга автоматизированной системой входящего сетевого трафика может конфигурироваться как «выключено», тогда как возможность мониторинга автоматизированной системой сетевого трафика, входящего во внутреннюю сеть, конфигурируется как «включено». В результате для различных доменов безопасности могут существовать различные или уникальные цели безопасности. Для определенных доменов безопасности могут существовать дополнительные цели доверия для выполнения уникальных требований к доверию, применимых только к этим областям.

А.2.7 Определение компонентов расширения

В некоторых случаях подходящие компоненты для описания требований безопасности отсутствуют в стандартах серии ИСО/МЭК 15408 или в настоящем стандарте. В таких случаях в настоящем подразделе ПЗС необходимо определить новые компоненты. Новые расширенные компоненты могут использоваться для определения дополнительных функциональных требований и требований доверия.

А.2.8 Требования безопасности

Настоящий подраздел должен предоставлять полный и последовательный набор требований безопасности для СОО. Он включает в себя как функциональные требования безопасности автоматизированной системы, так и требования к доверию безопасности автоматизированной системы. Это относится как к техническим, так и организационным мерам безопасности, которые должны предоставляться для выполнения целей безопасности автоматизированной системы. Эти требования должны обеспечить адекватную основу для разработки процессов, процедур, механизмов и услуг безопасности, которые можно конфигурировать для осуществления определенных политик и противодействия идентифицированным рискам. Обоснование требований безопасности должно продемонстрировать пригодность набора для выполнения всех целей безопасности ЗБС и их прослеживаемость достижения этих целей.

В некоторых случаях требования безопасности в ПЗС могут излагаться без обоснования, т.е. они не являются следствием целей безопасности, которые сами выведены из определений проблем безопасности. В этих случаях подразделы «цели безопасности» и «определение проблем безопасности» в ПЗС можно опустить.

В настоящем подразделе должны излагаться функции безопасности системы и меры доверия к безопасности системы, требуемые для автоматизированной системы, соответствующей требованиям ПЗС, исходя из завершенных компонентов безопасности.

Вполне возможно, что различные домены безопасности автоматизированных систем, соответствующих требованиям ПЗС, оказывают поддержку и реализуются в различных средах эксплуатации.

В результате могут существовать различные или уникальные функциональные требования для каждого домена безопасности, необходимые для выполнения уникальных целей безопасности этого домена. Аналогично требования доверия к безопасности нельзя применять ко всем компонентам автоматизированной системы в одинаковом объеме. Различным доменам безопасности, определенным в ПЗС, необходимо распределять соответствующие уровни и типы доверия.

А.2.9 Информация о доменах безопасности

Настоящий подраздел ПЗС должен предоставлять информацию, относящуюся к каждому домену безопасности, имеющему полномочия от ПЗС. Он должен обеспечивать точную и правильную идентификацию каждого домена безопасности и информацию по безопасности, являющуюся специфической для любого домена.

Если ПЗС не дает полномочия более чем одному домену безопасности, его не следует называть явно или идентифицировать, и этот подраздел следует опустить. Следует отметить, что соображения, связанные с архитектурой, могут означать, что ЗБС, основанное на ПЗС, вводит дополнительные домены безопасности с целью осуществления рентабельного решения проблем безопасности.

Информация о каждом домене безопасности должна содержать следующую информацию:

a) введение домена безопасности должно предоставлять маркировочную и описательную информацию для управления и идентификации домена безопасности и СОО, к которому он относится, и резюмировать область в форме отчета (повествовательной форме). Общее положение должно быть достаточно подробным для понимания бизнес-функций домена безопасности и его требований безопасности;

b) утверждения соответствия домена безопасности должны определять любые утверждения соответствия, уникальные для этого домена. Если у домена безопасности подобные утверждения отсутствуют, этот подраздел можно опустить;

c) определение проблем безопасности домена безопасности должно определять любые проблемы безопасности, уникальные для этого домена, а также включать в себя политики и риски, уникальные для домена. Если у домена безопасности отсутствуют уникальные проблемы безопасности, этот подраздел можно опустить;

d) цели безопасности домена безопасности должны определять любые цели безопасности, уникальные для этого домена, а также любые цели безопасности, которые доступны другим доменам или которые реализуются другими доменами. Если у домена безопасности отсутствуют уникальные цели безопасности, этот подраздел можно опустить;

e) требования безопасности домена безопасности должны определять любые требования безопасности, уникальные для этого домена. Если у домена безопасности отсутствуют уникальные требования безопасности, этот подраздел можно опустить.

Приложение В
(обязательное)

Функциональные требования безопасности автоматизированных систем

В.1 Введение

В данном приложении определены функциональные требования к мерам обеспечения безопасности автоматизированных систем, охватывающие аспекты управления и процедурные аспекты СОО. Описанные ниже требования используются в сочетании с техническими функциональными требованиями по ИСО/МЭК 15408-2 для удовлетворения целей безопасности для СОО. ИСО/МЭК 15408-2 используется в качестве основы для структуры этих компонентов.

Функциональные требования к мерам обесечения безопасности автоматизированных систем классифицируются по рассматриваемым объектам, функциональным областям и действиям.

Объект — непосредственный объект применения мер обеспечения безопасности, такой как бизнес-данные, средства обработки информации или системы ИТ. Функциональная область — объект для таких определенных операций, как политика, менеджмент рисков или регистрация/запись. Каждая функциональная область образует в рамках класса семейство.

Действие — операция в определенной функциональной области; действие образует компонент в рамках семейства. Элементами являются конкретные определения правил и процедур для мер обеспечения безопасности.

В данном приложении определены новые классы организационных мер безопасности. Они включают в себя:

a) администрирование (FOD); специфицирует требования к организационным мерам, связанным с администрированием;

b) системы ИТ (FOS); специфицирует требования к организационным мерам, поддерживающие использование систем ИТ и оборудования;

c) активы пользователей (FOA); специфицирует требования к организационным мерам, связанные с управлением активами пользователей;

d) бизнес (FOB); специфицирует требования к организационным мерам, связанные с бизнес-процессами и функциями;

e) аппаратура и оборудование (FOP); специфицирует требования к организационным мерам, связанные с бизнес-оборудованием, аппаратурой и зданиями (сооружениями);

f) третьи стороны (FOT); специфицирует требования к организационным мерам, связанные с третьими сторонами;

g) управление (FOM); специфицирует требования к организационным мерам, связанные с деятельностью по менеджменту безопасности.

Семейства функций организационного управления в рамках этих классов приведены в таблице В.1.

Таблица В.1 — Семейства функций организационного управления

Класс	Семейство
Администрирование (FOD)	Администрирование политик (FOD_POL)
	Администрирование по отношению к персоналу (FOD_PSN)
	Администрирование управления рисками (FOD_RSM)
	Администрирование управления инцидентами (FOD_INC)
	Администрирование организации безопасности (FOD_ORG)
	Администрирование соглашений об услугах (FOD_SER)
Системы ИТ (FOS)	Политика для систем ИТ (FOS_POL)_
	Конфигурация систем ИТ (FOS_CNF)
	Сетевая безопасность систем ИТ (FOS_NET)
	Мониторинг систем ИТ (FOS_MON)

Окончание таблицы В.1

Класс	Семейство
Системы ИТ (FOS)	Управление персоналом систем ИТ (FOS_PSN)
	Активы систем ИТ в автоматизированных системах (FOS_OAS)
	Протоколирование в системах ИТ (FOS_RCD)
Активы пользователей (FOA)	Защита приватных данных (FOA_PRO)
	Защита информации в активах пользователей (FOA_INF)
Бизнес (FOB)	Бизнес-политики (FOB_POL)
	Непрерывность бизнеса (FOB_BCN)
Оборудование и аппаратура (FOP)	Передвижное оборудование (FOP_MOB)
	Съемное оборудование (FOP_RMM)
	Дистанционное оборудование (FOP_RMT)
	Системное оборудование (FOP_SYS)
	Управление аппаратурой (FOP_MNG)
Третьи стороны (FOT)	Обязательства третьих сторон (FOT_COM)
	Управление взаимодействием с третьей стороной (FOT_MNG)
Управление (FOM)	Управление параметрами безопасности (FOM_PRM)
	Управление классификацией активов (FOM_CLS)
	Управление обязанностями персонала, связанными с безопасностью (FOM_PSN)
	Управление организацией безопасности (FOM_ORG)
	Управление отчетами о безопасности (FOM_INC)

Зависимости между компонентами этих семейств показаны в таблице В.2. Для каждого из компонентов, от которого зависит какой-либо функциональный компонент, выделена колонка таблицы В.2. Знак «X» в таблице В.2 указывает на наличие зависимости между рассматриваемыми компонентами этих семейств.

Таблица В. 2 — Зависимости между компонентами организационного управления

Компоненты семейств	FOD_PSN.1	FOD_PSN.3	FOD_PSN.5	FOD_PSM.1	FOD_ORG.1	FOD_ORG.2	FOS_POL.1	FOS_POL.4	FOS_NET.1	FOA_POL.3	FOM_PRM.2	FOM_INC.1
FOD_INC.1						X						X
FDS_SER.1									X			
FOS_POL.1										X		
FOS_PSN.1	X	X								X		
FOS_OAS.1							X					

Окончание таблицы 2

Компоненты семейств	FOD_PSN.1	FOD_PSN.3	FOD_PSN.5	FOD_PSM.1	FOD_ORG.1	FOD_ORG.2	FOS_POL.1	FOS_POL.4	FOS_NET.1	FOA_POL.3	FOM_PRM.2	FOM_INC.1
FOA_INF.1							X					
FOB_POL.1							X					
FOB_BCN.1				X								
FOP_MNG.1			X									
FOT_MNG.1		X										
FOM_PRM.1								X				
FOM_PSN.1										X		
FOM_ORG.1					X							
FOM_ORG.2						X						

Некоторые требования для организационных мер обеспечения безопасности всегда реализуются как организационные требования и, следовательно, определяются как ОФБ. Другие требования могут быть организационными или техническими и, следовательно, описываться как ФБС.

По сравнению с требованиями ИСО/МЭК 15408-2 в настоящем стандарте имеется четыре различия в представлении. Иерархические компоненты организационных мер отсутствуют, так что соответствующие подзаголовки отсутствуют. Все действия по управлению регулируются явными компонентами, поэтому подзаголовки для действий по управлению не требуются. Подзаголовок аудита заменен на записи, которые лучше отражают процесс сбора необходимых свидетельств для организационных мер безопасности. Разрешенная заданием организация безопасности осуществляется более гибко, чем в ИСО/МЭК 15408-2. Идентификацию документов, описывающих сопутствующие политику, процедуры, правила, требования безопасности и другие меры обеспечения безопасности, можно определить как задание безопасности.

B.2 Класс FOD:Администрирование

Данный класс определяет требования к организационным мерам для администрирования автоматизированной системы.

B.2.1 Администрирование политик (FOD_POL)

B.2.1.1 Характеристика семейства

Данное семейство определяет политики безопасности автоматизированной системы для управления и включает в себя детализацию политик безопасности, собрания руководства, проверку руководством и управленческие меры обеспечения безопасности при нарушении безопасности.

B.2.1.2 Ранжирование компонентов

FOD_POL.1 Политика безопасности

Определены управленческие меры безопасности, цели и объекты политики безопасности, проверка руководством и управленческие меры безопасности при ее нарушении.

FOD_POL.2 Политика защиты данных и приватности

Определяется политика защиты данных и приватности.

B.2.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_POL.1: описание обязательств руководства, политики безопасности, проверки руководством и управленческие меры безопасности при нарушении безопасности с конкретными действиями и спецификациями.

Для FOD_POL.2: описание политики защиты данных и приватности.

B.2.1.4 Политика безопасности FOD_POL.1

Зависимости: зависимости отсутствуют.

FOD_POL.1.1 ОФБ должны определять [назначение: обязательства руководства] по активному поддержанию безопасности в организации посредством четкого управления, продемонстрированной приверженности, назначения и признания обязанностей по обеспечению информационной безопасности.

FOD_POL.1.2 ОФБ должны определять политику информационной безопасности, включая задачи, цели, область применения, соответствие законодательству, требования договора и стандартов, оценку риска и менеджмент риска, обучение безопасности, подготовку и требования к осведомленности, управление непрерывностью бизнес-процессов, последствия нарушения информационной безопасности, обязательства организации и ее подход к менеджменту информационной безопасности.

FOD_POL.1.3 ОФБ должны определять формальные процедуры проверок руководством, включая информацию о способе независимых проверок, результатах предыдущих проверок руководством, изменения, могущие повлиять на подход организации к менеджменту информационной безопасности, рекомендации, предоставляемые соответствующими органами, тенденции, связанные с угрозами и уязвимостями, и зарегистрированные инциденты безопасности в качестве входных данных.

FOD_POL1.4 ОФБ должны определять политику в отношении персонала, определяющую порядок прохождения персоналом переподготовки в части нарушения организационных мер безопасности.

FOD_POL.1.5 ОФБ должны определять требования безопасности для средств передачи сообщений о действиях при нарушении организационных мер безопасности, которые осуществляются до предоставления персоналу доступа к активам системы.

FOD_POL.1.6 ОФБ должны определять политику в отношении персонала, обеспечивающую меры наложения санкций, таких, например, как денежный штраф, лишение привилегий, дисквалификация или другое наказание за нарушение организационных мер безопасности.

FOD_POL.1.7 ОФБ должны определять требования безопасности, по которым нарушитель лишается доступа к активам системы, ограничивается его доступ к ним или инициируются другие подобные действия, до восстановления его прав.

FOD_POL.1.8 ОФБ должны определять политику в отношении персонала, обеспечивая меры, разрешенные законом по увольнению персонала при нарушении правил и процедур.

FOD_POL.1.9 ОФБ должны определять требования безопасности для всех соответствующих требований закона, обязательных требований и требований контракта и подход организации к выполнению этих требований и поддержанию их актуальности для каждой информационной системы и организации.

FOD_POL.1.10 ОФБ должны определять политику информационной безопасности, которая предусматривает разработку и внедрение соответствующего набора процедур маркирования и обработки информации в соответствии с классификационной схемой, принятой организацией.

FOD_POL.1.11 ОФБ должны определять политику информационной безопасности, которая предусматривает независимый пересмотр подхода организации к менеджменту информационной безопасности и его реализацию (т.е. пересмотр целей обеспечения безопасности, политики, процессов и процедур обеспечения информационной безопасности) через запланированные периоды времени или при внесении значительных изменений в процесс реализации безопасности.

FOD_POL.1.12 ОФБ должны определять политику информационной безопасности в части учета определенных требований безопасности перед предоставлением пользователям доступа к информации или активам организации.

FOD_POL.1.13 ОФБ должны определять политику информационной безопасности в части одобрения документа политики безопасности руководством, его опубликования и передачи документа всем служащим и соответствующим внешним сторонам.

B.2.1.5 FOD_POL.2 Политика защиты данных и приватности

Зависимости: зависимости отсутствуют.

FOD_POL.2.1 OSF должны разрабатывать и реализовывать политику защиты данных и приватности.

B.2.2 Администрирование по отношению к персоналу (FOD_PSN)

B.2.2.1 Характеристика семейства

Данное семейство определяет администрирование по отношению к персоналу, связанное с безопасностью, в автоматизированной системе, а также включает в себя подробное изложение должностей и обязанностей персонала, административные взыскания, содержание договоров с персоналом, управление идентификацией пользователей, контроль за активами и осведомленность, обучение и подготовку персонала.

B.2.2.2 Ранжирование компонентов

FOD_PSN.1 Должности и обязанности персонала

Определены обязанности руководства, обязанности по осуществлению процесса выхода, правовые обязательства и меры обеспечения безопасности для персонала, работающего на охраняемых участках. Определены условия договора о передаче и правила подписания соглашения о конфиденциальности или неразглашения. Определены правила соблюдения точных границ области разрешенного доступа. Определены правила наблюдения за посетителями и их удаления. Определены правила, касающиеся приемлемого применения и возврата активов организации.

FOD_PSN.2 Обеспечение осведомленности об информационной безопасности, обучения и профессиональной подготовки

Определены требования по обеспечению осведомленности об информационной безопасности, обучению и профессиональной подготовке.

B.2.2.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_PSN.1: описание обязанностей руководства, обязанностей по осуществлению процесса выхода, правовых обязательств и мер обеспечения безопасности для персонала, работающего на охраняемых участках, официального дисциплинарного процесса с конкретными действиями, детализацией и записями о наложении дисциплинарных взысканий, условий договора о передаче и правил подписания договора, правил подписания соглашения о конфиденциальности или неразглашении, правил проведения идентификации пользователей, правил соблюдения точных границ области разрешенного доступа и правил, касающихся приемлемого применения и возврата активов организации с конкретными действиями и детализацией, и записей об осуществлении контроля.

Для FOD_PSN.2: записи об обеспечении осведомленности об информационной безопасности, обучению и профессиональной подготовке.

B.2.2.4 FOD_PSN.1 Должности и обязанности персонала

Зависимости:

FOD_PSN.1 Политика безопасности;

FOD_RSM.1 Менеджмент рисков внутри организации.

FOD_PSN.1.1 ОФБ должны разработать и документировать должности и обязанности служащих, подрядчиков и пользователя третьей стороны в соответствии с политикой безопасности организации.

FOD_PSN.1.2 ОФБ должны определять обязанности по окончании работы по найму или при изменении вида деятельности.

FOD_PSN.1.3 ОФБ должны определять текущие требования безопасности, правовые обязанности, соглашения о конфиденциальности и условия, сохраняющиеся в течение определенного периода после выполнения задания служащим, подрядчиком или пользователем третьей стороны, по передаче обязанностей при увольнении.

FOD_PSN.1.4 ОФБ должны определять требования безопасности для персонала, работающего на охраняемых участках.

FOD_PSN.1.5 ОФБ должны определять требования безопасности при лишении прав доступа служащих, подрядчиков и пользователей третьей стороны к информации и средствам обработки информации по окончании их срока службы, прекращении действия контракта или соглашения или корректировки этих прав при изменении вида деятельности.

FOD_PSN.1.6 ОФБ должны определять требования безопасности по всем кандидатурам для кадров, подрядчиков и пользователей третьей стороны в соответствии с релевантными законами и положениями.

FOD_PSN.1.7 ОФБ должны определять процедуры, разработанные и выполняемые при сборе и предоставлении свидетельств для наложения дисциплинарного взыскания, внутри организации.

FOD_PSN.1.8 ОФБ должны определять требования безопасности по официальному дисциплинарному процессу в отношении служащих, подрядчиков и пользователей третьей стороны, нарушивших правила безопасности.

FOD_PSN.1.9 ОФБ должны определять требования безопасности по условиям договора о передаче, которые формулируют: правовые обязанности и права служащих, подрядчиков и пользователей третьей стороны, обязанности по классификации и управлению данными организации, используемыми служащими, подрядчиками и пользователями третьей стороны, обязанности служащего по обработке персональной информации, включая персональную информацию, созданную в результате или в ходе выполнения задания организации, обязанности, выполняемые за пределами помещений организации и в сверхурочное время, и действия, предпринимаемые в случае игнорирования служащими, подрядчиками и пользователями третьей стороны требований безопасности, обязательных для всех работников организации, новых служащих, подрядчиков и пользователей третьей стороны. Обязанности, содержащиеся в условиях найма, должны оставаться в силе в течение определенного периода времени после завершения работы по найму.

FOD_PSN.1.10 ОФБ должны определять правила, с которыми согласны служащие, подрядчики и пользователи третьей стороны и которые подписываются ими в качестве их договорного обязательства в отношении обязательств организации по обеспечению информационной безопасности.

FOD_PSN.1.11 ОФБ должны определять правила подписания соглашения о конфиденциальности или неразглашении как части начальных условий найма перед предоставлением права доступа к средствам обработки информации и то, что требования соглашений о конфиденциальности или неразглашении, отражающие потребность организации в защите информации, идентифицированы и регулярно пересматриваются.

FOD_PSN.1.12 ОФБ должны определять требования безопасности для соглашения о конфиденциальности при внесении изменений в условия задания или контракта, особенно в случае необходимости для работников покинуть организацию или в случае окончания контракта.

FOD_PSN.1.13 ОФБ должны определять правила ношения персоналом каких-либо знаков визуального распознавания.

FOD_PSN.1.14 ОФБ должны определять правила предотвращения допуска к оборудованию организации любых несанкционированных лиц.

FOD_PSN.1.15 ОФБ должны определять правила использования информации и активов организации.

Примечание — Активы организации включают в себя ранее выпущенное программное обеспечение, корпоративные документы, переносные вычислительные устройства, кредитные карточки, карточки доступа, программное обеспечение, руководства и хранимую на электронных носителях информацию.

FOD_PSN.1.16 ОФБ должны определять правила возврата всеми служащими, подрядчиками и пользователями третьей стороны всех активов организации, находящихся в их владении, по завершении их работы по найму, контракта или договора.

FOD_PSN.1.17 ОФБ должны определять правила предотвращения выноса активов организации служащими, подрядчиками и пользователями третьей стороны за территорию организации без разрешения.

FOD_PSN.1.18 ОФБ должны определять правила разделения обязанностей и доменов ответственности для уменьшения вероятности несанкционированного или непреднамеренного изменения или неправильного использования активов организации.

FOD_PSN.1.19 ОФБ должны определять требования безопасности по официальному процессу наложения дисциплинарных взысканий на работников, нарушивших правила безопасности.

B.2.2.5 FOD_PSN.2 Обеспечение осведомленности об информационной безопасности, обучении и профессиональной подготовке

Зависимости: зависимости отсутствуют.

FOD_PSN.2.1 ОФБ должны определять и документировать требования безопасности, по которым все служащие, подрядчики и пользователи третьей стороны получили соответствующую подготовку в отношении осведомленности о регулярных обновлениях политик и процедур организации соответственно своей должности.

FOD_PSN.2.2 ОФБ должны определять и документировать требования безопасности, по которым подготовка в отношении осведомленности должна начинаться с формального ознакомительного процесса, предназначенного для ознакомления с политиками безопасности и ожиданиями организации перед предоставлением доступа к информации или услугам.

FOD_PSN.2.3 ОФБ должны определять и документировать требования безопасности, по которым текущее обучение должно включать в себя знание требований безопасности, правовых обязанностей и мер обеспечения деловой деятельности, а также обучение правильному использованию средств обработки информации, пакетов программ и информации о процессе наложения дисциплинарных взысканий.

B.2.3 Администрирование менеджмента риска (FOD_RSM)

B.2.3.1 Характеристика семейства

Данное семейство определяет управления рисками для администрирования и включает в себя менеджмент рисков для организации и связанных с ней третьих сторон.

B.2.3.2 Распределение компонентов по уровню

FOD_RSM.1 Менеджмент рисков внутри организации

Определены процедуры менеджмента рисков.

FOD_RSM.2 Менеджмент рисков, связанных с доступом третьих сторон

Определены процедуры менеджмента рисков, связанных с доступом третьих сторон.

B.2.3.3 Записи

Для FOD_RSM.1: описание менеджмента рисков для организации с конкретными действиями и записями о проведении менеджмента рисков.

Для FOD_RSM.1: описание менеджмента рисков, связанных с доступом третьих сторон, с конкретными действиями и детализацией и записями о проведении менеджмента рисков.

B.2.3.4 FOD_RSM.1 Менеджмент рисков внутри организации

Зависимости: зависимости отсутствуют.

FOD_RSM.1.1 ОФБ должны определять процедуры менеджмента рисков для списков информации и средств обработки информации, включая надомников и других удаленных или мобильных пользователей.

FOD_RSM.1.2 ОФБ должны определять требования безопасности проведения менеджмента рисков для автоматизированной системы с бизнес-процессом.

FOD_RSM.1.3. ОФБ должны определять требования безопасности, по которым получается своевременная информация о технических уязвимостях используемых информационных систем, оценивается подверженность организации таким уязвимостям и принимаются соответствующие действия по обработке рисков, связанных с этими уязвимостями.

B.2.3.5 FOD_RSM 2 Менеджмент рисков, связанных с доступом третьих сторон

Зависимости: зависимости отсутствуют.

FOD_RSM.2.1 ОФБ должны определять процедуры менеджмента рисков для перечней информации и средств обработки информации, к которым третьи стороны получат доступ с учетом перечней мер обеспечения безопасности, используемых третьими сторонами, правовые и нормативные требования, которые должна учитывать третья сторона, и договорные обязательства, которые должны учитывать организация и третья сторона.

FOD_RSM.2.2 ОФБ должны определять процедуры идентификации рисков для информации и средств обработки информации организации, исходящих от бизнес-процессов, включая внешние организации, и реализации соответствующих мер перед предоставлением доступа.

В.2.4 Администрирование управления инцидентами (FOD_INC)

В.2.4.1 Характеристика семейства

Данное семейство определяет управление инцидентами для администрирования и включает в себя детализацию управления инцидентами.

В.2.4.2 Ранжирование компонентов

FOD_INC.1 Инциденты безопасности

Определены процедура сообщения об инцидентах безопасности, процедуры управления инцидентами и действия по восстановлению.

В.2.4.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_INC.1: описание формальной процедуры сообщения об инцидентах, процедур управления инцидентами и действий по восстановлению с конкретными действиями и спецификациями (детализацией) и записи сообщений об инцидентах безопасности и их управлении.

В.2.4.4 FOD_INC.1 Инциденты безопасности

Зависимости: FOM_INC.1 Сообщение об обнаруженных проблемах безопасности.

FOD_ORG.2 Обязанности собрания руководства.

FOD_INC.1.1 ОФБ должны определять процедуры формального сообщения об инцидентах безопасности совместно с процедурой реагирования на инциденты, намечая действия по принятию сообщения об инциденте.

FOD_INC.1.2 ОФБ должны установить требования безопасности, контактный пункт, в который может обратиться лицо, желающее сообщить об инциденте.

FOD_INC.1.3 ОФБ должны определять процедуры управления инцидентами для обработки потенциальных типов инцидента безопасности, включая отказы системы и невыполненное обслуживание, вирусы и другие виды злоумышленного кода, отказ в обслуживании, ошибки в результате неполной или неточной деловой информации, нарушения конфиденциальности, целостности, подотчетности, аутентичности, надежности или частной жизни и неправильное использование информационных систем.

FOD_INC.1.4 ОФБ должны определять требования безопасности для действий по восстановлению после нарушений безопасности и устранению отказов системы.

FOD_INC.1.5 ОФБ должны определять требования безопасности по регистрации отказов, о которых сообщили пользователи, относительно проблем с обработкой информации и системами связи.

FOD_INC.1.6 ОФБ должны определять процедуры, посредством которых необходимо как можно скорее сообщать об инцидентах безопасности по соответствующим каналам управления.

FOD_INC.1.7 ОФБ должны определять правила обеспечения осведомленности всех служащих, подрядчиков и пользователей третьей стороны информационными системами и услугами о процедуре сообщения об инцидентах безопасности и точке контакта.

FOD_INC.1.8 ОФБ должны определять правила, по которым от всех служащих, подрядчиков и пользователей третьей стороны требуется сообщать о любых наблюдаемых или заподозренных слабых местах в системе безопасности различных систем или услуг.

FOD_INC.1.9 ОФБ должны определять обязанности и процедуры для руководства по обеспечению быстрого, эффективного и организованного реагирования на инциденты информационной безопасности.

FOD_INC.1.10 ОФБ должны определять механизмы, позволяющие определять число типов, масштабов инцидентов информационной безопасности и расходы на них, и контролировать их.

FOD_INC.1.11 ОФБ должны определять требования безопасности для случаев, когда дополнительное расследование, направленное против лица или организации после инцидента информационной безопасности, включает в себя правовое действие (гражданский или уголовный иск) и сбор свидетельств, которые сохраняются и предоставляются в соответствии с правилами для свидетельств, изложенными в сответствующей юрисдикции.

В.2.5 Администрирование организации безопасности (FOD_ORG)

В.2.5.1 Характеристика семейства

Данное семейство определяет администрирование организации безопасности и включает в себя подробное изложение заседания руководства.

В.2.5.2 Ранжирование компонентов

FOD_ORG.1 Обязанности по координации безопасности

Определены обязанности по координации безопасности.

FOD_ORG.2 Обязанности заседания руководства

Определены обязанности заседания руководства.

В.2.5.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_ORG.1: описание обязанностей по координации безопасности с конкретными действиями и детализацией.

Для FOD_ORG.2: описание обязанностей заседания руководства с конкретными действиями и детализацией.

B.2.5.4 FOD_ORG.1 Ответственность за координацию безопасности

Зависимости: зависимости отсутствуют.

FOD_ORG.1.1 ОФБ должны определять обязанности по координации действий по обеспечению информационной безопасности представителями различных подразделений организации с соответствующими должностными обязанностями.

FOD_ORG.1.2 ОФБ должны определять требования безопасности поддержания соответствующих контактов с релевантными органами управления (власти).

FOD_ORG.1.3 ОФБ должны определять требования безопасности поддержания соответствующих контактов со специальными группами по интересам или другими форумами специалистов по безопасности и профессиональными объединениями.

B.2.5.5 FOD_ORG.2 Обязанности заседания руководства

Зависимости: зависимости отсутствуют.

FOD_ORG.2.1 ОФБ должны определять обязанности заседания руководства, занимающегося вопросами безопасности.

FOD_ORG.2.2 ОФБ должны определять требования, предъявляемые к заседанию руководства по обеспечению выполнения действий, связанных с безопасностью, в соответствии с политикой информационной безопасности; по утверждению методологий и процессов, связанных с информационной безопасностью, идентификации изменений угроз и подверженности информации и средств обработки информации угрозам, оценке адекватности и координации средств обеспечения информационной безопасности.

B.2.6 Администрирование соглашений об услугах (FOD_SER)

B.2.6.1 Характеристика семейства

Данное семейство определяет соглашения об услугах относительно администрирования безопасности и включает в себя детализацию требований безопасности сетевых услуг.

B.2.6.2 Ранжирование компонентов

FOD_SER.1 Договоры по сетевым услугам. Определены характеристики безопасности, уровни безопасности и требования управления сетевыми услугами.

B.2.6.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_SER.1: описание характеристик безопасности, уровней безопасности и требований управления сетевыми услугами.

B.2.6.4 FOD_SER.1 Договоры по сетевым услугам

Зависимости: FOS_NET.1 Сетевые услуги.

FOD_SER.1.1 ОФБ должны определять требования безопасности по идентификации характеристик безопасности, уровней безопасности и требований управления всеми сетевыми услугами и включению их в договор по сетевым услугам.

FOD_SER.1.2 ОФБ должны определять требования безопасности в отношении способности провайдера сетевых услуг управлять согласованными услугами безопасным образом и соглашения о праве на аудит.

FOD_SER.1.2 ОФБ должны устанавливать соглашения по обмену информацией и программным обеспечением между организацией и внешними сторонами.

B.3 Системы ИТ: Класс FOS

Данный класс определяет требования к организационным мерам для систем ИТ в автоматизированной системе.

B.3.1 Политика для систем ИТ (FOS_POL)

B.3.1.1 Характеристика семейства

Данное семейство определяет политики безопасности для систем ИТ в автоматизированной системе и включает в себя детализацию требований безопасности, управление изменениями, контроль за вредоносными кодами и криптографию.

B.3.1.2 Ранжирование компонентов

FOS_POL.1 Требования безопасности

Определены процедуры управления обновлением и идентификацией изменений, управления изменениями и введения измененной системы.

FOS_POL.2 Политика вредоносных кодов

Определены процедуры управления при работе с вредоносными кодами.

FOS_POL.3 Политика мобильных кодов

Определены процедуры управления при работе с мобильными кодами.

FOS_POL.4 Криптографическая политика

Определены процедуры использования криптографических методов и процедуры назначения криптографических ключей.

FOS_POL.5 Общедоступные системы

Определены процедуры защиты общедоступных систем.

B.3.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_POL.1: описание требований безопасности и управленческих мер с изменениями с конкретными действиями, спецификациями и записями об осуществлении управления.

Для FOS_POL.2: описание процедур управления при работе с вредоносными кодами с конкретными действиями, спецификациями и записями об осуществлении контроля за вредоносными кодами.

Для FOS_POL.3: описание процедур управления при работе с мобильными кодами с конкретными действиями, спецификациями и записями об осуществлении контроля за мобильными кодами.

Для FOS_POL.4: описание политики использования криптографических методов и записей по проведению криптографического контроля.

Для FOS_POL.5:описание процедур защиты общедоступных систем с конкретными действиями, спецификациями и записями по проведению контроля.

B.3.1.4 FOS_POL.1 Требования безопасности

Зависимости: FOM_PRM.2 Разделение привилегий.

FOS_POL.1.1 ОФБ должны определять процедуры процесса управления обновлением программного обеспечения для обеспечения установки самых современных утвержденных патчей и приложений в санкционированное программное обеспечение.

FOS_POL.1.2 ОФБ должны определять процедуры идентификации изменений в средствах обработки информации и системах и оценки потенциальных воздействий.

FOS_POL.1.3 ОФБ должны определять процедуры формального контроля за изменениями для управления внедрением изменений в средства обработки информации и системы.

FOS_POL.1.4 ОФБ должны определять процедуры сохранения и копирования библиотек программных источников в соответствии с контролем за изменениями.

FOS_POL.1.5 ОФБ должны определять процедуры регулярных проверок информационных систем на соответствие стандартам внедрения безопасности.

FOS_POL.1.6 ОФБ должны излагать средства обеспечения безопасности в списках бизнес-требований для новых информационных систем или расширений имеющихся информационных систем.

FOS_POL.1.7 ОФБ должны определять процедуры управления установкой программного обеспечения в автоматизированные системы.

FOS_POL.1.8 ОФБ должны определять процедуры пересмотра и испытания критичных для бизнеса приложений при внесении изменений в операционные системы для обеспечения отсутствия отрицательного влияния на деятельность или безопасность организации.

FOS_POL.1.9 ОФБ должны определять правила препятствования модифицированию пакетов программ, ограничиваясь необходимыми изменениями при условии строгого контроля за ними.

FOS_POL.1.10 ОФБ должны документировать, сохранять и предоставлять процедуры всем нуждающимся в них пользователям.

B.3.1.5 FOS_POL.2. Политика защиты от вредоносных кодов

Зависимости: зависимости отсутствуют.

FOS_POL.2.1 ОФБ должны определять процедуры управления защитой систем от вредоносных кодов, сообщения об их восстановлении после атак вредоносных кодов.

FOS_POL.2.2 ОФБ должны определять процедуры обнаружения и защиты от вредоносных кодов, которые могут быть переданы посредством средств связи.

FOS_POL.2.3 ОФБ должны определять обязанности по защите систем от вредоносных кодов, обучению в их применении и восстановлению после атак вредоносных кодов.

FOS_POL.2.4 ОФБ должны определять процедуры реализации управленческих мер обнаружением, предотвращением и восстановлением для защиты от вредоносных кодов и осведомленности соответствующих пользователей.

B.3.1.6 FOS_POL.3 Политика защиты от мобильных кодов

Зависимости: зависимости отсутствуют.

FOS_POL.3.1 ОФБ должны определять процедуры управления санкционированием использования мобильного кода.

FOS_POL.3.2 ОФБ должны определять требования безопасности к конфигурации мобильного кода для обеспечения функционирования санкционированного мобильного кода в соответствии с четко определенной политикой безопасности и предотвращения реализации несанкционированного мобильного кода.

B.3.1.7 FOS_POL.4 Политика в области криптографии

Зависимости: зависимости отсутствуют.

FOS_POL.4.1 ОФБ должны определять криптографическую политику использования криптографических мер обеспечения безопасности для защиты информации в соответствии с релевантными соглашениями, законами и положениями.

FOS_POL.4.2 ОФБ должны определять криптографическую политику использования криптографических мер обеспечения безопасности для защиты информации.

FOS_POL.4.3 ОФБ должны определять процедуры назначения ключей для поддержки использования организацией криптографических методов.

FOS_POL.4.4 ОФБ должны определять требования безопасности к проведению юридической консультации перед перемещением зашифрованной информации или криптографических средств управления в другую страну.

FOS_POL.4.5 ФБС должны обеспечивать меры обеспечения безопасности хранения любых криптографических ключей, связанных с зашифрованными архивами или цифровыми подписями, и, при необходимости, предоставления их санкционированным лицам.

B.3.1.8 FOS_POL.5 Общественные системы

Зависимости: зависимости отсутствуют.

FOS_POL.5.1 ФБС должны обеспечивать меры безопасности для защиты программного обеспечения, данных и другой информации, требующей высокого уровня целостности при предоставлении в общедоступной системе.

FOS_POL.5.2 ОФБ должны обеспечивать требования безопасности по тестированию общедоступной системы на предмет наличия слабых мест и отказов перед предоставлением информации.

FOS_POL.5.3 ФБС должны обеспечивать требования безопасности по наличию формального процесса утверждения перед опубликованием информации.

FOS_POL.5.4 ФБС должны обеспечивать требования безопасности по проверке и утверждению всех входных данных.

B.3.2 Конфигурация систем ИТ (FOS_CNF)

B.3.2.1 Характеристика семейства

Данное семейство определяет конфигурацию системы ИТ и включает в себя разделение среды разработки и среды эксплуатации и конфигурацию системы.

B.3.2.2 Ранжирование компонентов

FOS_CNF.1 Разделение среды разработки и среды эксплуатации

Определены разделение среды разработки и среды эксплуатации и управление доступом.

FOS_CNF.2 Конфигурация системы

Определены управление разделяемыми ресурсами и конфигурация системы.

B.3.2.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_CNF.1: описание разделения среды разработки и среды эксплуатации с конкретными действиями, спецификациями и записями об осуществлении контроля.

Для FOS_CNF.2: описание управления разделяемыми ресурсами и конфигурации системы с конкретными действиями, спецификациями и записями об осуществлении контроля.

B.3.2.4 FOS_CNF.1 Разделение среды разработки и среды эксплуатации

Зависимости: зависимости отсутствуют.

FOS_CNF.1.1 ОФБ должны определять правила разделения по уровням, которые необходимы между средами эксплуатации, испытания и разработки для предотвращения проблем с эксплуатацией.

FOS_CNF.1.2 ОФБ должны определять [задача: правила] перевод программного обеспечения из состояния разработки в эксплуатационное состояние.

FOS_CNF.1.3 ФБС должны обеспечивать управленческие меры доступа, применимые к автоматизированным прикладным системам и тестовым прикладным системам с целью защиты эксплуатационных данных.

FOS_CNF.1.4 ФБС должны обеспечивать управленческие меры ограничениями для вспомогательного персонала, занимающегося ИТ, по доступу к библиотекам программных источников.

FOS_CNF.1.5 ОФБ должны определять правила для инструментального и системного программного обеспечения, работающего в различных системах или процессорах.

FOS_CNF.1.6 ОФБ должны определять правила копирования оперативной информации в тестовую прикладную систему.

B.3.2.5 FOS_CNF.2 Конфигурация системы

Зависимости: зависимости отсутствуют.

FOS_CNF.2.1 ОФБ должны определять правила разделения групп информационных услуг, пользователей и информационных систем на сети.

FOS_CNF.2.2 При необходимости применения конфиденциальной прикладной программы в совместно используемой среде ОФБ должны определить правила идентификации прикладных систем, с которыми она будет делить ресурсы с владельцем конфиденциальной прикладной программы.

FOS_CNF.2.3 ОФБ должны определять правила владения конфиденциальной системой специализированной (изолированной) вычислительной среды.

B.3.3 Сетевая безопасность систем ИТ (FOS_NET)

B.3.3.1 Характеристика семейства

Данное семейство определяет сетевую безопасность систем ИТ и включает в себя детализацию безопасности сетей и сетевых услуг.

B.3.3.2 Ранжирование компонентов

FOS_NET.1 Сетевые услуги

Определены сетевые услуги и доступ к ним.

FOS_NET.2 Безопасность сетей

Определены защита сетей, безопасность информации в сетях, конфиденциальности и целостности передаваемых данных.

B.3.3.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_NET.1: описание сетевых услуг с конкретными действиями и спецификациями и записи о доступе к сети.

Для FOS_NET.2: описание защиты сетей, безопасность информации в сетях с конкретными действиями и спецификациями и записи о контроле.

B.3.3.4 FOS_NET.1 Сетевые услуги

Зависимости: зависимости отсутствуют.

FOS_NET.1.1 ОФБ должны определять правила для сетей и сетевых услуг, к которым разрешен доступ, и правила процедур авторизации для определения, кому и к каким сетям и сетевым услугам разрешен доступ.

B.3.3.5 FOS_NET.2 Безопасность сетей

Зависимости: зависимости отсутствуют.

FOS_NET.2.1 ФБС должны обеспечить меры обеспечения безопасности для закрытия неактивных сеансов в местах высокого риска после определенного периода бездействия.

FOS_NET.2.2 ФБС должны обеспечить меры безопасности для очистки экрана терминала и закрытия как сеансов прикладных программ, так и сетевых сеансов после определенного периода бездействия простаивающего оборудования.

FOS_NET.2.3 ФБС должны обеспечить меры обеспечения безопасности для наложения ограничений на время соединения с целью дополнительной защиты приложений с высокой степенью риска.

FOS_NET.2.4 ФБС должны обеспечить меры связывания прав доступа к сетям с определенным временем или датами.

FOS_NET.2.5 ФБС должны обеспечить меры обеспечения безопасности для разделения групп информационных услуг, пользователей и информационных систем в сетях.

FOS_NET.2.6 ФБС должны обеспечить меры обеспечения безопасности по ограничению возможности пользователей подсоединяться к одной из совместно используемых сетей, особенно сетей, выходящих за пределы организации, параллельно с политикой управления доступом и требованиями бизнес-приложений.

FOS_NET.2.7 ФБС должны обеспечить меры обеспечения безопасности для маршрутизации сетей во избежания нарушения политики управления доступом бизнес-приложений компьютерными соединениями и информационными потоками.

B.3.4 Мониторинг систем ИТ (FOS_MON)

B.3.4.1 Характеристика семейства

Данное семейство определяет мониторинг систем ИТ и включает в себя детализацию требований к журналу аудита, юридической консультации, тревоге и мониторингу.

B.3.4.2 Ранжирование компонентов

FOS_MON.1 Журналы аудита

Определены требования к аудиту, управление аудитом, результаты аудита, информация, записанная в журнале, и регистрация системного администратора.

FOS_MON.2 Юридическая консультация

Определена юридическая консультация перед реализацией процедур мониторинга.

FOS_MON.3 Требования к тревоге

Определены установки параметров тревоги и реакция на тревогу.

FOS_MON.4 Определен мониторинг использования системы.

B.3.4.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_MON.1: подробное описание процедур ведения журналов аудита с конкретными действиями и спецификациями и записей журналов аудита.

Для FOS_MON.2: описание юридической консультации с конкретными действиями и спецификациями.

Для FOS_MON.3: описание установок параметров тревоги и записей о реакциях на тревогу с конкретными действиями и спецификациями и записи об осуществлении контроля.

Для FOS_MON.4: описание процедур проверки действий по мониторингу с конкретными действиями и спецификациями и записи об осуществлении проверок.

B.3.4.4 FOS_MON.1 Журналы аудита

Зависимости: зависимости отсутствуют.

FOS_MON.1.1 ОФБ должны планировать требования безопасности по аудиту и действиям, включающим в себя проверку автоматизированных систем, и согласовывать минимизацию риска прерывания бизнес-операций.

FOS_MON.1.2 ОФБ должны определять требования безопасности по аудиту соответствующим руководством.

FOS_MON.1.3 ОФБ должны осуществлять регистрацию системного администратора и действий системного оператора. Записи должны включать в себя время, когда произошло событие или отказ, информацию о событии

или отказе, какой клиент и какой администратор или оператор принимали в этом участие, изменения, внесенные в оборудование, программное обеспечение или процедуры.

FOS_MON.1.4 ОФБ должны определять правила регистрации выхода и входа в оборудование после возвращения.

FOS_MON.1.5 ОФБ должны определять требования безопасности регистрации копирования и использования оперативной информации для обеспечения следов аудита.

FOS_MON.1.6 ОФБ должны определять процедуры сбора следов аудита и аналогичных свидетельств.

FOS_MON.1.7 ОФБ должны определять требования безопасности к регистрации удаления всех съемных носителей информации из организации для сохранения записи аудита.

FOS_MON.1.8 ОФБ должны устанавливать процедуры мониторинга использования средств обработки информации и для регулярного анализа результатов действий по мониторингу.

FOS_MON.1.9 ФБС должны обеспечивать меры обеспечения безопасности для защиты средств регистрации и информации в журнале от фальсификации и несанкционированного доступа.

FOS_MON.1.10 ФБС должны осуществлять процедуры регистрации отказов, их анализа и действий, предпринятых для их устранения.

B.3.4.5 FOS_MON.2 Юридическая консультация

Зависимости: зависимости отсутствуют.

FOS_MON.2.1 ОФБ должны определять правила принятия юридической консультации перед реализацией процедур мониторинга.

B.3.4.6 FOS_MON.3 Требования к объявлению тревоги

Зависимости: зависимости отсутствуют.

FOS_MON.3.1 ФБС должны обеспечивать меры объявления тревоги для автоматизированной системы.

FOS_MON.3.2 ФБС должны обеспечивать возможности установки параметров предупредительного сигнала, предварительного определения аварийного события и внесения изменений в настройки аварийной сигнализации автоматизированной системы.

FOS_MON.3.3 ОФБ должны определять правила и процедуры действий по получении предупредительных сигналов, а также необходимых действий, включая любые ограничения по времени, задействование ответственных лиц и отчетность.

B.3.4.7 FOS_MON.4 Использование системы мониторинга

Зависимости: зависимости отсутствуют.

FOS_MON.4.1 ОФБ должны определять процедуры применения мониторинга для средств обработки информации и анализа результатов действий по мониторингу.

FOS_MON.4.2 ОФБ должны определять требования безопасности к тому, что степень мониторинга, требуемая для отдельного оборудования, определяется посредством оценки риска.

B.3.5 Управление персоналом системам ИТ (FOS_PSN)

B.3.5.1 Характеристика семейства

Данное семейство определяет меры управления персоналом систем ИТ и включает в себя подробное изложение авторизации пользователя, вредоносных кодов и средств использования системы.

B.3.5.2 Ранжирование компонентов

FOS_PSN.1 Авторизация пользователя

Определены регистрация и аутентификация пользователя и такие правила хранения информации об аутентификации, как применение секретных паролей.

FOS_PSN.2 Использование системы

Определены процедуры завершения активных сеансов.

B.3.5.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_PSN.1: описание регистрации пользователя, аутентификации пользователя и правил хранения конфиденциальной информации об аутентификации с конкретными действиями, спецификациями и записей об осуществлении контроля.

Для FOS_PSN.2: описание процедур завершения активных сеансов с конкретными действиями, спецификациями и записей об осуществлении контроля.

B.3.5.4 FOS_PSN.1 Аутентификация пользователя

Зависимости:

FOM_PRM.1 Разделение привилегий;

FOM_PRM.2 Роли и обязанности персонала;

FOM_PRM.3 Соглашение с персоналом.

FOS_PSN.1.1 ОФБ должны определять процедуры формальной регистрации пользователя и удаления записи из журнала предоставления и аннулирования доступа ко всем информационным системам и услугам.

FOS_PSN.1.2 ОФБ должны определять процедуры, включающие в себя использование уникальных идентификаторов пользователей для связывания этих пользователей со своими действиями и возложения на них ответственности за эти действия (применение групповых идентификаторов допускается только в случае их

пригодности для выполняемой работы), проверку авторизации пользователя владельцем системы на использование требуемой системы или услуги в процедуре управления доступом в пределах процесса регистрации и дерегистрации пользователя.

FOS_PSN.1.3 ОФБ должны определять процедуры выдачи временной аутентификационной информации после позитивной идентификации пользователя в случае, если пользователь забыл или утратил свою аутентификационную информацию. Временная аутентификационная информация должна передаваться пользователям безопасным способом.

FOS_PSN.1.4 ОФБ должны определять правила предотвращения утраты или компрометации аутентификационной информации, например, для избежания необходимости хранения записи паролей, если только ее нельзя запомнить безопасным образом: выбирают качественные пароли достаточно минимальной длины, не основанные на том, о чем можно легко догадаться или которые можно легко получить с помощью связанной с личностью информацией, регулярно меняют пароли или на основе числа доступов; избегают повторного использования или чередования старых паролей; изменяют временные пароли при первом входе в систему; не включают пароли в автоматизированный процесс входа в систему и не используют совместно индивидуальные пароли пользователей.

FOS_PSN.1.5 ОФБ должны определять правила подписания утверждения (оператора) для предотвращения утраты, компрометации или неправильного использования аутентификационной информации, например, хранить секретные персональные пароли и пароли рабочей группы исключительно между членами группы (внутри группы).

FOS_PSN.1.6 ФБС должны предусматривать меры предоставления пользователям на начальной стадии надежной (защищенной) временной аутентификационной информации, которую они вынуждены изменить или подтвердить немедленно.

FOS_PSN.1.7 ОФБ должны определять правила постоянного хранения информации об аутентификации пользователя в защищенном виде.

FOS_PSN.1.8 ОФБ должны определять формальный процесс управления для контроля за назначением аутентификационных данных среди пользователей.

B.3.5.5 FOS_PSN.2 Использование системы

Зависимости: зависимости отсутствуют.

FOS_PSN.2.1 ОФБ должны определять процедуры прекращения активных сеансов после их окончания, если только их нельзя защитить соответствующим блокирующим механизмом.

FOS_PSN.2.2 ОФБ должны определять процедуры отключения универсальных ЭВМ, серверов или офисных ПК по завершении сеанса работы.

FOS_PSN.2.3 ОФБ должны определять правила применения различных профилей пользователей для автоматизированных и испытательных систем и меню.

FOS_PSN.2.4 ОФБ должны определять правила, предписывающие не оставлять персональные компьютеры, компьютерные терминалы и принтеры, подсоединенные к сети, без присмотра и защищать их при помощи фиксаторов клавиш, паролей или других средств защиты во время простоя этих устройств.

B.3.6 Активы систем информационных технологий в автоматизированных системах (FOS_OAS)

B.3.6.1 Характеристика семейства

Данное семейство определяет безопасность операционных активов систем ИТ и включает в себя подробное изложение защиты операционных активов, системных программ, вспомогательной и аутентификационной информации.

B.3.6.2 Ранжирование компонентов

FOS_OAS.1 Защита операционных активов

Определены стирание оперативной информации, управление доступом и безопасное хранение системной документации. Определены критерии приемки новых систем, правила использования обслуживающей программы, процедуры аутентификации обслуживающих программ, процедуры обновления системного программного обеспечения, правила неприменения несанкционированного программного обеспечения и ответственность за отслеживание выпуска поставщиком патчей.

FOS_OAS.2 Процедуры поддержки

Описаны процедуры резервного копирования информации и программного обеспечения.

B.3.6.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_OAS.1: описание стирания оперативной информации, управления доступом и безопасного хранения системной документации с конкретными действиями и спецификациями и записей о проведении контроля. Описание критериев приемки новых систем, правил использования обслуживающей программы, процедур аутентификации обслуживающих программ, процедур обновления системного программного обеспечения, правил неприменения несанкционированного программного обеспечения и ответственности за отслеживание выпуска поставщиком патчей с конкретными действиями и спецификациями и записей о проведении контроля.

Для FOS_OAS.2: описание процедур резервного копирования информации и программного обеспечения с конкретными действиями и спецификациями и записей о проведении контроля.

B.3.6.4 FOS_OAS.1 Защита операционных активов

Зависимости: FOS_POL.1 Требования безопасности.

FOS_OAS.1.1 ОФБ должны определять правила стирания оперативной информации из испытательной прикладной системы сразу после завершения испытаний.

FOS_OAS.1.2 ОФБ должны определять требования безопасности для управления распечатками программ в безопасной среде.

FOS_OAS.1.3 ФБС должны обеспечивать меры защиты системной документации от несанкционированного доступа и меры ее безопасного хранения.

FOS_OAS.1.4 ФБС должны обеспечивать средства управления для предотвращения доступа к компилирующим программам, программам редактирования и другим средствам разработки из автоматизированных систем.

FOS_OAS.1.5 ОФБ должны определять критерии приемки для новых и модернизированных информационных систем и новых версий, предназначенных для приемки, а также соответствующих испытаний, проводимых во время разработки перед приемкой.

FOS_OAS.1.6 ОФБ должны определять требования безопасности для обнаружения, предупреждения и восстановления с целью защиты от вредоносных кодов и утечки информации.

FOS_OAS.1.7 ОФБ должны определять правила ограничения и управления применением обслуживающих программ, которые могут заменять управленческие меры системой и приложениями.

FOS_OAS.1.8 ФБС должны обеспечивать управленческие меры аутентификацией обслуживающих программ системы, разделением обслуживающих программ системы от прикладного программного обеспечения, ограничением использования обслуживающих программ системы минимальным практическим числом доверенных санкционированных программ.

FOS_OAS.1.9 ОФБ должны определять процедуры обновления системного программного обеспечения, приложений и библиотек программ опытными администраторами, санкционированными соответствующим руководством.

FOS_OAS.1.10 ОФБ должны определять правила хранения в автоматизированной системе только исполнимого кода.

FOS_OAS.1.11 ОФБ должны определять правила внедрения приложений и программного обеспечения операционных систем после всесторонних и успешных испытаний.

FOS_OAS.1.12 ОФБ должны определять правила предоставления физического или логического доступа поставщикам только для вспомогательных целей, при необходимости и с разрешения руководства.

FOS_OAS.1.13 ОФБ должны определять правила неприменения несанкционированного программного обеспечения.

FOS_OAS.1.14 ОФБ должны определять ответственность за отслеживание выпуска поставщиком патчей и фиксаторов для прикладных программ.

FOS_OAS.1.15 ОФБ должны определять процедуры модернизации до получения нового варианта с учетом его безопасности, внедрения новых функций безопасности или числа и сложности проблем, влияющих на модернизируемый вариант.

FOS_OAS.1.16 ОФБ должны определять правила приемлемого использования информации и активов, связанных со средствами обработки информации, предназначенных для идентификации, документирования и внедрения.

B.3.6.5 FOS_OAS.2 Вспомогательные процедуры

Зависимости: зависимости отсутствуют.

FOS_OAS.2.1 ФБС должны обеспечивать процедуры регулярной проверки резервных копий информации и программного обеспечения в соответствии с согласованной политикой дублирования.

FOS_OAS.2.2 ОФБ должны определять процедуры выдачи необходимого уровня вспомогательной информации наряду с точными и полными записями резервных копий и документированных процедур восстановления.

FOS_OAS.2.3 ОФБ должны определять процедуры для выбора носителей резервных копий для обеспечения их надежности в случае аварийного использования.

FOS_OAS.2.4 ОФБ должны обеспечивать эффективность процедур и их завершение за время, отведенное в последовательности операций на восстановление.

FOS_OAS.2.5 ОФБ должны определять требования безопасности для резервной компоновки отдельных систем для обеспечения их соответствия требованиям планов обеспечения непрерывности деловой деятельности.

B.3.7 Протоколирование в системах ИТ (FOS_RCD)

B.3.7.1 Характеристика семейства

Данное семейство определяет записи, которые должны сохраняться для систем ИТ, и включает в себя подробное описание записей.

B.3.7.2 Ранжирование компонентов

FOS_RCD.1 Записи

Определена регистрация всех предполагаемых отказов.

B.3.7.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOS_RCD.1: описание всех предполагаемых отказов с конкретными действиями, спецификациями и записями по проведению контроля.

В.3.7.4 FOS_RCD.1 Записи

Зависимости: зависимости отсутствуют.

FOS_RCD.1.1 ФБС должны обеспечивать меры регистрации всех предполагаемых или фактических отказов и восстановительного ремонта оборудования.

В.4 Класс FOA: Активы пользователя

В данном классе представлены требования оперативного управления активами пользователя автоматизированной системы.

В.4.1 Защита приватных данных (FOA_PRO)

В.4.1.1 Характеристика семейства

Данное семейство определяет политику в отношении активов пользователей и включает в себя детальное изложение приватных данных, криптографию, управление активами, роли и обязанности пользователей.

В.4.1.2 Ранжирование компонентов

FOA_PRO.1 Персональные данные. Определены правила неприменения оперативных баз данных, содержащих персональную информацию, для испытаний, правила получения общедоступной информации в соответствии с законодательством о защите данных и обязанности владельца данных по информированию санкционированного должностного лица организации, ответственного за защиту данных.

В.4.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOA_PRO.1: описание правил неприменения баз персональных данных, содержащих персональную информацию, правила получения общедоступной информации в соответствии с политикой безопасности законодательства о защите данных, обязанности владельца данных по информированию санкционированного должностного лица организации, ответственного за защиту данных, с конкретными действиями и спецификациями и записями о проведении контроля.

В.4.1.4 FOA_PRO.1 Данные о частной жизни

Зависимости: зависимости отсутствуют.

FOA_PRO.1.1 ОФБ должны определять правила неприменения оперативных баз данных, содержащих персональную информацию, для испытательных целей.

FOA_PRO.1.2 ОФБ должны определять правила получения общедоступной информации в соответствии с законодательством о защите данных, полной, точной и своевременной обработки информации и для ее защиты в процессе сбора и при хранении.

FOA_PRO.1.3 ОФБ должны определять обязательства и правила для владельца данных по информированию санкционированного должностного лица организации, ответственного за защиту данных, о любых предложениях по хранению персональной информации и обеспечению осведомленности о принципах защиты данных, определенных в соответствующем законодательстве.

В.4.2 Защита информации в активах пользователей (FOA_INF)

В.4.2.1 Характеристика семейства

Данное семейство определяет защиту информации в активах пользователей и включает в себя защиту данных, процедуры и правила.

В.4.2.2 Ранжирование компонентов

FOA_INF.1: руководства по удержанию передаваемых данных, процедуры разрешения на соответствующее уничтожение записей и обеспечения безопасности для электронных коммуникаций с конкретными действиями и спецификациями. Описание процедур маркирования и обработки информации с конкретными действиями и спецификациями и записей о проведении контроля.

В.4.2.3 FOA_INF.1 Защита данных

Зависимости: FOS_POL.1 Требования безопасности.

FOA_INF.1.1 ОФБ должны определять руководства по удержанию, сохранению, обработке и ликвидации записей и информации.

FOA_INF.1.2 ОФБ должны определять правила планирования удержания, определяющего необходимые типы записей и период времени их удержания.

FOA_INF.1.3 ОФБ должны определять процедуры разрешения соответствующего уничтожения записей после этого периода, если они не нужны организации.

FOA_INF.1.4 ФБС должны обеспечивать меры обязательного уничтожения, стирания или перезаписи с помощью методов, утвержденных для устройств, содержащих секретную информацию.

FOA_INF.1.5 ФБС должны обеспечивать меры обеспечения электронной связи путем защиты сообщений от несанкционированного доступа, модификации или отказа в обслуживании, обеспечения правильной адресации и передачи сообщения, надежности и доступности услуг и юридической консультации.

FOA_INF.1.6 ОФБ должны определять процедуры маркировки и обработки информации, включая как физический, так и электронный форматы в соответствии со схемой классификации, принятой организацией.

FOA_INF.1.7 ОФБ должны определять правила определения привилегий, связанных с каждым продуктом системы и каждым приложением, и категорий персонала, к которому они должны быть отнесены.

FOA_INF.1.8 ОФБ должны определять правила назначения привилегий пользователям на основе «необходимости для использования» и по ходу возникновения событий в соответствии с политикой управления доступом.

FOA_INF.1.9 ОФБ должны определять требования безопасности по защите информации, задействованной в электронной коммерции, проходящей по общественным сетям, от мошенничества, споров по контракту, а также от несанкционированного раскрытия и модифицирования.

B.5 Класс FOB: деловая деятельность

В данном классе определяются требования оперативного управления для использования автоматизированной системы в деловой деятельности.

B.5.1 Бизнес-политики (FOD_POL)

B.5.1.1 Характеристика семейства

Данное семейство определяет политики деловой деятельности и включает в себя подробное изложение требований безопасности и проблем с интеллектуальной собственностью.

B.5.1.2 Ранжирование компонентов

FOD_POL.1 Требования безопасности

Определены ценность задействованных информационных активов для бизнеса, требования безопасности для отдельных коммерческих применений, идентификация всей информации, относящейся к коммерческим применениям и безопасности, роли и обязанности по внедрению и поддержанию политик безопасности. Определены соответствующие процедуры обеспечения соответствия правовым ограничениям на использование материала.

B.5.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOD_POL.1: описание ценности задействованных информационных активов для бизнеса, требований безопасности для отдельных коммерческих применений, идентификации всей информации, относящейся к коммерческим применениям и безопасности и ролей и обязанностей по внедрению и поддержанию политик безопасности, соответствующие процедуры обеспечения соответствия правовым ограничениям на использование материала с конкретными действиями и записями по проведению управления.

B.5.1.4 FOD_POL.1 Требования безопасности

Зависимости: FOS_POL.1 Требования безопасности

FOD_POL.1.1 ОФБ должны обозначить политику безопасности для определения ценности системы и информационных активов, которые образуют часть общей системы, для бизнеса.

FOD_POL.1.2 ОФБ должны обозначить требования безопасности для отдельных коммерческих применений, идентификации всей информации, относящейся к коммерческим применениям, и рисков для информации, политик распространения и авторизации информации, соответствия между политиками управления доступом и классификации информации различных систем и сетей, релевантного законодательства и любых контрактных обязательств, относящихся к защите доступа к данным или услугам, управления правами доступа в распределенной и сетевой среде, которая распознает все имеющиеся типы соединений.

FOD_POL.1.3 ОФБ должны обозначить роли и обязанности по внедрению и поддержанию политик безопасности и защите актива.

FOD_POL.1.4 ОФБ должны обозначить роли и обязанности и их передачу претендентам на должность перед назначением.

FOD_POL.1.5 ОФБ должны обозначить процедуры обеспечения соответствия законодательным, регулятивным и контрактным требованиям к использованию материала, для которого могут существовать права на собственность, и к использованию специализированных программных изделий.

FOD_POL.1.6 ОФБ должны разрабатывать и внедрять политики и процедуры защиты информации, связанной с межсоединениями коммерческих информационных систем.

B.5.2 Непрерывность бизнеса (FOB_BCN)

B.5.2.1 Характеристика семейства

Данное семейство определяет действия по обеспечению непрерывности деловой деятельности и включает в себя подробное описание анализа воздействия на бизнес, локализации неисправностей и планирования непрерывности деловой деятельности.

B.5.2.2 Ранжирование компонентов

FOB_BCN.1 Анализ воздействия

Определены анализ воздействия на непрерывность деловой деятельности, планы обеспечения непрерывности деловой деятельности для поддержания или восстановления деловых операций, локализация неисправностей и специальный доступ, предоставляемый во время сбоев при обеспечении безопасности.

B.5.2.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOB_BCN.1: описание анализа воздействия на непрерывность деловой деятельности, планов обеспечения непрерывности деловой деятельности для поддержания или восстановления деловых операций, локализации неисправностей и специального доступа, предоставляемого во время сбоев при обеспечении безопасности, с конкретными действиями и спецификациями.

B.5.2.4 FOB_BCN.1 Анализ воздействия

Зависимости: FOD_RSM.1 Менеджмент риска внутри организации.

FOB_BCN.1.1 ОФБ должны определять требования безопасности по проведению анализа воздействия на непрерывность деловой деятельности для идентификации событий, которые могут вызвать прерывания деловых процессов, наряду с анализом вероятности и воздействия таких прерываний и их последствий для информационной безопасности.

FOB_BCN.1.2 ОФБ должны определять требования безопасности к проведению анализа воздействия на непрерывность деловой деятельности с вовлечением владельцев бизнес-ресурсов и бизнес-процессов.

FOB_BCN.1.3 ОФБ должны определять требования безопасности к планам обеспечения непрерывности деловой деятельности для восстановления после атак вредоносных кодов, включая мероприятия по восстановлению и резервированию всех необходимых данных и программного обеспечения.

FOB_BCN.1.4 ОФБ должны определять требования безопасности к осознанию рисков, стоящих перед организацией, в отношении их вероятности и воздействия; пониманию влияния, которое прерывание может оказывать на деловую деятельность; формулированию и документированию стратегии обеспечения непрерывности деловой деятельности, согласующейся с установленными бизнес-целями и бизнес-приоритетами; формулированию и документированию планов обеспечения непрерывности деловой деятельности, соответствующих установленной стратегии, регулярному тестированию и обновлению текущих планов и процессов и к обеспечению включения управления непрерывностью бизнес-процессов организации, и к структуре ее обеспечения.

FOB_BCN.1.5 ОФБ должны определять требования безопасности к разработке и внедрению планов обеспечения непрерывности деловой деятельности для поддержания или восстановления операций и обеспечения доступности информации на необходимом уровне и в требуемых масштабах времени после прерывания или сбоя критически важных бизнес-процессов.

FOB_BCN.1.6 ОФБ должны определять процедуры хранения копии планов обеспечения непрерывности деловой деятельности в удаленном пункте на значительном удалении для избежания ущерба вследствие бедствия на главной территории организации. Необходимо обеспечить актуальность этих копий и их защиту на соответсвующем уровне безопасности, аналогичном уровню безопасности, установленному и на главной территории.

FOB_BCN.1.7 ОФБ должны определять требования безопасности для условий ее активации, а также лиц, ответственных за выполнение каждого пункта каждого плана обеспечения непрерывности деловой деятельности.

FOB_BCN.1.8 ОФБ должны определять требования безопасности к проверке и обновлению планов обеспечения непрерывности деловой деятельности для обеспечения их современности и эффективности.

FOB_BCN.1.9 ОФБ должны определять требования безопасности к планам локализации сбоев в обеспечении безопасности с тем, чтобы сбой оказывал минимальное воздействие на непрерывность деловой деятельности при возникновении инцидентов безопасности.

FOB_BCN.1.10 ОФБ должны определять правила специального доступа к активам автоматизированной системы во время сбоев в обеспечении безопасности.

FOB_BCN.1.11 ОФБ должны определять требования безопасности к разработке и поддержанию управляемого процесса непрерывности деловой деятельности во всей организации, который учитывает требования безопасности, необходимые для сохранения непрерывности деловой деятельности организации.

FOB_BCN.1.12 ОФБ должны определять требования безопасности для единой схемы планов обеспечения непрерывности деловой деятельности с целью обеспечения последовательности всех планов, постоянного учета требований информационной безопасности и определения приоритетов для проверки и обслуживания.

B.6 Класс FOP: оборудование и аппаратура

В данном классе представлены требования к организационным мерам для оборудования, аппаратуры и помещений в пределах автоматизированной системы.

B.6.1 Передвижное оборудование (FOP_MOB)

B.6.1.1 Характеристика семейства

В данном семействе определены требования безопасности для передвижного оборудования и включают в себя подробное изложение требований безопасности, ролей и обязанностей.

B.6.1.2 Ранжирование компонентов

FOP_MOB.1 Требования безопасности для передвижного оборудования. Определены требования физической защиты и процедур принятия мер обеспечения безопасности при использовании передвижной вычислительной аппаратуры в общественных местах. Определены правила использования средств обработки персональной информации и информации частного пользования и правила применения полностью автоматизированного оборудования.

B.6.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOP_MOB.1: описание требований физической защиты и процедур принятия мер обеспечения безопасности при использовании передвижной вычислительной аппаратуры в общественных местах с конкретными действиями и спецификациями. Описание правила использования средств обработки персональной информации и информации частного пользования и правила применения полностью автоматизированного оборудования с конкретными действиями и спецификациями и записями о проведении контроля.

В.6.1.4 FOP_MOB.1 Требования безопасности для передвижного оборудования

FOP_MOB.1.1 ОФБ должны определять требования безопасности в политике для переносной вычислительной техники в отношении рисков работы с переносным вычислительным оборудованием в незащищенных средах.

FOP_MOB.1.2 ОФБ должны определять требования безопасности для физической защиты, управления доступом, криптографических методов и средств, резервного копирования и защиты от вирусов в политике для передвижной вычислительной техники.

FOP_MOB.1.3 ФБС должны обеспечить меры защиты от рисков при использовании передвижной вычислительной аппаратуры.

FOP_MOB.1.4 ОФБ должны определять процедуры принятия мер обеспечения безопасности при использовании передвижной вычислительной аппаратуры в общественных местах, совещательных комнатах и других незащищенных доменах за пределами помещений организации. ОФБ должны обеспечивать соответствующую защиту использованию передвижной вычислительной аппаратуры, подсоединенной к сетям.

FOP_MOB.1.5 ФБС должны обеспечивать меры защиты передвижной вычислительной аппаратуры, особенно оставленной без присмотра, от хищений.

FOP_MOB.1.6 ОФБ должны определять правила использования средств обработки персональных данных и приватной информации при обработке деловой информации.

FOP_MOB.1.7 ОФБ должны определять правила, предписывающие не оставлять оборудование и носители информации без присмотра в общественных местах, переноски портативных компьютеров в качестве ручного багажа и скрывать их при совершении переездов.

В.6.2 Съемное оборудование (FOP_RMM)

В.6.2.1 Характеристика семейства

Данное семейство определяет процедуры безопасности для сменного оборудования и включает в себя подробное изложение управления сменными носителями.

В.6.2.2 Ранжирование компонентов

FOP_RMM.1 Управление сменными носителями

Описаны процедуры управления сменными компьютерными носителями, процедуры авторизации для носителей, удаленных из организации, и процедуры стирания содержимого любых повторно используемых носителей.

В.6.2.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOP_RMM.1: описание процедур управления сменными компьютерными носителями, процедур авторизации для носителей, удаленных из организации, и процедур стирания содержимого любых повторно используемых носителей с конкретными действиями и спецификациями и записями о проведении контроля.

В.6.2.4 FOP_RMM.1 Управление сменными носителями

Зависимости: зависимости отсутствуют.

FOP_RMM.1.1 ОФБ должны определять процедуры управления сменными компьютерными носителями.

FOP_RMM.1.2 ОФБ должны определять процедуры авторизации для носителей, удаленных из организации.

FOP_RMM.1.3 ОФБ должны определять процедуры минимизации рисков, связанных с утечкой секретной информации несанкционированным лицам, установления формальных процедур безопасной ликвидации носителей.

FOP_RMM.1.4 ОФБ должны определять процедуры стирания, включая любые секретные данные и лицензионное программное обеспечение, любых повторно используемых носителей и оборудования, содержащего носители информации, которые должны быть удалены из организации в случае их ненадобности и проверены на выполнение стирания.

В.6.3 Дистанционное оборудование (FOP_RMT)

В.6.3.1 Характеристика семейства

Данное семейство определяет процедуры безопасности и включает в себя подробное изложение управления дистанционным оборудованием.

В.6.3.2 Ранжирование компонентов

FOP_RMT.1 Управление дистанционным оборудованием

Определены обязанности и процедуры управления и использования дистанционного оборудования и процедуры дистанционного доступа к деловой информации.

В.6.3.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOP_RMT.1: описание обязанностей и процедуры управления и использования дистанционного оборудования и процедур дистанционного доступа к деловой информации с конкретными действиями и спецификациями и записями о проведении контроля.

В.6.3.4 FOP_RMT.1 Управление дистанционным оборудованием

Зависимости: зависимости отсутствуют.

FOP_RMT.1.1 ОФБ должны определять обязанности и процедуры управления оборудованием и его использования, включая оборудование на территории пользователя.

FOP_RMT.1.2 ОФБ должны определять процедуры осуществления дистанционного доступа к деловой информации через общедоступную сеть с помощью передвижной вычислительной аппаратуры только после успешной идентификации и аутентификации и с применением соответствующих механизмов управления доступом.

FOP_RMT.1.3 ФБС должны обеспечивать меры блокировки клавиатуры или эквивалентные меры обеспечения безопасности для защиты ПК или терминалов от несанкционированного доступа.

FOP_RMT.1.4 ФБС должны обеспечивать меры автоматической идентификации оборудования как средства аутентификации соединений из специфических местоположений оборудования.

FOP_RMT.1.5 ФБС должны обеспечивать управленческие меры физическим и логическим доступом к диагностическим и конфигурационным портам.

В.6.4 Системное оборудование (FOP_SYS)

В.6.4.1 Характеристика семейства

Данное семейство определяет процедуры безопасности для системного оборудования и включает в себя подробное изложение управления системным оборудованием.

В.6.4.2 Ранжирование компонентов

FOP_SYS.1 Управление системным оборудованием

Определены запасное оборудование и резервные носители, правила хранения опасных и воспламеняющихся материалов. Процедуры проверки поступающего материала и защиты сетевой проводки с конкретными действиями и спецификациями.

В.6.4.3 FOP_SYS.1 Управление системным оборудованием

Зависимости: зависимости отсутствуют.

FOP_SYS.1.1 ОФБ должны определять правила размещения запасного оборудования и резервных носителей на безопасном расстоянии для избежания ущерба, причиненного бедствием на главной территории.

FOP_SYS.1.2 ОФБ должны определять правила хранения опасных и воспламеняющихся материалов безопасным образом на безопасном расстоянии на защищенном участке.

FOP_SYS.1.3 ОФБ должны определять правила хранения каталогов внутренних телефонных справочников, указывающих местоположение оборудования для обработки секретной информации, недоступной для общественности.

FOP_SYS.1.4 ОФБ должны определять процедуры проверки поступающего материала на наличие потенциальных угроз перед его перемещением от района доставки и разгрузки к месту использования.

FOP_SYS.1.5 ФБС должны обеспечить меры защиты сетевой проводки от несанкционированного прослушивания или повреждения при ее прокладке через площади общественного пользования.

FOP_SYS.1.6 ОФБ должны определять правила обслуживания оборудования в соответствии с рекомендованными поставщиком интервалами и спецификациями.

FOP_SYS.1.7 ОФБ должны определять правила проведения ремонта или обслуживания оборудования только санкционированным обслуживающим персоналом.

FOP_SYS.1.8 ОФБ должны определять управленческие меры для соответствующего уровня физической защиты и защиты от воздействия окружающей среды в соответствии со стандартами, применяемыми на главной территории для резервной информации. Меры обеспечения безопасности, применяемые к носителям на основной территории, должны быть распространены на резервную территорию.

FOP_SYS.1.9 ОФБ должны определять правила хранения всех носителей в безопасной и защищенной среде в соответствии со спецификацией изготовителей.

FOP_SYS.1.10 ОФБ должны определять обязанности по защите оборудования, работающего в автономном режиме для всех работников, подрядчиков и пользователей третьей стороны в отношении требований и процедур безопасности.

FOP_SYS.1.11 ОФБ должны определять процедуры обеспечения переноса всей релевантной информации в организацию и ее надежного стирания из оборудования в случае покупки оборудования организации работником, подрядчиком и пользователем третьей стороны или использования ими собственного оборудования.

FOP_SYS.1.12 ОФБ должны обеспечить меры обеспечения безопасности для носителей, содержащих информацию, которая должна быть защищена от несанкционированного доступа, неправильного использования или искажения во время транспортирования за пределами организации.

В.6.5 Управление аппаратурой (FOP_MNG)

В.6.5.1 Характеристика семейства

Данное семейство определяет управление аппаратурой и включает в себя физическую защиту, вспомогательное оборудование и каналы связи.

В.6.5.2 Ранжирование компонентов

FOP_MNG.1 Физическая защита

Определена физическая защита офисов, помещений и аппаратуры. Определено разделение аппаратуры, используемой для разработки, испытания и эксплуатации. Определены требования для адекватной резервной аппаратуры и защиты средств обработки информации.

FOP_MNG.2 Силовое вспомогательное оборудование

Определены управление вспомогательным оборудованием и применение резервного генератора.

FOP_MNG.3 Каналы связи

Определено управление внешними каналами связи.

В.6.5.3 Записи

Для FOP_MNG.1: описание физической защиты офисов, помещений и аппаратуры, разделения аппаратуры, используемой для разработки, испытания и эксплуатации, адекватной резервной аппаратуры и защиты средств обработки информации с конкретными действиями и спецификациями.

Для FOP_MNG.2: описание управления силовым вспомогательным оборудованием и применение резервного генератора с конкретными действиями и спецификациями.

Для FOP_MNG.3: описание управления каналами связи и мер по устранению неисправностей с конкретными действиями и спецификациями.

В.6.5.4 FOP_MNG.1 Физическая защита

Зависимости: FOD_PSN.5 Доступ к аппаратуре и оборудованию.

FOP_MNG.1.1 ОФБ должны определять требования безопасности для физической защиты офисов, других помещений и аппаратуры от ущерба вследствие пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других видов бедствий природных или антропогенных катастроф.

FOP_MNG.1.2 ОФБ должны определять требования безопасности разделения аппаратуры разработки, испытания и эксплуатации с целью снижения рисков несанкционированного доступа или внесения изменений в автоматизированную систему.

FOP_MNG.1.3 ОФБ должны определять требования безопасности для адекватной резервной аппаратуры в целях обеспечения возможности восстановления всей значимой информации и программного обеспечения после какого-либо бедствия или неисправности носителей информации.

FOP_MNG.1.4 ОФБ должны определять требования безопасности для защиты оборудования обработки информации с целью избежания несанкционированного доступа или раскрытия информации, хранящейся в этом оборудовании и обрабатываемой им.

В.6.5.5 FOP_MNG.2 Силовое вспомогательное оборудование

Зависимости: зависимости отсутствуют.

FOP_MNG.2.1 ФБС должны обеспечить меры обеспечения безопасности для защиты оборудования от перебоев в питании и других сбоев, вызванных неисправностями во вспомогательном оборудовании.

FOP_MNG.2.2 ОФБ должны определять требования безопасности для применения оборудования УПС.

FOP_MNG.2.3 ОФБ должны определять требования безопасности для применения резервного генератора при необходимости продолжения обработки информации в случае длительного перебоя в питании.

В.6.5.6 FOP_MNG.3 Каналы связи

Зависимости: зависимости отсутствуют.

FOP_MNG.3.1 ФБС должны обеспечить меры защиты силовой и телекоммуникационной проводки, передающей данные или предоставляющей вспомогательные информационные услуги, от прослушивания или повреждения.

FOP_MNG.3.2 ФБС должны определять требования безопасности при поддержании связности коммуникаций в случае неисправности аппаратуры связи или прерывания в его работе.

В.7 Класс 7: Третьи стороны

В данном классе представлены требования к организационным мерам для третьих сторон.

В.7.1 Управление взаимодействием с третьей стороной (FOT_MNG)

В.7.1.1 Характеристика семейства

Данное семейство определяет управление взаимодействием с третьей стороной и обязательства третьих сторон и включает в себя требования безопасности для аутсорсинга и третьих сторон.

В.7.1.2 Ранжирование компонентов

FOT_MNG.1 Аутсорсинг.

Определен план необходимых передач информации, лицензионных соглашений, владения кодами и прав на интеллектуальную собственность.

FOT_MNG.2 Требования безопасности для третьих сторон.

Определены все требования безопасности, являющиеся результатом работы с третьими сторонами. Определены достаточное общее управление и правила непредоставления доступа к информации организации. Определен менеджмент риска, применимый к взаимоотношениям с третьей стороной.

В.7.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства:

Для FOT_MNG.1: описание плана необходимых передач информации, лицензионных соглашений, владения кодами и прав на интеллектуальную собственность с конкретными действиями и спецификациями.

Для FOT_MNG.2: описание всех требований безопасности, проистекающих из работы с третьими сторонами, достаточного общего управления и правил непредоставления доступа к информации организации и менеджмента риска с конкретными действиями и спецификациями.

В.7.1.4 FOT_MNG.1 Аутсорсинг

Зависимости: FOD_PSN.3 Персональное соглашение.

FOT_MNG.1.1 ОФБ должны определять требования безопасности для плана необходимых передач информации, средств обработки информации и всего подлежащего перемещению и поддержанию безопасности во время периода передачи информации при мероприятиях аутсорсинга.

FOT_MNG.1.2 ОФБ должны определять требования безопасности для лицензионных соглашений, владения кодами и прав на интеллектуальную собственность, сертификации качества и точности выполняемой работы, мероприятий по условному депонированию в случае неудачи третьей стороны, прав доступа для аудита качества и точности проделанной работы, договорных требований к качеству кода и тестированию для обнаружения троянского кода там, где было разработано программное обеспечение.

B.7.1.5 FOT_MNG.1 Требования безопасности для третьей стороны

Зависимости: зависимости отсутствуют.

FOT_MNG.1.1 ОФБ должны определять требования безопасности, являющиеся результатом работы с третьими сторонами или внутрифирменными мерами контроля по согласованию с третьей стороной.

FOT_MNG.1.2 ОФБ должны определять требования безопасности для обеспечения соответствия политикам и стандартам безопасности организации по согласованию с третьими сторонами, включая доступ к информации организации, ее обработку, передачу или управление ею, или к средствам обработки информации.

FOT_MNG.1.3 ОФБ должны определять требования безопасности для достаточного общего контроля и аспектов безопасности для секретной или критически важной информации или средств обработки информации, доступ к которой осуществляется третьей стороной и которая обрабатывается или управляется третьей стороной.

FOT_MNG.1.4 ОФБ должны определять правила, предписывающие не предоставлять доступ к информации организациям третьей стороны, пока не будут определены меры обеспечения безопасности и подписано соглашение, определяющее условия подсоединения или доступа, и рабочее соглашение.

FOT_MNG.1.5 ОФБ должны определять требования безопасности для осуществления менеджмента рисками, связанными с бизнес-процессами с третьими сторонами или их персоналом.

FOT_MNG.1.6 ОФБ должны определять требования безопасности для осуществления менеджмента рисками, связанными с различными средствами хранения и обработки информации, которые будут использоваться третьей стороной.

FOT_MNG.1.7 ОФБ должны определять процедуры надзора и контролирования организацией разработки программного обеспечения, осуществляемой на стороне.

FOT_MNG.1.8 ОФБ должны определять требования безопасности для подтверждения реализации, эксплуатации и поддержания мер обеспечения безопасности, классификации служб и уровней поставки, включенных в договор о поставке услуг третьей стороной, этой третьей стороной.

FOT_MNG.1.9 ОФБ должны определять требования безопасности для регулярного мониторинга и пересмотра услуг, отчетов и записей, предоставляемых третьей стороной, а также проведения аудитов.

FOT_MNG.1.10 ОФБ должны определять требования безопасности к управлению внесением изменений в предоставление услуг, включая поддержание и усовершенствование существующих политик, процедур и мер обеспечения информационной безопасности с учетом критичности задействованных бизнес-систем и процессов и повторной оценки рисков.

FOT_MNG.1.11 ОФБ должны определять требования безопасности, предназначенные для внесения в договоры с третьими сторонами, включающие доступ к информации или средствам обработки информации организации, обработке, передаче этой информации или к управлению ею или добавлению продуктов или услуг к средствам обработки информации.

B.8 Класс FOM: управление

В данном классе представлены требования по управлению организационными мерами безопасности.

B.8.1 Управление параметрами безопасности (FOM_PRM)

B.8.1.1 Характеристика семейства

Данное семейство определяет управление параметрами безопасности и включает в себя подробное описание применения криптографии и привилегий.

B.8.1.2 Ранжирование компонентов

FOM_PRM.1 Использование криптографии

Определены подход к распределению ключей, включая методы защиты криптографических ключей и восстановления зашифрованной информации.

FOM_PRM.2 Разделение привилегий

Определено разделение привилегий.

B.8.1.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOM_PRM.1: описание подхода к распределению ключей, включая методы защиты криптографических ключей и восстановления зашифрованной информации с конкретными действиями и спецификациями.

Для FOM_PRM.2: описание разделения привилегий с конкретными действиями и спецификациями.

B.8.1.4 FOM_PRM.1 Использование криптографии

Зависимости: FOS_POL.4 Криптографическая политика.

FOM_PRM.1.1 ОФБ должны определять требования безопасности к методу управления использованием криптографических средств управления в организации, методу назначения ключей, включая методы защиты криптографических ключей и восстановления зашифрованной информации в случае утерянных, скомпрометированных или поврежденных ключей; роли и обязанности тех, кто отвечает за реализацию политики, а также положения и государственные ограничения, которые могут применяться к использованию криптографических мето-

дов в различных частях мира, и проблемы потока зашифрованной информации через границу для криптографической политики организации.

B.8.1.5 FOM_PRM.2 Разделение привилегий

FOM_PRM.2.1 ОФБ должны определять правила разделения привилегий для снижения возможностей несанкционированного или неправильного применения активов, отделения инициирования события от его авторизации.

FOM_PRM.2.2 ОФБ должны определять требования безопасности при назначении привилегий пользователю, отличных от тех, которые используются в обычной деловой деятельности.

B.8.2 Управление классификацией активов (FOM_CLS)

B.8.2.1 Характеристика семейства

В данном семействе определяется классификация активов. Она включает в себя категорирование.

B.8.2.2 Ранжирование компонентов

FOM_CLS.1 Категорирование

Определено категорирование записей.

FOM_CLS.2 Идентификация активов

Определена идентификация активов.

B.8.2.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOM_CLS.1: описание категоризации записей с конкретными спецификациями.

Для FOM_CLS.2: описание идентификации активов с конкретными спецификациями.

B.8.2.4 FOM_CLS.1 Категоризация

Зависимости: зависимости отсутствуют.

FOM_CLS.1.1 ОФБ должны определять требования безопасности к категоризации записей на типы записей, записи баз данных, журналы транзакций, журналы аудита и эксплуатационные процедуры (каждая с подробностями о периодах сохранности и типе среды для хранения информации).

B.8.2.5 FOM_CLS.2 Идентификация активов

Зависимости: зависимости отсутствуют.

FOM_CLS.2.1 ОФБ должны определять требования безопасности к спецификации идентификации, спецификации типа актива, функции актива, требований к управлению, предоставлять уровни защиты, соответствующие значимости активов, согласовывать владение и категорию защиты и регистрировать текущее местоположение каждого актива в реестре.

FOM_CLS.2.2 ОФБ должны определять требования безопасности к составлению и поддержанию реестра всех значимых активов.

FOM_CLS.2.3 ОФБ должны определять требования безопасности к периоду сохранности важной деловой информации, а также любые требования по постоянному хранению архивных копий.

B.8.3 Управление обязанностями персонала, связанными с безопасностью (FOM_PSN)

B.8.3.1 Характеристика семейства

Данное семейство определяет обязанности персонала по обеспечению безопасности. Определение обязанностей персонала осуществляется в отношении владельцев активов и менеджеров безопасности.

B.8.3.2 Ранжирование компонентов

FOM_PSN.1 Владение активами

Определено владение активами.

FOM_PSN.2 Менеджеры безопасности

Определено назначение менеджеров безопасности.

B.8.3.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOM_PSN.1: описание владения активами с конкретными спецификациями.

Для FOM_PSN.2: описание назначения менеджеров безопасности.

B.8.3.4 FOM_PSN.1 Владение активами

Зависимости: FOA_POL.3 Управление активами пользователя.

FOM_PSN.1.1 ОФБ должны определять требования безопасности к владению всей информацией и активами, связанными со средствами обработки информации, определенным подразделением организации.

B.8.3.5 FOM_PSN.2 Менеджеры безопасности

Зависимости: зависимости отсутствуют.

FOM_PSN.2.1 ОФБ должны определять требования безопасности к назначению конкретного ответственного менеджера каждому средству безопасности.

FOM_PSN.2.2 ОФБ должны определять требования безопасности с тем, чтобы руководство настаивало на применении мер обеспечения безопасности всеми работниками, подрядчиками и пользователями третьих сторон в соответствии с установленными политиками и процедурами организации.

B.8.4 Управление организацией безопасности (FOM_ORG)

B.8.4.1 Характеристика семейства

Данное семейство определяет организацию руководства по обеспечению безопасности и включает в себя обязанности руководства по обеспечению безопасности и участие в совещании руководства.

В.8.4.2 Ранжирование компонентов

FOM_ORG.1 Обязанности руководства

Определены обязанности руководства по обеспечению безопасности.

FOM_ORG.2 Членство в руководстве

Определено участие в совещании руководства.

В.8.4.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOM_ORG.1: описание обязанности руководства с конкретными действиями и спецификациями.

Для FOM_ORG.2: описание участия в заседании руководства с конкретными подробностями.

В.8.4.4 FOM_ORG.1 Обязанности руководства

Зависимости: FOD_ORG.1 Обязанности по координации безопасности

FOM_ORG.1.1 ОФБ должны определять обязанности руководства по обеспечению соответствия действий по обеспечению безопасности политике безопасности, утверждению конкретных методологий и процессов по информационной безопасности, мониторинга значительных изменений угроз и подвергания информационных активов угрозам, оценке адекватности и координации внедрения специфических мер обеспечения безопасности в новые системы или услуги, содействию доступности поддержки информационной безопасности в организации.

FOM_ORG.1.2 ОФБ должны определять обязанности менеджеров по обеспечению необходимого уровня выполнения процедур безопасности в своей зоне ответственности для достижения соответствия политикам и стандартам безопасности.

FOM_ORG.1.3 ОФБ должны определять обязанности руководства по пересмотру политики информационной безопасности через запланированные промежутки времени или, в случае внесения изменений, по обеспечению ее непрерывной стабильности, адекватности и эффективности.

В.8.4.5 FOM_ORG.2 Членство в совещании руководства

Зависимости: FOD_ORG.2 Обязанности совещания руководства.

FOM_ORG.2.1 ОФБ должны определять назначение представителей руководства и различных подразделений организации с соответствующими ролями и должностями для участия в совещании руководства с целью координации действий по обеспечению информационной безопасности.

В.8.5 Управление отчетами о безопасности (FOM_INC)

В.8.5.1 Характеристика семейства

Данное семейство определяет управление отчетами об инцидентах безопасности и включает в себя управление сообщенными проблемами безопасности.

В.8.5.2 Ранжирование компонентов

FOM_INC.1 Сообщение об обнаруженных проблемах безопасности

Определено управление сообщенными проблемами безопасности.

В.8.5.3 Записи

Автоматизированная система должна сохранять и предоставлять для проверки следующие свидетельства.

Для FOM_INC.1: описание процедур сообщения об инцидентах безопасности с конкретными действиями и спецификациями и записями о проведении контроля.

В.8.5.4 FOM_INC.1 Сообщение об обнаруженных проблемах безопасности

Зависимости: зависимости отсутствуют.

FOM_INC.1.1 ОФБ должны как можно быстрее определять процедуры обнаружения и сообщения о любых наблюдаемых или подозреваемых слабых местах в области безопасности или услугах в системах или сервисах руководству или непосредственно поставщику услуг для скорейшего предотвращения инцидентов безопасности.

FOM_INC.1.2 ОФБ должны определять правила запрещения попыток доказать наличие подозреваемых слабых мест посредством процесса эксплуатации системы.

Приложение С
(обязательное)

Требования доверия к безопасности автоматизированной системы

С.1 Введение

В настоящем приложении определены дополнительные требования доверия к безопасности автоматизированных систем, кроме требований ИСО/МЭК 15408-3. ИСО/МЭК 15408-3 использован в качестве основы для структуры компонентов этих систем.

Доверие к безопасности можно рассматривать в двух аспектах — корректность и эффективность. Корректность означает правильность внедрения механизмов безопасности, их функционирования в соответствии со спецификациями безопасности и поддержания доступности услуг по обеспечению безопасности. Эффективность означает, что механизмы безопасности противодействуют угрозам и уязвимостям, направленным против безопасности, и предотвращают такие несанкционированные процессы, как обход механизмов безопасности или несанкционированное вмешательство в работу этих механизмов. Доверие к безопасности можно достигать посредством действий на всех стадиях жизненного цикла системы. Доверие к безопасности автоматизированных систем приведено в таблице С.1.

Как корректность, так и эффективность можно оценить путем оценивания безопасности. Кроме того, может потребоваться принятие во внимание других форм доверия, таких как доверие, связанное с репутацией разработчика системы, и доверие, достигнутое в результате завершения использованных процессов разработки системы. Дополнительную информацию по этой теме см. в ИСО/МЭК ТО 15443 [7].

Таблица С.1 — Доверие к безопасности автоматизированных систем

Фактор	Этап жизненного цикла	Цель доверия	Класс доверия/семейство	Действие по оценке
Эффективность	Разработка/интеграция	Противодействие рискам. Требования безопасности, указанные в задании по безопасности системы, эффективны при снижении неприемлемых рисков до допустимого уровня	Оценка ЗБС/ПЗС (AST/ASP)	В целях безопасности все идентифицированные риски должны рассматриваться как неприемлемые. Требования безопасности должны соответствовать целям безопасности. Защитные меры противодействия должны соответствовать спецификации СОО
		Архитектура автоматизированной системы Защитные меры противодействия подсистем, компонентов и т.д. работают вместе для реализации необходимых характеристик безопасности общей системы	Описание архитектуры автоматизированной системы (ASD_SAD). Конструкция подсистемы (ASD_SSD). Конструкция компонента (ASD_CMP). Представления реализации (ASD_IMP) Интерфейсы безопасности (ASD_IFS) Концепция безопасности функционирования (ASD_CON)	Защитные меры противодействия должны работать эффективно совместно с другими мерами противодействия

Продолжение таблицы С.1

Фактор	Этап жизненного цикла	Цель доверия	Класс доверия/семейство	Действие по оценке
Эффективность	Разработка/ интеграция	Безопасная среда разработки	Меры обеспечения безопасности и их проверка в среде разработки (AOL_DVS)	Меры обеспечения безопасности для среды разработки должны быть подтверждены
	Установка	Надежность механизмов безопасности. Надежность механизмов безопасности эффективна для системы	Анализ уязвимостей (AOV_VLA)	Необходимо проводить анализ уязвимостей, а уязвимости не должны использоваться предполагаемой потенциальной атакой. Необходимо проводить испытание на проникновение, и проблем с безопасностью быть не должно
		Обучение в области коммуникации и осведомленности. Эффективное обучение соответствующего персонала ролям и процедурам и передача ему этих ролей	Подтверждение коммуникации и осведомленности (ASI_CMM, ASI_AWA)	Коммуникация и осведомленность должны быть подтверждены записями и опросами
	Функционирование	Мониторинг защитных мер противодействия. Для демонстрации должного функционирования защитных мер противодействия собираются контрольные журналы и записи мониторинга	Обнаружение незащищенного состояния (AOV_MSU). Проверка работы ФБС (AOD_ADM, AOD_USR, AOD_OCD, ASI_AWA, ASI_CMM, ASO_RCD, ASO_VER)	Необходимо подтвердить должное функционирование защитных мер противодействия
		Проверка Подтверждено что риски, которым надо оказать противодействие, не обнаружены, и меры обеспечения безопасности функционируют должным образом		Необходимо подтвердить с помощью контрольных журналов и опросов, что неприемлемые риски не обнаружены
	Модификация	Регрессионное тестирование. Меры обеспечения безопасности продолжают работать должным образом	Регрессионное тестирование (AOT_REG)	Обнаруженные проблемы безопасности должны исследоваться, и результаты возвращаться
		Испытание на проникновение. Изменения в системе не нарушают область действия мер обеспечения безопасности	Испытание на проникновение (AOV_VLA). Испытание на наличие незащищенных состояний (AOV_MSU)	Обнаруженные проблемы безопасности должны исследоваться, и результаты возвращаться

Продолжение таблицы С.1

Фактор	Этап жизненного цикла	Цель доверия	Класс доверия/семейство	Действие по оценке
Правильность	Разработка/ интеграция	Соответствие между рисками безопасности и требованиями безопасности, а также требованиями безопасности и защитными мерами противодействия. Требования безопасности относятся ко всем неприемлемым рискам. Защитные меры противодействия соответствуют всем требованиям безопасности	Оценка ЗБС/ПЗС (AST/ASP)	Цели безопасности должны учитывать все риски, определенные как неприемлемые. Требования безопасности должны соответствовать целям безопасности. Защитные меры противодействия должны соответствовать спецификации СОО
		Управление конфигурацией. Управление элементами конфигурации защитных мер противодействия осуществляется правильно	Конфигурация (AOD_OCD)	Элементами конфигурации необходимо управлять и применять их в системе
		Соответствие проектно-исследовательским разработкам. Защитные меры противодействия реализуются правильно. Защитные меры противодействия → назначение → внедрение	Описание архитектуры автоматизированной системы (ASD_SAD). Конструкция подсистем (ASD_SSD), Конструкция компонентов (FSD_CMP). Представления внедрения (ASD_IMP). Интерфейсы безопасности (ASD_IFS). Концепция безопасности операций (ASD_CON). Испытание (AOT)	Защитные меры противодействия должны реализовываться без несанкционированных модификаций, дополнений или исключений
		Описание руководств. Безопасные операции описаны в руководстве правильно	Описание (AOD_ADM, AOD_USR)	Функционирование защитных мер противодействия должны быть описаны достаточно подробно
	Установка	Соответствие. Организационные меры безопасности соответствуют требованиям безопасности	Изучение руководств (AOV_MSU)	Руководства должны быть понятными и полными
		Авторизация. Установка организационных мер обеспечения безопасности разрешена санкционированным лицом	(Отсутствует)	(Отсутствует)

Окончание таблицы С.1

Фактор	Этап жизненного цикла	Цель доверия	Класс доверия/семейство	Действие по оценке
Правильность	Установка	Конфигурация. Компоненты и подсистемы сконфигурированы правильно	Конфигурация (AOC). Испытание (AOT)	Необходимо проверить конфигурацию компонентов и подсистем и функционирование мер обеспечения безопасности
		Пуск. Пуск СОО выполняется правильно	Установка и пуск (ASI_SIC)	Необходимо подтвердить правильность установки и пуска
	Функционирование	Мониторинг защитных мер противодействия. Защитные меры противодействия выполняются правильно	Мониторинг (ASO_MON)	Необходимо проверить следы аудита и записи мониторинга доступа к активам и их использования
		Проверка. Подтверждено, что риски, которым надо оказать противодействие, не обнаружены, а меры обеспечения безопасности функционируют должным образом	Проверка конфигурации (AOC_OBM). Проверка среды эксплуатации (AOC_ECP, AOC_PPC, AOC_NCP). Проверка безопасной установки (AOC_SIC). Проверка записей (ASO_RCD). Независимая проверка (ASO_VER)	Необходимо проверить меры обеспечения безопасности
	Модификация	Проверка проекта. Подтверждено, что модификации не сделали недействительными другие части проекта. Регрессионное тестирование. Подтверждено должное функционирование измененных мер обеспечения безопасности	Проверка проекта (AOD_GVR, FSD_GVR). Регрессионное тестирование (AOT_REG)	Необходимо проанализировать изменения в проекте. Необходимо исследовать обнаруженные проблемы безопасности и возвратить результаты

Критерии оценки по ИСО/МЭК 15408-3 содержат многие аспекты доверия к безопасности автоматизированных систем. Однако для некоторых других аспектов доверия к безопасности автоматизированных систем требуются дополнительные критерии.

В настоящем приложении определены новые классы требований доверия. Ими являются:

a) оценка ПЗС (ASP); специфицирует требования к оценке профилей защиты для АС;

b) оценка ЗБС (ASS); специфицирует требования к оценке заданий по безопасности для АС;

c) руководства для автоматизированных систем (AOD); специфицирует требования к оценке руководств для автоматизированных систем;

d) документация по проектированию архитектуры автоматизированных систем и конфигурационная документация (ASD); специфицирует требования к оценке документации по конфигурированию и проектированию автоматизированных систем;

e) управление конфигурацией автоматизированных систем (AOC); специфицирует требования к оценке управления конфигурацией автоматизированных систем;

f) тестирование автоматизированных систем (AOT); специфицирует требования к оценке тестирования автоматизированных систем;

g) анализ уязвимостей автоматизированных систем (AOV); специфицирует требования к оценке анализа уязвимостей автоматизированных систем;

h) поддержка жизненного цикла автоматизированных систем (AOL); специфицирует требования к оценке поддержки жизненного цикла автоматизированных систем;

i) безопасная установка системы (ASL); специфицирует требования к оценке безопасной установки системы;

j) регистрация и запись в автоматизированных системах (ASO); специфицирует требования к оценке регистрации и мониторинга организационных мер безопасности.

Имеются новые классы доверия для оценки профилей защиты системы (ПЗС) и заданий по безопасности системы (ЗБС), поскольку содержимое ПЗС или ЗБС расширено из содержимого ПЗ или ЗБ. Другие новые классы относятся к дополнительным требованиям доверия к оценке автоматизированных систем.

Взаимосвязь между дополнительными требованиями доверия, определенными в данном приложении, и этапами жизненного цикла автоматизированных систем приведены в таблице С.2

Таблица С.2 — Требования доверия и жизненный цикл автоматизированных систем

Жизненный цикл	Требование доверия	
Разработка/интеграция	FOD_OCD.1	Описание конфигурации в руководстве по конфигурации
	AOD_ADM.1	Описание связанных с администраторами ФБС в руководстве для администраторов
	AOD_USR.1	Описание связанных с пользователями ФБС в Руководстве для пользователей
	ASD_SAD.1	Описание архитектуры
	ASD_IFS.1	Описание внешних интерфейсов
	ASD_SSD.1	Описание структуры подсистем
	ASD_CMP.1	Описание структуры базисного элемента (примитива)
	ASD_IMP.1	Получение конкретного представления внедрения
	ASD_CON.1	Концепция безопасности функционирования
	AOL_DVS.1	Меры обеспечения безопасности для среды разработки
	AOT_FUN.1	Функциональная проверка ФБС
	AOT_COV.1	Покрытие тестами для ФБС
	AOT_COV.2	Завершенность покрытия тестами для ФБС
	AOT_DPT.1	Глубина испытания для спецификации интерфейса
	AOT_DPT.2	Глубина испытания для проекта подсистем
	AOT_DPT.3	Глубина испытания для проекта компонентов
	AOT_DPT.4	Глубина испытания для представления реализации
	AOL_DVS.2	Проверка мер обеспечения безопасности для среды разработки
Установка	AOC_OBM.1	Управление конфигурацией
	AOC_ECP.1	Идентификация оцененных продуктов
	AOC_PPC.1	Идентификация соответствия ПЗ
	AOC_NPC.1	Новая оценка новых продуктов
	AOT_FUN.1	Функциональное испытание ФБС

Окончание таблицы С.2

Жизненный цикл	Требование доверия	
Установка	AOT_COV.1	Покрытие тестами для ФБС
	AOT_COV.2	Завершенность покрытия тестами для ФБС
	AOT_DPT.1	Глубина испытания для спецификации интерфейса
	AOT_DPT.2	Глубина испытания для проекта подсистем
	AOT_DPT.3	Глубина испытания для проекта компонентов
	AOT_DPT.4	Глубина испытания для представления реализации
	AOT_IND.1-3	Независимое тестирование
	AOV_MSU.1	Проверка руководств автоматизированной системы
	AOV_VLA.1-4	Испытание на проникновение
	ASI_AWA.1	Повышение осведомленности
	ASI_CMM.1	Передача информации о ФБС соответствующему персоналу
	ASI_SIC.1	Безопасная установка и пуск СОО
Функционирование	AOD_OCD.2	Проверка спецификаций в руководстве по конфигурациям
	AOD_ADM.2	Проверка проводимости ФБС в руководстве для администраторов
	AOD_USR.2	Проверка проводимости ФБС в руководстве для пользователей
	AOC_OBM.2	Проверка управления конфигурациями
	AOC_ECP.2	Проверка среды эксплуатации для оцененных продуктов
	AOC_PPC.2	Проверка среды эксплуатации для заявленного соответствия ПЗ
	AOC_NCP.2	Проверка среды эксплуатации для новых оцененных продуктов
	AOV_MSU.2	Обнаружение незащищенных рабочих состояний и восстановлений
	ASI_AWA.2	Проверка повышения уровня осведомленности
	ASI_CMM.2	Проверка передачи информации о ФБС персоналу
	ASI_SIC.2	Проверка безопасной установки и пуска
	ASO_RCD.1-2	Проверка рабочих записей
	ASO_VER.1-2	Проверка организационных мер безопасности
	ASO_MON.1	Мониторинг управления для ФБС
	ASO_MON.2	Независимая проверка мониторинга управления
Модификация	AOD_GVR.1	Проверка руководств
	ASD_GVR.1	Проверка проекта
	AOT_REG.1	Регрессивное испытание
	AOV_MSU.2	Анализ и испытание незащищенных состояний
	AOV_VLA.1-4	Испытание на проникновение

Настоящее приложение содержит два существенных отличия от ИСО/МЭК 15408-3 «элементы действий разработчика» были переименованы в «элементы действий разработчика/интегратора», чтобы показать, что автоматизированная система может быть составлена системным интегратором, который отличается от разработчика компонентов и продуктов, используемых в системе, и оба они могут сотрудничать в получении и доставке необходимых свидетельств. В некоторых случаях менеджеры автоматизированной системы отвечают за получение свидетельств, поэтому в этих семействах элементы действий определены как действия управления.

Зависимости между компонентами доверия представлены в таблицах С.3 — С.5. По причине независимого проведения оценок ПЗС, ЗБС и СОО были использованы три таблицы, и поэтому между каждым набором не может быть взаимозависимостей. Каждый из компонентов, являющийся зависимостью какого-либо компонента доверия, находится в соответствующем столбце таблицы. Каждый компонент доверия с зависимостями находится в соответствующей строке. Значение в таблице указывает на прямую потребность маркировочного компонента строки в маркировочном компоненте колонки (знак «X») или косвенную потребность (знак «—»).

Таблица С.3 — Зависимости доверия к ПЗС

	ASP_INT.1	ASP_ECD.1	ASP_SPD.1	ASP_OBJ.1	ASP_REQ.1	ASP_DMP.1	ASP_DMO.1	ASP_DMR.1
ASP_CCL.1	X	X	X	X	X			
ASP_OBJ.1			X					
FSP_REQ.1		X						
ASP_REQ.2		X	—	X				
ASP_DMI.1	X							
ASP_DMC.1	—	—				X	X	X
ASP_DMO.1	X					X		
ASP_DMR.1		X						
ASP_DMR.2	—	X				—	X	

Таблица С.4 — Зависимости доверия к ЗБС

	ASS_INT.1	ASS_ECD.1	ASS_SPD.1	ASS_OBJ.1	ASS_REQ.1	ASS_DMI.1	ASS_DMP.1	ASS_DMO.1	ASS_DMR.1
ASS_CCL.1	X	X	X	X	X				
ASS_OBJ.1			X						
ASS_REQ.1		X							
ASS_REQ.2		X	—	X					
ASS_TSS.1	X	—			X				
ASS_DMI.1	X								
ASS_DMC.1	—	—					X	X	X
ASS_DMO.1	X						X		
ASS_DMR.1		X							
ASS_DMR.2	—	X					—	X	
ASS_DMS.1	—	—				X			X

Таблица С.5 — Зависимости доверия к СОО

	AOD_OCD.1	AOD_ADM.1	AOD_USR_1	ASD_SAD.	ASD_IFS.1	ASD_SSD 1	ASD_CMP1	ASD_IMP1	ASD_CON.1	AOS_OBM.1	AOT_FUN.1
AOD_OCD.1/2				—	—	—	X		X		
AOD_ADM.1/2				X							
AOD_USR.1/2X				X							
AOD_GVR.1	X	X	X	—	—	—	—		—		
ASD_IFS.1				X							
ASD_SSD.1				X	X						
ASD_CMP.1				—	X	X					
ASD_IMP.1				—	—	—	X				
ASD_CON.1				X							
ASD_GVR.1				X	X	X	X		X		
AOC_ECP.1/2										X	
AOC_PPC.1/2										X	
AOC_NCP.1/2										X	
AOT_COV.1/2				—	X						X
AOT_DPT.1				—	X						X
AOT_DPT.2				—	X	X					X
AOT_DPT.3				—	X	X	X				X
AOT_DPT.4				—	X	X	X	X			X
AOT_IND.1		X	X	—	X						
AOT_IND.2/3		X	X	—							X
AOV_MSU.1/2		X	X	—							
AOV_VLA.1		X	X	—	X	X			X		
AOV_VLA.1		X	X	—	X	X			X		

С.2 Класс ASP: оценка профиля защиты системы

С.2.1 Введение

В настоящем разделе представлены критерии доверия к оценке профилей защиты системы (ПЗС). Оценка ПЗС требуется для демонстрации того, что ПЗС является обоснованным и внутренне непротиворечивым, и, если ПЗС получен из одного или нескольких ПЗ или пакетов, ПЗС является корректным представлением этих ПЗС и пакетов. Данные характеристики необходимы, чтобы использовать ПЗС в качестве основы при последующей оценке СОО.

Ниже перечислены семейства в этом классе:

a) ASP_INT: введение ПЗС;

в) ASP_CCL: утверждения о соответствии;

c) ASP_SPD: определение проблемы безопасности;

d) ASP_OBJ: цели безопасности;

e) ASP_ECD: определение компонентов расширения;
f) ASP_REQ: требования безопасности;
g) ASPP_DMI: введение для домена безопасности;
h) ASP_DMC: утверждения о соответствии домена безопасности;
i) ASP_DMP: определение проблемы безопасности домена безопасности;
j) ASP_DMO: цели безопасности домена безопасности;
k) ASP_DMR: требования безопасности домена безопасности.

С.2.2 Общая часть ПЗС

Следующие спецификации применимы к целому ПЗС. Спецификации для конкретных доменов должны описываться с помощью семейств доменов (см. С.2.9).

С.2.3 Введение ПЗС (ASP_INT)

С.2.3.1 Цели

Целью данного семейства является описание СОО в повествовательном виде.

Оценка введения ПЗС требуется для демонстрации правильной идентификации ПЗС и согласованности между собой краткого анализа СОО и спецификации доменной организации. Введения конкретных доменов безопасности определены в подразделе С.2.10 «Введение доменов безопасности».

С.2.3.2 ASP_INT.1 Введение ПЗС

Зависимости: зависимости отсутствуют.

С.2.3.2.1 Элементы действий разработчика/интегратора

ASP_INT.1.1D Разработчик/интегратор должен обеспечит введение ПЗС.

С.2.3.2.2 Элементы содержания и представления свидетельств

ASP_INT.1.1C Введение ПЗС должно содержать ссылку ПЗС, краткий анализ СОО и спецификацию доменной организации.

ASP_INT.1.2C Ссылка ПЗС должна однозначно идентифицировать ПЗС.

ASP_INT.1.3C В кратком обзоре СОО должны резюмироваться использование и основные характеристики безопасности СОО.

ASP_INT.1.4C Краткий обзор СОО должен идентифицировать тип СОО.

ASP_INT.1.5C Краткий обзор СОО должен идентифицировать взаимосвязь и интерфейсы, необходимые для СОО, с любыми внешними автоматизированными системами.

ASP_INT.1.6C В спецификации доменной организации должна описываться организация мандатных доменов безопасности и их идентификация, физическая сфера применения и границы каждого домена безопасности.

ASP_INT.1.7C Для каждого домена безопасности в спецификации должны описываться все услуги по обеспечению безопасности, предоставляемые этим доменом и доступные другим доменам, и все характеристики безопасности домена, задаваемые другим доменам.

С.2.3.2.3 Элементы действий оценщика

ASP_INT.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_INT.1.2E Оценщик должен подтверждать совместимость краткого обзора СОО и спецификации доменной организации.

С.2.4 Утверждение соответствия (ASP_CCL)

С.2.4.1 Цели

Целью данного семейства является определение достоверности различных утверждений соответствия: утверждение соответствия стандартам серии ИСО/МЭК 15408, утверждение соответствия ПЗС, утверждение соответствия ПЗ и утверждение соответствия пакета требований. В утверждении соответствия стандартов серии ИСО/МЭК 15408 описывается версия ИСО/МЭК 15408, соответствие которой утверждается ПЗС и СОО, в утверждении ПЗ (если имеются) описывается, как ПЗС утверждает соответствие идентифицированным ПЗ, в утверждении пакета (если он имеется) описывается, как ПЗС утверждает соответствие с установленным пакетом, тогда как ПЗС идентифицирует ПЗС (если имеются), о соответствии которым утверждает ПЗС. Определяют достоверность утверждения ПЗС, утверждение ПЗ и пакета влекут за собой определение, четко ли идентифицированы все заявленные ПЗС, ПЗ и пакеты, полностью ли ПЗС содержит эти ПЗС, ПЗ и пакеты, и правильно ли выполнены все требования безопасности, выведенные из этих ПЗС, ПЗ и пакетов. Утверждения соответствия для конкретного домена безопасности определены в С.2.11 «Утверждение о соответствия домена безопасности».

С.2.4.2 ASP_CCL.1 Утверждения соответствия

Зависимости:
ASP_INT.1 Введение ПЗС;
ASP_SPD.1 Определение проблем безопасности;
ASP_OBJ.1. Цели безопасности;
ASP_ECD.1 Определение расширенных компонентов;
ASP_REQ.1 Установленные требования безопасности.

С.2.4.2.1 Элементы действий разработчика/интегратора

ASP_CCL.1.1D Разработчик/интегратор должен предоставить утверждение соответствия.

ASP_CCL.1.2D Разработчик/интегратор должен предоставить обоснование утверждения соответствия.

С.2.4.2.2 Элементы содержания и представления свидетельств

ASP_CCL.1.1C Утверждение соответствия должно содержать утверждение соответствия критериям, идентифицирующее версию ИСО/МЭК ТО 19791, соответствие которому утверждается в ПЗС.

ASP_CCL.1.2C В утверждении соответствия критериям должно быть описано функциональное соответствие ПЗС ИСО/МЭК ТО 19791 как функционально соответствующий ИСО/МЭК ТО 19791 или функционально расширенный по отношению к ИСО/МЭК ТО 19791.

ASP_CCL.1.3C В утверждении соответствия критериям должно быть описано соответствие доверия ПЗС ИСО/МЭК ТО 19791 в виде матрицы отображения доверия соответствующего ИСО/МЭК ТО 19791 или как доверие стандартов серии ИСО/МЭК 15408 с расширением по стандарту ИСО/МЭК ТО 19791.

ASP_CCL.1.4C Утверждение соответствия должно согласовываться с определением расширенных компонентов.

ASP_CCL.1.5C Утверждение соответствия должно идентифицировать все ПЗС, ПЗ и пакеты требований безопасности, соответствие которым утверждает ПЗС.

ASP_CCL.1.6C В утверждении соответствия должно быть описано любое соответствие ПЗС пакету или как полностью соответствующее, или как дополненное к пакету.

ASP_CCL.1.7C Обоснование утверждений соответствия должно демонстрировать согласование типа СОО с типом СОО в ПЗС,ПЗ и пакетах, о соответствии которым делается утверждение.

ASP_CCL.1.8C Обоснование утверждений соответствия должно демонстрировать согласование формулировки определения проблемы безопасности с формулировкой определения проблемы безопасности в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASP_CCL.1.9C Обоснование утверждений соответствия должно демонстрировать согласование формулировки целей с формулировкой целей в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASP_CCL.1.10C Обоснование утверждений соответствия должно демонстрировать согласование формулировки требований безопасности с формулировкой требований безопасности в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASP_CCL.1.11C Обоснование утверждений соответствия должно демонстрировать, что все операции, связанные с требованиями безопасности, которые были взяты из ПЗС, ПЗ или пакета, завершены в согласовании с соответствующими ПЗС, ПЗ или пакетом.

С.2.4.2.3 Элементы действий оценщика

ASP_CCL.1.1E Оценщик должен подтвердить, что предоставленная информация отвечает всем требованиям к содержанию и представлению свидетельств.

ASP_CCL.1.2E Оценщик должен подтвердить, что ПЗС удовлетворяет утверждению соответствия стандартам серии ИСО/МЭК 15408.

С.2.5 Определение проблем безопасности (ASP_SPD)

С.2.5.1 Цели

В данном подразделе ПЗС определяются проблемы безопасности, относящиеся к СОО, включая среду его разработки. Эти проблемы безопасности применимы к СОО в целом. Проблемы безопасности конкретного домена безопасности определены в подразделе С.2.12 «Определение проблем доменов безопасности». Оценка определения проблем безопасности нужна для демонстрации, что проблемы безопасности, предназначенные для рассмотрения СОО, включая его среду разработки, четко определены.

С.2.5.2 ASP_SPD.1 Определение проблем безопасности

Зависимости: зависимости отсутствуют.

С.2.5.2.1 Элементы действий разработчика/интегратора

ASP_SPD.1.1D Разработчик/интегратор должен обеспечивать определение проблем безопасности.

С.2.5.2.2 Элементы содержания и представления свидетельств

ASP_SPD.1.1C. В определении проблем безопасности должны быть указаны все риски, применимые к СОО. Каждый риск должен категорироваться как «приемлемый» или «неприемлемый».

ASP_SPD.1.2C Все неприемлемые риски должны быть описаны на основе угроз и уязвимостей. Каждая угроза должна описываться с точки зрения источника угрозы, актива и враждебного действия.

ASP_SPD.1.3C В определении проблем безопасности должны быть описаны ПБОр.

С.2.5.2.3 Элементы действий оценщика

ASP_SPD.1.1E Оценщик должен подтверждать соответствие поставленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_SPD.1.2E Оценщик должен подтверждать внутреннюю непротиворечивость определения проблемы безопасности.

С.2.6 Цели безопасности (ASP_OBJ)

С.2.6.1 Цели

Целями безопасности является краткая формулировка намеченной реакции на проблему безопасности, определенную при помощи семейства ASP_SPD. Определенные цели безопасности в этой части применимы к СОО в целом. Цели безопасности для конкретного домена безопасности определены в подразделе С.2.13 «Цели безопасности домена безопасности». Оценка целей безопасности требуется для демонстрации того, что цели безопасности адекватно и полностью учитывают определение проблем безопасности, и распределение

этой проблемы между СОО, средой ее разработки и внешними автоматизированными системами четко определено, и что цели безопасности внутренне согласованы.

С.2.6.2 ASP_OBJ.1 Цели безопасности

Зависимости: ASP_SPD.1 Определение проблемы безопасности.

С.2.6.2.1 Элементы действий разрботчика/интегратора

ASP_OBJ.1.1D Разработчик/интегратор должен предоставить формулировку целей безопасности.

ASP_OBJ.1.2D Разработчик/интегратор должен предоставить обоснование целей безопасности.

С.2.6.2.2 Элементы содержания и представления свидетельств

ASP_OBJ.1.1C В формулировке целей безопасности должны излагаться цели безопасности для СОО.

ASP_OBJ.1.2C В формулировке целей безопасности должны излагаться все цели безопасности, которым соответствуют внешние автоматизированные системы.

ASP_OBJ.1.3C В формулировке целей безопасности должны излагаться цели безопасности для среды разработки.

ASP_OBJ.1.4C В обосновании целей безопасности должна отслеживаться каждая цель безопасности для СОО обратно к рискам, которым противостоит эта цель безопасности, и ПБОр, которым соответствует эта цель безопасности.

ASP_OBJ.1.5C В обосновании целей безопасности должна отслеживаться каждая цель безопасности для внешних автоматизированных систем обратно к рискам, которым противостоит эта цель безопасности, и ПБОр, которым соответствует эта цель безопасности.

ASP_OBJ.1.6C В обосновании целей безопасности должна отслеживаться каждая цель безопасности для среды разработки обратно к рискам, которым противостоит эта цель безопасности, и ПБОр, которым соответствует эта цель безопасности.

ASP_OBJ.1.7C Обоснование целей безопасности должно демонстрировать противостояние целей безопасности всем неприемлемым рискам.

ASP_OBJ.1.8C Обоснование целей безопасности должно демонстрировать, что цели безопасности осуществляют все ПБОр.

С.2.6.2.3 Элементы действий оценщика

ASP_OBJ.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.2.7 Определение расширенных компонентов (ASP_ECD)

С.2.7.1 Цели

Расширенные требования безопасности основаны не на компонентах стандартов серии ИСО/МЭК 15408 или настоящего стандарта, а на расширенных компонентах, определенных автором ПЗС. Оценка определения расширенных компонентов необходима для определения их ясности, однозначности и необходимости, т.е. для того, чтобы они не могли быть выражены с помощью существующих компонентов стандартов серии ИСО/МЭК 15408 или настоящего стандарта.

С.2.7.2 ASP_ECD.1 определение расширенных компонентов

Зависимости: зависимости отсутствуют.

С.2.7.2.1 Элементы действий разработчика/интегратора

ASP_ECD.1.1D Разработчик/интегратор должен предоставлять формулировку требований безопасности.

ASP_ECD.1.2D Разработчик/интегратор должен предоставлять определение расширенных компонентов.

С.2.7.2.2 Элементы содержания и представления свидетельств

ASP_ECD.1.1C В формулировке требований безопасности должны идентифицироваться все расширенные требования безопасности.

ASP_ECD.1.2C В определении расширенных компонентов должен определяться расширенный компонент для каждого расширенного требования безопасности.

ASP_ECD.1.3C В определении расширенных компонентов должно быть изложено, как каждый расширенный компонент связан с существующими компонентами, семействами и классами по стандартам серии ИСО/МЭК 15408.

ASP_ECD.1.4C В определении расширенных компонентов должны использоваться существующие компоненты, семейства, классы и методология по стандартам серии ИСО/МЭК 15408 в качестве модели для представления.

ASP_ECD.1.5C Расширенные компоненты должны состоять из измеримых и объективных элементов так, чтобы можно было продемонстрировать соответствие или несоответствие этим элементам.

С.2.7.2.3 Элементы действий оценщика

ASP_ECD.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_ECD.1.2E Оценщик должен подтверждать, что ни один расширенный компонент не может быть ясно выражен с помощью существующих компонентов.

С.2.8 Требования безопасности (ASP_REQ)

С.2.8.1 Цели

ФБС формируют ясное и недвусмысленное изложение предполагаемого поведения СОО в сфере безопасности. Доверие к безопасности системы формирует ясное и недвусмысленное изложение предполагаемых

действий, которые будут предприняты для получения доверия к СОО. Требования безопасности, определенные в данном подразделе, применимы к СОО в целом. Требования безопасности для конкретного домена безопасности определены в подразделе С.2.14 «Требования безопасности к домену безопасности». Оценка требований безопасности необходима для обеспечения их ясности и однозначности.

С.2.8.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются по уровням, исходя из того, заявлены ли они в оригинальном виде или выведены из целей безопасности для СОО и среды его разработки.

С.2.8.3 ASP_REQ.1 Заданные требования безопасности

Зависимости: ASP_REQ.1 Определение расширенных компонентов.

С.2.8.3.1 Элементы действий разработчика/интегратора

Зависимости: зависимости отсутствуют.

С.2.8.3.2 Элементы содержания и представления свидетельств

ASP_REQ.1.1C В формулировке требований безопасности должны быть описаны ФБС и ДБС.

ASP_REQ.1.2C В формулировке требований безопасности должны идентифицироваться все операции, связанные с требованиями безопасности.

ASP_REQ.1.3C Все операции должны выполняться правильно.

ASP_REQ.1.4C Каждая зависимость между требованиями безопасности должна быть или удовлетворена, или идентифицирована как «неудовлетворенная».

С.2.8.3.3 Элементы действий оценщика

ASP_REQ.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_ REQ .1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности.

С.2.8.4 ASP_ REQ.2 Производные требования безопасности

Являются иерархическими для: ASP_ REQ .1 Установленные требования безопасности.

Зависимости:

ASP_OBJ.1 Цели безопасности;

ASP_ECD.1 Определение расширенных компонентов.

С.2.8.4.1 Элементы действий разработчика/интегратора

ASP_ REQ.2.1D Разработчик/интегратор должен предоставить обоснование требований безопасности.

С.2.8.4.2 Содержание и представление элементов безопасности

ASP_REQ.2.1C В формулировке должны быть описаны ФБС и ДБС.

ASP_REQ.2.2C В формулировке требований безопасности должны идентифицироваться все операции, связанные с требованиями безопасности.

ASP_REQ.2.3C Все операции должны выполняться правильно.

ASP_REQ.2.4C Каждая зависимость между требованиями безопасности должна быть удовлетворена, или обоснование требований безопасности должно объяснять причину неудовлетворения зависимости.

ASP_REQ.2.5C Обоснование требований безопасности должно сопоставлять каждую ФБС с целями безопасности СОО.

ASP_REQ.2.6C Обоснование требований безопасности должно сопоставлять каждую ФБС с целями целей безопасности СОО или среды его разработки.

ASP_REQ.2.7C Обоснование требований безопасности должно демонстрировать соответствие ФБС и ДБС целям безопасности СОО и среды его разработки, которым не соответствуют внешние системы.

С.2.8.4.3 Элементы действий оценщика

ASP_REQ.2.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_ REQ.2.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности.

С.2.9 Домены безопасности профиля защиты системы

Каждый домен безопасности ПЗС определяет проблемы безопасности, цели безопасности и требования безопасности, уникальные для этого конкретного домена безопасности.

В последующих разделах определяются семейства, применяющиеся для определения доменов безопасности внутри ПЗС.

С.2.10 Введение доменов безопасности (ASP_DMI)

С.2.10.1 Цели

Целью данного семейства является описание домена безопасности в повествовательной форме на трех уровнях абстракции: ссылка на домен безопасности, краткий обзор домена безопасности и описание домена безопасности.

С.2.10.2 ASP_DMI.1 Введение доменов безопасности

Зависимости: ASP_INT.1 Введение ПЗС.

С.2.10.2.1 Элементы действий разработчика/интегратора

ASP_DMI.1D Разработчик/интегратор должен обеспечить введение доменов безопасности.

С.2.10.2.2 Элементы содержания и представления свидетельств

ASP_DMI.1.1C Введение доменов безопасности должно содержать ссылку на домен безопасности, краткий обзор домена безопасности и описание домена безопасности.

ASP_DMI.1.2C Ссылка на домен безопасности должна однозначно идентифицировать домен безопасности.

ASP_DMI.1.1.3C Домен безопасности должен резюмировать использование и основные характеристики безопасности домена безопасности.

ASP_DMI.1.1.4C В описании домена безопасности должны быть изложены включенные в нее подсистемы и/или компоненты.

ASP_DMI.1.1.5C В описании домена безопасности должны быть изложены взаимосвязи и интерфейсы с другими доменами.

С.2.10.2.3 Элементы действий оценщика

ASP_DMI.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_DMI.1.2.E Оценщик должен подтверждать согласование ссылки на домен безопасности, краткий обзор домена безопасности и описаний доменов безопасности друг с другом и с введением ПЗС.

С.2.11 Утверждение соответствия для доменов безопасности (ASP_DMC)

С.2.11.1 Цели

Данная часть ПЗС определяет уникальные утверждения соответствия для доменов безопасности.

С.2.11.2 ASP_DMC.1 Утверждения о соответствии

Зависимости:

ASP_DMP.1 Определение проблем безопасности доменов безопасности;

ASP_DMO.1 Цели безопасности доменов безопасности;

ASP_DMR.1 Установленные требования безопасности для доменов безопасности.

С.2.11.2.1 Элементы действий разработчика/интегратора

ASP_DMC.1.1D Разработчик/интегратор должен обеспечить утверждения соответствия домена безопасности.

ASP_DMC.1.2D Разработчик/интегратор должен обеспечить обоснование утверждений о соответствии.

С.2.11.2.2 Элементы содержания и представления свидетельств

ASP_DMC.1.1C В утверждении соответствия домена должны идентифицироваться все ПЗС, ПЗ и пакеты требований безопасности, о соответствии которым делается утверждение.

ASP_DMC.1.2C В утверждении соответствия домена должно быть описано любое соответствие домена пакету как соответствующее полностью или как дополнение к пакету.

ASP_DMC.1.3C Обоснование утверждения соответствия домена должно демонстрировать согласование типа СОО с типом СОО в ПЗС, ПЗ и пакетами, о соответствии которых делается утверждение.

ASP_DMC.1.4C Обоснование утверждения соответствия домена должно демонстрировать согласование формулировки определения проблем безопасности домена с формулировкой определения проблем безопасности с ПЗС,ПЗ и пакетами, о соответствии которым делается утверждение.

ASP_DMC.1.5C Обоснование утверждения соответствия домена должно демонстрировать согласование формулировки определения целей безопасности домена с формулировкой целей в ПЗС, ПЗ и пакетами, о соответствии которым делается утверждение.

ASP_DMC.1.6C Обоснование утверждения соответствия домена должно демонстрировать согласование формулировки определения целей безопасности домена с формулировкой целей в ПЗС,ПЗ и пакетами, о соответствии которым делается утверждение.

ASP_DMC.1.7C Обоснование утверждения соответствия домена должно демонстрировать завершение всех операций, связанных с требованиями безопасности, которые были взяты из ПЗС, ПЗ или пакетов, согласно соответствующим ПЗС, ПЗ или пакетам.

С.2.11.2.3 Элементы действий оценщика

ASP_DMC.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.2.12 Определение проблем безопасности домена безопасности (ASP_DMP)

С.2.12.1 Цели

В данной части ПЗС определяются уникальные проблемы безопасности для домена безопасности.

ASP_DMP.1 Определение проблем безопасности домена безопасности.

Зависимости: зависимости отсутствуют.

С.2.12.2 Элементы действий разработчика/интегратора

ASP_DMP.1.1D Разработчик/интегратор должен обеспечить определение проблем безопасности домена.

С.2.12.3 Элементы содержания и представления свидетельств

ASP_DMP.1.1C В определении проблем безопасности домена должны быть приведены все уникальные риски, применимые к домену. Каждый риск должен категорироваться как «приемлемый» или «неприемлемый».

ASP_DMP.1.2C Все неприемлемые риски должны излагаться с точки зрения угроз и уязвимостей. Каждая угроза должна быть описана исходя из источника угрозы, актива и враждебного действия.

ASP_DMP.1.3C В определении проблем безопасности домена должны быть приведены уникальные ПБОР, применимые к домену.

С.2.12.4 Элементы действий оценщика

ASP_DMP.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_DMP.1.2E Оценщик должен подтверждать внутреннюю согласованность определения проблем безопасности домена.

С.2.13 Цели безопасности домена безопасности (ASP_DMO)

С.2.13.1 Цели

В данной части ПЗС приведена краткая формулировка предполагаемой реакции на уникальные проблемы безопасности, определенная посредством семейства ASP_DMP.

С.2.13.2 ASP_DMO.1 Цели безопасности домена безопасности

Зависимости:

ASP_INT.1 Введение ПЗС;

ASP_DMP.1 Определении проблем безопасности домена безопасности.

С.2.13.2.1 Элементы действий разработчика/интегратора

ASP_DMO.1.1D Разработчик/интегратор должен обеспечить формулировку целей безопасности домена.

ASP_DMO.1.2D Разработчик/интегратор должен обеспечить обоснование целей безопасности домена.

С.2.13.2.2 Элементы содержания и представления свидетельств

Каждая зависимость между требованиями безопасности должна быть удовлетворена, или обоснование требований безопасности должно объяснять причину неудовлетворения зависимости.

ASP_DMO.1.1C В формулировке целей безопасности домена должны излагаться уникальные цели безопасности для домена.

ASP_DMO.1.2C В формулировке целей безопасности домена должны излагаться любые цели безопасности для домена, которым соответствуют другие домены или внешние автоматизированные системы.

ASP_DMO.1.3C В формулировке целей безопасности домена должны излагаться любые цели безопасности, которые задаются другим доменам или доступны им.

ASP_DMO.1.4C В формулировке целей безопасности домена должны излагаться любые цели безопасности для среды разработки домена.

ASP_DMO.1.5C В обосновании целей безопасности домена каждая уникальная цель безопасности для домена должна сопоставляться с рисками, которым противостояла эта цель безопасности и ПБОр, которым соответствовала эта цель безопасности.

ASP_DMO.1.6C В обосновании целей безопасности домена каждая уникальная цель безопасности для домена должна сопоставляться с рисками, которым противостояла эта цель безопасности и ПБОр, которым соответствовала эта цель безопасности.

ASP_DMO.1.7C В обосновании целей безопасности домена каждая уникальная цель безопасности для домена должна сопоставляться с рисками, которым противостояла эта цель безопасности и ПБОр, которым соответствовала эта цель безопасности.

ASP_DMO.1.8C Обоснование целей безопасности домена должно демонстрировать противодействие целей безопасности всем уникальным неприемлемым рискам для домена.

ASP_DMO.1.9C Обоснование целей безопасности домена должно демонстрировать выполнение целями безопасности всех уникальных ПБОр для домена.

С.2.13.2.3 Элементы действий оценщика

ASP_DMO.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_DMO.1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки целей безопасности домена.

ASP_DMO.1.3E Оценщик должен подтверждать согласование формулировки целей безопасности домена со спецификацией доменной организации.

С.2.14 Требования безопасности домена безопасности (ASP_DMR)

С.2.14.1 Цели

В данной части ПЗС представлено ясное и однозначное описание предполагаемого уникального поведения домена безопасности.

С.2.14.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются по уровням, исходя из того, заявлены ли они в оригинальном виде или выведены из целей безопасности для СОО и среды его разработки.

С.2.14.3 ASP_DMR.1 Заданные требования безопасности домена

Зависимости: ASP_ECD.1 Определение расширенных компонентов.

С.2.14.3.1 Элементы действий разработчика/интегратора

Зависимости: зависимости отсутствуют.

С.2.14.3.2 Элементы содержания и представления свидетельств

ASP_DMR.1.1C В формулировке требований безопасности домена должны излагаться уникальные ФБС и ДБС, применимые к домену.

ASP_DMR.1.2C В формулировке требований безопасности домена должны идентифицироваться все операции, связанные с требованиями безопасности.

ASP_DMR.1.3C Каждая зависимость между требованиями безопасности домена должна быть удовлетворена или идентифицирована как «неудовлетворенная».

С.2.14.3.3 Элементы действий оценщика

ASP_DMR.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASP_DMR.1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности домена.

С.2.14.4 ASP_DMR.2 Производные требования безопасности домена

Является иерархической для: ASP_DMR.1 Заданные требования безопасности домена.

Зависимости:

ASP_DMO.1 Цели безопасности домена безопасности;

ASP_ECD.1 Определение расширенных компонентов.

С.2.14.4.1 Элементы действий разработчика/интегратора

ASP_DMR.2.1D Разработчик/интегратор должен обеспечить обоснование требований безопасности домена.

С.2.14.4.2 Элементы содержания и представления свидетельств

ASP_DMR.2.1C В формулировке требований безопасности домена должны излагаться уникальные ФБС и ДБС, применимые к домену.

ASP_DMR.2.2C В формулировке требований безопасности домена должны идентифицироваться все операции, связанные с требованиями безопасности.

ASP_DMR.2.3C Все операции должны выполняться правильно.

ASP_DMR.2.4C Каждая зависимость между требованиями безопасности домена должна быть удовлетворена, или обоснование требований безопасности должно объяснять причину неудовлетворения зависимости.

ASP_DMR.2.5C В обосновании требований безопасности домена каждая ФБС домена должна сопоставляться с целями безопасности домена.

ASP_DMR.2.6C В обосновании требований безопасности домена каждая ФБС домена должна сопоставляться с целями безопасности домена или среды ее разработки.

ASP_DMR.2.7C Обоснование требований безопасности домена должно демонстрировать соответствие ФБС и ДБС домена всем уникальным целям безопасности для домена или среды его разработки, которым не соответствуют другие домены или внешние системы.

С.2.14.4.3 Элементы действий оценщика

ASP_DMR.2.1E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности домена.

ASP_DMR.2.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности домена.

С.3 Класс ASS: оценка задания по безопасности системы

С.3.1 Введение

В данном разделе представлены критерии доверия к оценке задания по безопасности системы (ЗБС). Оценка ЗБС требуется для демонстрации того, что ЗБС является обоснованным и внутренне непротиворечивым и, если ЗБС основано на одном или нескольких ПЗС или пакетах, что ЗБС является корректным представлением этих ПЗС и пакетов.

Ниже приведены семейства этого класса:

a) ASS_INT: Введение ЗБС;

b) ASS_CCL: Утверждения о соответствии;

c) ASS_SPD: Определение проблемы безопасности;

d) ASS_OBJ: Цели безопасности;

e) ASS_ECD: Определение компонентов расширения;

f) ASS_REQ: Требования безопасности;

g) ASS_TSS: Краткая спецификация СОО;

h) ASS_DMI: Введение домена безопасности;

i) ASS_DMC: Утверждение соответствия домена безопасности;

j) ASS_DMP: Определение проблем безопасности домена безопасности;

k) ASS_DMO: Цели безопасности домена безопасности;

l) ASS_DMR: Требования безопасности домена безопасности.

С.3.2 Общая часть ПЗС

Последующие спецификации применимы ко всему ПЗС. Спецификации для конкретных доменов должны описываться с помощью семейств доменов (см. С.3.10).

С.3.3 Введение ПЗС (ASS_INT)

С.3.3.1 Цели

Назначением данного семейства является изложение СОО в описательной форме на следующих уровнях абстракции: ссылка на ПЗС/СОО, краткий обзор СОО, описание СОО и организация доменов.

Оценка введения ПЗС требуется для демонстрации правильности идентификации СОО, правильности описания СОО на четырех уровнях абстракции и согласованности этих четырех описаний друг с другом. Введения конкретных доменов безопасности определены в С.3.11 «Введение доменов безопасности».

С.3.3.2 ASS_INT.1 Введение ПЗС

Зависимости: зависимости отсутствуют.

С.3.3.2.1 Элементы действий разработчика/интегратора

ASS_INT.1.1D Разработчик/интегратор должен обеспечить введение ПЗС.

С.3.3.2.2 Элементы содержания и представления свидетельств

ASS_INT.1.1C Введение ПЗС должно содержать ссылку на ПЗС, ссылку на СОО, краткий обзор СОО, описание СОО и спецификацию доменной организации.

ASS_INT.1.2C Ссылка на ПЗС должна однозначно идентифицировать ПЗС.

ASS_INT.1.3C Ссылка на СОО должна идентифицировать СОО.

ASS_INT.1.4C Краткий обзор СОО должен резюмировать использование и главные характеристики безопасности.

ASS_INT.1.5C Краткий обзор СОО должен идентифицировать тип СОО.

ASS_INT.1.6C Краткий обзор СОО должен идентифицировать взаимосвязи и интерфейсы с любыми внешними автоматизированными системами, требуемыми для СОО.

ASS_INT.1.7C В описании СОО должны быть описаны физическая область действия и границы СОО.

ASS_INT.1.8C В описании СОО должны быть описаны логическая область действия и границы СОО.

ASS_INT.1.9C В описании СОО должны быть описаны среды разработки для СОО, включая любые однозначные характеристики отдельных сред разработки доменов безопасности.

ASS_INT.10C В спецификации доменной организации должны быть описаны организация конструированных доменов безопасности и идентификация, область действия и границы каждого домена безопасности.

ASS_INT.11C Для каждого домена в спецификации доменной организации должны быть описаны любые услуги по обеспечению безопасности, предоставляемые для этого домена, доступные другим доменам, и любые характеристики безопасности домена, навязываемые другим доменам.

С.3.3.2.3 Элементы действий оценщика

ASS_INT.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_INT.1.2E Оценщик должен подтверждать согласование ссылки на СОО, краткого обзора СОО, описания СОО и спецификации доменной организации друг с другом.

С.3.4 Утверждения о соответствии (ASS_CCL)

С.3.4.1 Цели

Целью данного семейства является определение достоверности различных утверждений соответствия: утверждение соответствия стандартами серии ИСО/МЭК 15408, утверждение соответствия ПЗС, утверждение соответствия ПЗ, утверждение соответствия ЗБ и утверждение соответствия пакету требований. В утверждении соответствия стандартам серии ИСО/МЭК 15408 описывается версия ИСО/МЭК 15408, соответствие которой утверждают ПЗС и СОО, в утверждении соответствия ПЗ, ЗБ и/или пакету (если имеется) описывается, как ЗБС утверждает соответствие заданным ПЗ, ЗБ и/или пакетами, тогда как в утверждении ЗБС идентифицируются ПЗС (если имеются), соответствие которым утверждает ЗБС. Определение достоверности утверждений соответствия ПЗС, ПЗ, ЗБ и пакету требований влечет за собой определение четкости идентификации всех утвержденных ПЗС, ПЗ, ЗБ и пакетов — полностью ли эти ПЗС, ПЗ, ЗБ и пакеты содержатся в ПЗС и правильно ли выполнены требования безопасности, выведенные из этих ПЗС, ПЗ, ЗБ и пакетов. Утверждения соответствия для конкретного домена безопасности определены в подразделе С.3.12 «Утверждение соответствия домена безопасности».

С.3.4.2 ASS_CCL.1 Утверждения соответствия

Зависимости:

ASS_INT.1 Введение ЗБС;

ASS_SPD.1 Определение проблем безопасности;

ASS_OBJ.1 Цели безопасности;

ASS_ECD.1 Определение расширенных компонентов;

ASS_REQ.1 Заданные требования безопасности.

С.3.4.2.1 Элементы действий разработчика/интегратора

ASS_CCL.1.1D Разработчик/интегратор должен предоставить утверждение соответствия.

ASS_CCL.1.2D Разработчик/интегратор должен предоставить обоснование утверждения соответствия.

С.3.4.2.2 Элементы содержания и представления свидетельств

ASS_CCL.1.1C Утверждение соответствия должно содержать утверждение соответствия критериям, которое идентифицирует версию ИСО/МЭК ТО 19791, соответствие которому утверждают ЗБС и СОО.

ASS_CCL.1.2C В утверждении соответствия критериям должно описываться функциональное соответствие ЗБС ИСО/МЭК ТО 19791 или как полностью соответствующее ИСО/МЭК ТО 19791, или функционально дополненное.

ASS_CCL.1.3C В утверждении соответствия критериям должно описываться соответствие доверия ЗБС ИСО/МЭК ТО 19791 как совместимое по доверию или расширенное по доверию в ИСО/МЭК ТО 19791.

ASS_CCL.1.4C Утверждение соответствия критериям должно согласовываться с определением расширенных компонентов.

ASS_CCL.1.5C В заявлении о соответствии должны быть определены ПЗС, ПЗ, ЗБ и пакеты, о соответствии которым заявляется в ЗБС.

ASS_CCL.1.6C В утверждении соответствия должно описываться соответствие ЗБС пакету требований как полностью соответствующее или как дополнение к пакету.

ASS_CCL.1.7C В обосновании утверждений соответствия должно демонстрироваться соответствие типа СОО типу СОО в ПЗС, ПЗ, ЗБ и пакетах требований, соответствие которым утверждается.

ASS_CCL.1.8C Обоснование утверждений соответствия должно демонстрировать согласованность формулировки определения проблем безопасности с формулировкой определения проблем безопасности в ПЗС, ПЗ, ЗБ и пакетах, о соответствии которым делается утверждение.

ASS_CCL.1.9C Обоснование заявления о соответствии должно демонстрировать согласованность формулировки целей с формулировкой целей в ПЗС, ПЗ, ЗБ и пакетах, о соответствии которым делается утверждение.

ASS_CCL.1.10C Обоснование заявлений о соответствии должно демонстрировать согласованность формулировки с формулировкой требований безопасности в ПЗС, ПЗ, ЗБ и пакетах, о соответствии которым делается утверждение.

ASS_CCL.1.11C Обоснование утверждений соответствия должно демонстрировать завершение всех заимствованных из ПЗС, ПЗ, ЗБ или пакетов операций в соответствии с соответствующими ПЗС, ПЗ, ЗБ или пакетами.

С.3.4.2.3 Элементы действий оценщика

ASS_CCL.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_CCL.1.2E Оценщик должен подтверждать соответствие ЗБС утверждению соответствия стандартов серии ИСО/МЭК 15408.

С.3.5 Определение проблем безопасности (ASS_SPD)

С.3.5.1 Цели

В настоящей части ЗБС определяются проблемы безопасности, рассматриваемые СОО, включая среду ее разработки. Эти проблемы безопасности применимы к СОО в целом. Проблемы безопасности для конкретного домена безопасности определены в С.3.13. Оценка определения проблем безопасности требуется для демонстрации четкого определения проблем безопасности, предназначенных для рассмотрения СОО.

С.3.5.2 ASS_SPD.1 Определение проблем безопасности

Зависимости: зависимости отсутствуют.

С.3.5.2.1 Элементы действий разработчика/интегратора

ASS_SPD.1.1D Разработчик/интегратор должен предоставить определение проблем безопасности.

С.3.5.2.2 Элементы содержания и представления свидетельств

ASS_SPD.1.1C В определении проблем безопасности должны быть изложены все применимые к СОО риски. Каждый риск должен идентифицироваться как «приемлемый» или «неприемлемый».

ASS_SPD.1.2C Все неприемлемые риски должны быть описаны на основе угроз и уязвимостей. Каждая угроза должна описываться с точки зрения источника угрозы, актива и враждебности действия.

ASS_SPD.1.3C В определении проблем безопасности должны быть изложены ПБОр.

С.3.5.2.3 Элементы действий оценщика

ASS_SPD.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_SPD.1.2E Оценщик должен подтвердить внутреннюю непротиворечивость определения проблемы безопасности.

С.3.6 Цели безопасности (ASS_OBJ)

С.3.6.1 Цели

Цели безопасности представлены в краткой формулировке предполагаемой реакции на проблему безопасности, определенную посредством семейства ASS_SPD. Определенные цели безопасности в данной части применимы к СОО в целом. Цели безопасности для конкретного домена безопасности определены в С.3.14 «Цели безопасности домена безопасности». Оценка целей безопасности требуется для демонстрации того, что цели безопасности адекватно и полностью учитывают определение проблем безопасности, и распределение этой проблемы между СОО, средой ее разработки и внешними автоматизированными системами четко определено и что цели безопасности внутренне согласованы.

С.3.6.2. ASS_OBJ.1 Цели безопасности

Зависимости: ASS_SPD.1 Определение проблем безопасности.

С.3.6.2.1 Элементы действий разработчика/интегратора

ASS_OBJ.1.1D Разработчик/интегратор должен предоставить формулировку целей безопасности.

ASS_OBJ.1.2D Разработчик/интегратор должен предоставить обоснование целей безопасности.

С.3.6.2.2 Элементы содержания и представления свидетельств

SS_OBJ.1.1C В формулировке целей безопасности должны излагаться цели безопасности для СОО.

ASS_OBJ.1.2C В формулировке целей безопасности должны излагаться любые цели безопасности, которым соответствуют внешние автоматизированные системы.

ASS_OBJ.1.3C В формулировке целей безопасности должны излагаться цели безопасности для среды разработки.

ASS_OBJ.1.4C В обосновании целей безопасности каждая цель безопасности СОО должна сопоставляться с рисками, которым противостоит эта цель безопасности, и ПБОр, которым соответствует эта цель безопасности.

ASS_OBJ.1.1.5C В обосновании целей безопасности каждая цель безопасности для внешних автоматизированных систем должна сопоставляться с рисками, которым противостояла эта цель безопасности, и ПБОр, которым соответствовала эта цель безопасности.

ASS_OBJ.1.1.6C В обосновании целей безопасности каждая цель безопасности для среды разработки должна сопоставляться с рисками, которым противостояла эта цель безопасности, и ПБОр, которым соответствовала эта цель безопасности.

ASS_OBJ.1.1.7C В обосновании целей безопасности должно демонстрироваться противостояние целей безопасности всем неприемлемым рискам.

ASS_OBJ.1.8C Обоснование целей безопасности должно демонстрировать выполнение целями безопасности всех ПБОр.

С.3.6.2.3 Элементы действий оценщика

ASS_OBJ.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_OBJ.1.2E Оценщик должен подтверждать внутреннюю согласованность определения проблем безопасности.

С.3.7 Определение расширенных компонентов (ASS_ECD)

С.3.7.1 Цели

Расширенные требования безопасности основаны не на компонентах стандартов серии ИСО/МЭК 15408 или настоящего стандарта, а на расширенных компонентах, определенных автором ПЗС. Оценка определения расширенных компонентов необходима для определения их ясности, однозначности и необходимости, т.е. для того, чтобы они не могли быть выражены с помощью существующих компонентов стандартов серии ИСО/МЭК 15408 или настоящего стандарта.

С.3.7.2 ASS_ECD.1 Определение расширенных компонентов

Зависимости: зависимости отсутствуют.

С.3.7.3 Элементы действий разработчика/интегратора

ASS_ECD 1.1D Разработчик/интегратор должен предоставить формулировку требований безопасности.

ASS_ECD 1.2D Определение расширенных компонентов.

С.3.7.3.1 Элементы содержания и представления свидетельств

ASS_ECD 1.1C В формулировке требований безопасности должны быть определены все расширенные требования безопасности.

ASS_ECD.1.2C Определение расширенных компонентов должно определять расширенный компонент для каждого расширенного требования безопасности.

ASS_ECD.1.3C В определении расширенных компонентов должно быть описано, как каждый расширенный компонент связан с существующими компонентами, семействами и классами по стандартам серии ИСО/МЭК 15408.

ASS_ECD.1.4C В определении расширенных компонентов должны использоваться существующие компоненты, семейства и классы по стандартам сериии ИСО/МЭК 15408 и методология в качестве модели для представления.

ASS_ECD.1.5C Расширенные компоненты должны состоять из измеримых и объективных элементов для того, чтобы можно было продемонстрировать соответствие или несоответствие этим элементам.

С.3.7.3.2 Элементы действий оценщика

ASS_ECD.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_ECD.1.2E Оценщик должен подтверждать, что ни один расширенный компонент не может быть ясно выражен с помощью существующих компонентов.

С.3.8 Требования безопасности (ASS_REQ)

С.3.8.1 Цели

ФБС образуют ясное и недвусмысленное описание ожидаемого поведения СОО в сфере безопасности. ДБС образуют ясное и недвусмысленное описание предполагаемых действий, которые будут предприняты для

достижения доверия к СОО. Требования безопасности, определенные в данной части, применимы к СОО в целом. Требования безопасности для конкретного домена безопасности определены в С.3.15 «Требования безопасности к домену безопасности». Оценка требований безопасности требуется для обеспечения их четкости и недвусмысленности.

С.3.8.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются по уровням, исходя из того, заявлены ли они в оригинальном виде или выведены из целей безопасности для СОО и среды его разработки.

С.3.8.3 ASS_REQ.1 Заданные требования безопасности

Зависимости: ASS_ECD.1 Определение расширенных компонентов

С.3.8.3.1 Элементы действий разработчика/интегратора

Зависимости: зависимости отсутствуют.

С.3.8.3.2 Элементы содержания и представления свидетельств

ASS_REQ 1.1C В формулировке требований безопасности должны быть описаны ФБС и ДБС.

ASS_REQ 1.2C В формулировке требований безопасности должны быть определены все операции, связанные с требованиями безопасности.

ASS_REQ.1.3C Все операции «назначение» и «выбор» должны быть завершены.

ASS_REQ 1.4C Все операции должны быть правильно выполнены.

ASS_REQ 1.5C Каждая зависимость между требованиями безопасности должна быть или удовлетворена, или идентифицирована как «неудовлетворенная».

С.3.8.3.3 Элементы действий оценщика

ASS_REQ.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_REQ.1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности.

С.3.8.4 ASS_REQ.2 Производные требования безопасности

Являются иерархическими для: ASS_REQ.1 Заданные требования безопасности.

Зависимости: ASS_OBJ.1 Цели безопасности;
ASS_ECD.1 Определение расширенных компонентов.

С.3.8.4.1 Элементы действий разработчика/интегратора

ASS_REQ.2.1D Разработчик/интегратор должен предоставить обоснование требований безопасности.

С.3.8.4.2 Элементы содержания и представления свидетельств

ASS_REQ.2.1C В формулировке должны быть описаны ФБС и ДБС.

ASS_REQ.2.2C В формулировке должны быть определены все операции, связанные с требованиями безопасности.

ASS_REQ.2.3C Все операции по распределению и выбору должны быть завершены.

ASS_REQ.2.4C Все операции должны выполняться правильно.

ASS_REQ 2.5C Каждая зависимость между требованиями безопасности должна быть удовлетворена или идентифицирована как «неудовлетворенная».

ASS_REQ 2.6C Обоснование требований безопасности должно сопоставлять каждую ФБС с целями безопасности для СОО.

ASS_REQ 2.7C Обоснование требований безопасности должно сопоставлять каждую ДБС с целями безопасности для СОО или среды его разработки.

ASS_REQ 2.8C Обоснование требований безопасности должно демонстрировать соответствие ФБС и ДБС целям безопасности СОО и среды его разработки, которым не соответствуют внешние системы.

С.3.8.4.3 Элементы действий оценщика

ASS_REQ 2.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_REQ 2.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности.

С.3.9 Краткая спецификация СОО (ASS_TSS)

С.3.9.1 Цели

Целью краткой спецификации СОО является предоставление потенциальным заказчикам СОО описания на высоком уровне того, как разработчик/интегратор намеревается выполнить свои ФБС и ДБС. Краткая спецификация СОО должна оказать помощь оценщикам и потенциальным заказчикам в понимании того, насколько СОО соответствует их ФБС и ДБС. Определенная в данной части краткая спецификация СОО применима к СОО в целом. Краткая спецификация безопасности для конкретного домена безопасности определена в С.3.16 «Краткая спецификация домена безопасности (ASS_DMS)». Оценка краткой спецификации СОО необходима для определения адекватности рассмотрения всех ФБС и согласованности краткой спецификации СОО с другими описаниями СОО.

С.3.9.2 ASS_TSS.1 Краткая спецификация СОО

Зависимости:

ASS_INT.1 Введение ЗБС;

ASS_REQ.1 Заданные требования безопасности.

С.3.9.2.1 Элементы действий разработчика/интегратора

ASS_TSS.1.1D Разработчик/интегратор должен предоставить краткую спецификацию СОО.

С.3.9.2.2 Элементы содержания и представления свидетельств

ASS_TSS.1.1C В краткой спецификации СОО должно быть описано, как СОО соответствует каждой ФБС.

ASS_TSS.1.2C В краткой спецификации СОО должно быть описано, как СОО и среда его разработки соответствует каждой ДБС.

С.3.9.2.3 Элементы действий оценщика

ASS_TSS.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_TSS.1.2E Оценщик должен подтверждать согласование краткой спецификации СОО с кратким обзором и описанием СОО.

С.3.10 Домены безопасности системы как объекта защиты

Каждый домен безопасности СОО определяет проблемы, цели и требования безопасности, уникальные для этого конкретного домена безопасности.

В последующих семействах определены семейства, используемые для определения доменов безопасности в СОО.

С.3.11 Введение доменов безопасности (ASS_DMI)

С.3.11.1 Цели

Целью данного семейства является описание домена безопасности в повествовательной форме на следующих уровнях абстракции: ссылка на домен безопасности, краткий обзор домена безопасности и описание домена безопасности.

С.3.11.2 ASS_DMI.1 Введение домена безопасности

Зависимости: ASS_INT.1 Введение ЗБС.

С.3.11.2.1 Элементы действий разработчика/интегратора

ASS_DMI.1.1D Разработчик/интегратор должен обеспечить введение домена безопасности.

С.3.11.2.2 Элементы содержания и представления свидетельств

ASS_DMI.1.1C Введение домена безопасности должно содержать ссылку, краткий обзор и описание домена безопасности.

ASS_DMI.1.2C Ссылка на домен безопасности должна однозначно определять домен безопасности.

ASS_DMI.1.3C Обзор домена безопасности должен резюмировать использование и главные характеристики безопасности домена безопасности.

ASS_DMI.1.4C В описании домена безопасности должны излагаться включенные подсистемы и компоненты.

ASS_DMI.1.5C В описании домена безопасности должны излагаться взаимосвязи и интерфейсы с другими системами.

С.3.11.2.3 Элементы действий оценщика

ASS_DMI.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_DMI.1.2E Оценщик должен подтверждать согласованность домена безопасности, краткого обзора домена безопасности и описания домена безопасности друг с другом и с введением СОО.

С.3.12 Утверждение соответствия доменов безопасности (ASS_DMC)

С.3.12.1 Цели

В данной части ЗБС определяется специфическое утверждение соответствия для домена безопасности.

С.3.12.2 ASS_DMC.1 Утверждения соответствия

Зависимости:

ASS_DMP.1 Определение проблем безопасности для доменов безопасности;

ASS_DMO.1 Цели безопасности доменов безопасности;

ASS_DMR.1 Заданные требования безопасности для домена.

С.3.12.2.1 Элементы действий разработчика/интегратора

ASS_DMC.1.1D Утверждение соответствия домена.

ASS_DMC.1.2D Разработчик/интегратор должен предоставить обоснование утверждения соответствия домена.

С.3.12.2.2 Элементы содержания и представления свидетельств

ASS_DMC.1.1C В заявлении о соответствии должны быть определены все ПЗС, ПЗ и пакеты требований безопасности, о соответствии которым утверждает домен.

ASS_DMC.1.2C В заявлении о соответствии домена должно быть изложено любое соответствие домена пакету как соответствующее полностью или приданное пакету.

ASS_DMC.1.3C Обоснование утверждения соответствия домена должно демонстрировать согласованность типа СОО с типом СОО в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASS_DMC.1.4C Обоснование утверждения соответствия домена должно демонстрировать согласованность формулировки определения проблемы безопасности домена с формулировкой определения проблемы безопасности в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASS_DMC.1.5C Обоснование утверждения соответствия домена должно демонстрировать согласованность формулировки целей безопасности домена с формулировкой целей безопасности в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASS_DMC.1.6C Обоснование утверждения соответствия домена должно демонстрировать согласованность формулировки требований безопасности домена с формулировкой требований безопасности в ПЗС, ПЗ и пакетах, о соответствии которым делается утверждение.

ASS_DMC.1.7C Обоснование утверждения соответствия домена должно демонстрировать, что все операции, связанные с требованиями безопасности, заимствованными из ПЗС, ПЗ и пакета, завершены в согласовании с соответствующими ПЗС, ПЗ и пакетом.

С.3.12.2.3 Элементы действий оценщика

ASS_DMC1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.3.13 Проблемы безопасности домена безопасности (ASS_DMP)

С.3.13.1 Цели

В данной части ЗБС определены специфические проблемы безопасности, относящиеся к какому-либо домену безопасности.

С.3.13.2 ASS_DMP.1 Определение проблем безопасности домена безопасности

Зависимости: зависимости отсутствуют.

ASS_DMP.1.1D Разработчик/интегратор должен предоставить определение проблем безопасности домена.

С.3.13.2.2 Элементы содержания и представления свидетельств

ASS_DMP.1.1C В определении проблем безопасности домена должны быть описаны все уникальные риски, применимые к домену. Каждый риск должен категорироваться как «приемлемый» или «неприемлемый».

ASS_DMP.1.2C Все неприемлемые риски должны быть изложены, исходя из угроз и уязвимостей. Каждая угроза должна быть изложены, исходя из источника угрозы, актива и враждебности действия.

ASS_DMP.1.3C В определении проблем безопасности домена должны быть описаны уникальные ПБОр, применимые к домену.

С.3.13.2.3 Элементы действий оценщика

ASS_DMP.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_DMP.1.2E Оценщик должен подтверждать внутреннюю согласованность определения проблем безопасности домена.

С.3.14 Цели безопасности домена безопасности (ASS_DMO)

С.3.14.1 Цели

В данной части ЗБС представлена краткая формулировка предполагаемого реагирования на уникальные проблемы безопасности домена, определенные с помощью семейства ASS_DMP.

С.3.14.2 ASS_DMO 1 Цели безопасности домена безопасности

Зависимости:

ASS_INT.1 Введение ЗБС;

ASS_DMP.1 Определение проблем безопасности домена безопасности.

С.3.14.2.1Элементы действий разработчика/интегратора

ASS_DMO.1.1D Разработчик/интегратор должен предоставить формулировку целей безопасности домена.

ASS_DMO.1.2D Разработчик/интегратор должен предоставить обоснование целей безопасности домена.

С.3.14.2.2 Элементы содержания и представления свидетельств

ASS_DMO.1.1C В формулировке целей безопасности домена должны быть описаны уникальные цели безопасности для домена.

ASS_DMO.1.2C В формулировке целей безопасности домена должны быть описаны любые цели безопасности для домена, которым соответствуют другие домены или внешние автоматизированные системы.

ASS_DMO.1.3C В формулировке целей безопасности домена должны быть описаны любые цели безопасности для домена, которые задаются другим доменам или доступны им.

ASS_DMO.1.4C В формулировке целей безопасности домена должны быть описаны уникальные цели безопасности для среды разработки домена.

ASS_DMO.1.5C Обоснование целей безопасности должно сопоставлять каждую уникальную цель безопасности для домена с рисками, которым противостояла эта цель безопасности, и ПБОр, которым соответствовала эта цель безопасности.

ASS_DMO.1.6C Обоснование целей безопасности должно сопоставлять каждую уникальную цель безопасности для среды разработки домена с рисками, которым противостояла эта цель безопасности, и ПБОр, которым соответствовала эта цель безопасности.

ASS_DMO.1.7C Обоснование целей безопасности должно сопоставлять каждую уникальную цель безопасности для других доменов с рисками, которым противостояла эта цель безопасности, и ПБОр, которым соответствовала эта цель безопасности.

ASS_DMO.1.8C Обоснование целей безопасности должно демонстрировать противодействие целей безопасности всем неприемлемым рискам, уникальным для домена.

ASS _DMO.1.9C Обоснование целей безопасности должно демонстрировать выполнение всеми целями безопасности всех уникальных ПБОр для домена.

С.3.14.2.3 Элементы действий оценщика

ASS_DMO1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_DMO.1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки целей безопасности домена.

ASS_DMO.1.3E Оценщик должен подтверждать согласованность формулировки целей безопасности домена со спецификацией доменной организации.

С.3.15 Требования безопасности домена безопасности (ASS_DMR)

С.3.15.1 Цели

В данной части ЗБС представляется четкое и однозначное описание ожидаемого уникального поведения доменов безопасности.

С.3.15.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются по уровням, исходя из того, заявлены ли они в оригинальном виде или выведены из целей безопасности для СОО и среды его разработки.

С.3.15.2.1 Элементы действий разработчика/интегратора

Зависимости: зависимости отсутствуют.

С.3.15.3.2 Элементы содержания и представления свидетельств

ASS_DMR.1.1C В формулировке требований безопасности домена должны быть описаны уникальные ФБС и ДБС, применимые к этому домену.

ASS_DMR.1.2C В формулировке требований безопасности домена должны быть определены все операции, связанные с требованиями безопасности.

ASS_DMR.1.3C Все операции по распределению и выбору должны быть завершены.

ASS_DMR.1.4C Все операции должны выполняться правильно.

ASS_DMR.1.5C Каждая зависимость между требованиями безопасности должна быть или удовлетворена, или идентифицирована как «неудовлетворенная».

С.3.15.3.3 Элементы действий оценщика

ASS_DMR.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_DMR.1.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности домена.

С.3.15.4 ASS_DMR.2 Производные требования безопасности домена

Является иерархическим для: ASS_DMR.1 Заданные требования безопасности домена.

Зависимости:

ASS_DMO.1 Цели безопасности домена безопасности;

ASS_ECD.1 Определение расширенных компонентов.

С.3.15.4.1 Элементы действий разработчика/интегратора

ASS_DMO.1.1D Разработчик/интегратор должен предоставить обоснование требований безопасности домена.

С.3.15.4.2 Элементы содержания и представления свидетельств

ASS_DMR.2.1C В формулировке требований безопасности домена должны быть описаны уникальные ФБС и ДБС, применимые к этому домену.

ASS_DMR.2.2C В формулировке требований безопасности домена должны быть определены все операции, связанные с требованиями безопасности.

ASS_DMR.2.3C Все операции по распределению и выбору должны быть завершены.

ASS_DMR.2.4C Все операции должны выполняться правильно.

ASS_DMR.2.5C Каждая зависимость между требованиями безопасности домена должна быть удовлетворена или идентифицирована как «неудовлетворенная».

ASS_DMR.2.6C Обоснование требований безопасности домена должно сопоставлять каждую ФБС домена с целями безопасности для домена.

ASS_DMR.2.7C Обоснование требований безопасности домена должно сопоставлять каждую ФБС домена с целями безопасности для домена и среды его разработки.

ASS_DMR.2.8C Обоснование требований безопасности домена должно демонстрировать соответствие ФБС и ДБС домена всем уникальным целям безопасности для домена и среды его разработки, которым не соответствуют другие домены или внешние системы.

С.3.15.4.3 Элементы действий оценщика

ASS_DMR.2.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_DMR.2.2E Оценщик должен подтверждать внутреннюю согласованность формулировки требований безопасности домена.

С.3.16 Краткая спецификация домена безопасности (ASS_DMS)

С.3.16.1 Цели

В данной части ЗБС определяется краткая спецификация домена безопасности.

С.3.16.2 ASS_DMS.1 Краткая спецификация домена безопасности

Зависимости:

ASS_DMI.1 Введение домена безопасности;

ASS_DMR.1 Требования безопасности домена безопасности.

С.3.16.2.1 Элементы действий разработчика/интегратора

ASS_DMS.1.1D Разработчик/интегратор должен предоставить краткую спецификацию домена.

С.3.16.2.2 Элементы содержания и представления свидетельств

ASS_DMS.1.1C В краткой спецификации домена должно быть описано, как домен соответствует каждой ФБС домена.

ASS_DMS.1.2C В краткой спецификации домена должно быть описано, как домен и его среда разработки соответствует каждой ДБС домена.

С.3.16.2.3 Элементы действий оценщика

ASS_DMS 1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASS_MS 1.2E Оценщик должен подтверждать согласованность краткой спецификации домена с кратким обзором домена и описанием домена.

С.4 Класс AOD: руководства для автоматизированных систем

С.4.1 Введение

Целью группы руководств по автоматизированной системе является принятие решения об адекватности документации, описывающей интеграцию и организационную структуру автоматизированной системы. Такая документация включает в себя документацию для интеграторов автоматизированной системы, доверенных администраторов и пользователей, не являющихся администраторами, чьи неправильные действия могут неблагоприятно воздействовать на состояние безопасности и характеристики автоматизированной системы, а также документацию, предназначенную для обычных пользователей, чьи неправильные действия могут неблагоприятно воздействовать на способность автоматизированной системы обеспечивать необходимые возможности защиты собственных данных.

Следовательно, действия AOD тесно связаны с процессами и процедурами, определенными организационными требованиями безопасности. Руководство для пользователя и администратора включает в себя информацию, относящуюся к технологическим аспектам автоматизированной системы, а также к процессам эксплуатации автоматизированной системы с участием человека.

С.4.2 Замечания по применению

Все требования к ФЭБ, определенные в ЗБС, по мере их применения к требуемому поведению персонала должны быть изложены в соответствующем руководстве по автоматизированной системе.

Необходимо определить профилактический режим, режим одного пользователя и любой специальный режим функционирования, следующие за ошибкой или исключением, и рассмотреть их на предмет последствий и воздействия на поддержание надежного функционирования.

В руководстве для администратора должна быть определена следующая информация:

- функции и привилегии, подлежащие контролю;
- типы необходимых мер контроля;
- причины применения мер обеспечения безопасности.

В руководство для администратора необходимо включить предупреждения об ожидаемых эффектах, возможных побочных эффектах и возможных взаимодействиях с другими функциями и привилегиями.

В руководстве для администратора должно быть изложено административное управление автоматизированной системой в целом в дополнение к управлению отдельными продуктами и подсистемами. Руководство для администратора, предназначенное не только для прикладных программ, но и для всей автоматизированной системы, должно быть документированным.

С.4.3 Спецификация конфигурации автоматизированной системы (AOD_OCD)

С.4.3.1 Цели

Назначением спецификации конфигурации автоматизированной системы является определение параметров конфигурации, релевантных для безопасности, которые поддерживают интеграцию компонентов автоматизированной системы и позволяют функциям безопасности автоматизированной системы внедрять и осуществлять концепцию безопасности функционирования и связанных с ним политик автоматизированной системы.

С.4.3.2 Ранжирование компонентов

Семейство состоит из двух компонентов. Эти компоненты распределяют по уровням на основе подтверждения изложения в документации и проверок в автоматизированной системе.

С.4.3.3 AOD_OCD.1 Спецификация конфигурации автоматизированной системы

Зависимости:

ASD_CON.1 Концепция безопасности операций;

ASD_CMP.1 Конструкция компонентов.

С.4.3.3.1 Элементы действий разработчика/интегратора

AOD_OCD.1.1D Разработчик/интегратор должен предоставлять спецификацию конфигурации, определяющую параметры конфигурации, требуемые для безопасности, которые поддерживают интеграцию компонентов автоматизированной системы и позволяют функциям безопасности автоматизированной системы внедрять и осуществлять концепцию безопасности функционирования и связанных с ним политик автоматизированной системы.

С.4.3.3.2 Элементы содержания и представления свидетельств

AOD_OCD.1.1C В спецификации конфигурации должны быть изложены все требования к конфигурации, относящиеся к СОО, включая среду ее эксплуатации.

AOD_OCD.1.2C В спецификации конфигурации должны быть изложены параметры конфигурации безопасности, доступные системному интегратору или равнозначным им пользователям/администраторам с такой же ролью и обязанностью.

AOD_OCD.1.3C В спецификации конфигурации должно быть изложено применение параметров безопасности, конфигурированных СОО для внедрения и осуществления политик безопасности системы.

AOD_OCD.1.4C В спецификации конфигурации должны содержаться предупреждения о доступных функциях и привилегиях конфигурации, которые должны контролироваться в защищенной среде обработки.

AOD_OCD.1.5C В спецификации конфигурации должны быть четко представлены связанные с конфигурацией обязанности, необходимые для безопасного функционирования СОО.

AOD_OCD.1.6C Спецификация конфигурации должна быть согласована со всей остальной документацией, представленной для оценки.

AOD_OCD.1.7C В спецификации конфигурации должна быть отражена реализация параметров безопасности компонентов, необходимых по концепции безопасности операций, в конструкции компонентов.

С.4.3.3.3 Элементы действий оценщика

AOD_OCD.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.4.3.4 AOD_OCD.2 Проверка спецификации конфигурации автоматизированной системы

Является иерархической для: AOD_OCD.1 Спецификация конфигурации автоматизированной системы.

Зависимости:

ASD_CON.1 Понятие безопасности операций;

ASD_CMP.1 Конструкция компонентов.

С.4.3.4.1 Элементы действий разработчика/интегратора

AOD_OCD.2.1D Разработчик/интегратор должен предоставлять спецификацию конфигурации, определяющую параметры конфигурации, релевантные для безопасности, которые поддерживают интеграцию компонентов системы и позволяют функциям безопасности автоматизированной системы внедрять и осуществлять концепцию безопасности функционирования и связанных с ним политик.

С.4.3.4.2 Элементы содержания и представления свидетельств

AOD_OCD.2.1C В спецификации конфигурации должны быть изложены все требования к конфигурации, относящиеся к СОО, включая среду ее эксплуатации.

AOD_OCD.2.2C В спецификации конфигурации должны быть изложены параметры конфигурации безопасности, доступные системному интегратору или равнозначным ему пользователям/администраторам с такой же ролью и обязанностью.

AOD_OCD.2.3C В спецификации конфигурации должно быть изложено применение параметров безопасности, сконфигурированных СОО для внедрения и осуществления политик безопасности системы.

AOD_OCD.2.4C В спецификации конфигурации должны содержаться предупреждения о доступных функциях и привилегиях конфигурации, которые должны контролироваться в защищенной среде обработки.

AOD_OCD.2.5C В спецификации конфигурации должны быть четко представлены связанные с конфигурацией обязанности, необходимые для безопасного функционирования СОО.

AOD_OCD.2.6C Спецификация конфигурации должна быть согласована со всей остальной документацией, представленной для оценки.

AOD_OCD.2.7C В спецификации конфигурации должна быть отражена реализация всех параметров безопасности компонентов, необходимых по концепции безопасности операций, в конструкции компонентов.

С.4.3.4.3 Элементы действий оценщика

AOD_OCD.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOD_OCD.2.2E Оценщик должен независимо проверять практитическое применение параметров конфигурации, определенное в спецификации конфигурации.

С.4.4 Руководство администратора автоматизированной системы (AOD_ADM)

С.4.4.1 Цели

Руководство администратора автоматизированной системы предназначено для лиц, ответственных за правильное конфигурирование, обслуживание и управление СОО в отношении обеспечения безопасности. В руководстве администратора также должны быть изложены политика, правила и процедуры обеспечения безопасности, определенные организационными требованиями и предназначенные для использования администраторами. Руководство администратора автоматизированной системы предназначено для оказания помощи администраторам в понимании мер обеспечения безопасности, установленных для СОО, включая как технические, так и организационные меры безопасности, которые требуют от администратора выполнения критичных для обеспечения безопасности действий.

С.4.4.2 Ранжирование компонентов

Семейство состоит из двух компонентов. Эти компоненты распределяются по уровням на основе подтверждения изложения в документации и проверок автоматизированной системы.

С.4.4.3 Замечания по применению

Содержимое руководства администратора непосредственно отражает политики, правила, обязанности, процедуры и организационные меры безопасности, связанные с администратором и определенные в организационных мерах безопасности. Требования AOD_ADM.1.3C и AOD_ADM.1.7C относятся к аспекту соответствующего представления всех предупреждений для пользователей СОО в отношении среды безопасности СОО и целей безопасности, изложенных в ПЗС/ЗБС.

Концепция защищенных значений в том виде, в котором она используется в AOD_ADM.1.6C, уместна в случае, если администратор осуществляет контроль за параметрами безопасности. Требуется руководство по защищенным и незащищенным установкам таких параметров.

С.4.4.4 AOD_ADM.1 Руководство администратора

Зависимости: ASD_SAD.1 Описание архитектуры.

С.4.4.4.1 Элементы действий администрации

AOD_ADM.1.1M Администрация должна обеспечить персонал управления системой руководством администратора автоматизированной системы.

С.4.4.4.2 Элементы содержания и представления свидетельств

AOD_ADM.1.1C В руководстве администратора должны излагаться административные функции и интерфейсы, доступные администратору СОО.

AOD_ADM.1.2C В руководстве администратора должны правильно излагаться требования организационного контроля, относящиеся к администратору.

AOD_ADM.1.3C В руководстве администратора должно излагаться безопасное управление СОО.

AOD_ADM.1.4C В руководстве администратора должны содержаться предупреждения о функциях и привилегиях, которые подлежат контролю в безопасной среде обработки.

AOD_ADM.1.5C В руководстве администратора должны описываться операции, имеющие отношение к поведению пользователя, которые связаны с безопасным функционированием СОО.

AOD_ADM.1.6C В руководстве администратора должны излагаться параметры безопасности, находящиеся под контролем администратора, при необходимости, с указанием безопасных значений.

AOD_ADM.1.7C В руководстве администратора должен описываться каждый тип связанного с безопасностью события, относящегося к административным функциям, предназначенным для выполнения, включая изменение характеристик безопасности, контролируемых ФБС.

AOD_ADM.1.8C Руководство администратора должно согласовываться со всей другой документацией, представленной для оценки.

AOD_ADM.1.9C В руководстве администратора должны описываться интерфейсы к внешним автоматизированным системам, относящиеся к администратору.

С.4.4.4.3 Элементы действий оценщика

AOD_ADM.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.4.4.5 AOD_ADM.2 Верификация

Является иерархическим для: AOD_ADM.1 Руководство администратора.

Зависимости: ASD_SAD.1 Описание архитектуры.

С.4.4.5.1 Элементы действий администрации

AOD_ADM.2.1M Администрация должна обеспечивать персонал управления системой руководством администратора автоматизированной системы.

С.4.4.5.2 Элементы содержания и представления свидетельств

AOD_ADM.2.1C В руководстве администратора должны описываться административные функции и интерфейсы, доступные администратору СОО.

AOD_ADM.2.2C В руководстве администратора должны правильно излагаться требования организационного контроля, относящиеся к администратору.

AOD_ADM.2.3C В руководстве администратора должно излагаться безопасное управление СОО.

AOD_ADM.2.4C В руководстве администратора должны содержаться предупреждения о функциях и привилегиях, которые подлежат контролю в безопасной среде обработки.

AOD_ADM.2.5C В руководстве администратора должны описываться все операции, имеющие отношение к поведению пользователя, которые связаны с безопасным функционированием СОО.

AOD_ADM.2.6C В руководстве администратора должны быть приведены все управляемые администратором параметры безопасности, обозначающие соответствующие безопасные значения.

AOD_ADM.2.7C В руководстве администратора должен описываться каждый тип связанного с безопасностью события, относящегося к административным функциям, предназначенным для выполнения, включая изменение характеристик сущностей, находящихся под управлением ФБС.

AOD_ADM.2.8C Руководство администратора должно согласовываться со всей другой документацией, представленной для оценки.

AOD_ADM.2.9C В руководстве администратора должны описываться все интерфейсы к внешним автоматизированным системам, относящиеся к администратору.

С.4.4.5.3 Элементы действий оценщика

AOD_ADM.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOD_ADM.2.2E Оценщик должен независимо верифицировать, посредством опроса персонала, выборки из руководства администратора и др., практическое применение руководства администратора.

С.4.5 Руководство пользователя автоматизированной системы (AOD_USR)

С.4.5.1 Цели

Руководство пользователя автоматизированной системы предназначено для не связанного с управлением человека — пользователя СОО. В руководстве пользователя должны быть изложены политика безопасности, процедуры, правила, обязанности и другие требования безопасности, определенные организационными требованиями и предназначенные для пользователей. В руководстве пользователя автоматизированной системы описаны меры обеспечения безопасности, предоставляемые ФБС, а также инструкции и рекомендации, включая предупреждения, для безопасного применения.

Руководство пользователя автоматизированной системы обеспечивает основу для работы с использованием СОО и уверенность в том, что свои пользователи, поставщики прикладных программ и другие лица, использующие внешние интерфейсы СОО, правильно поймут принцип безопасного функционирования СОО и будут использовать его должным образом.

С.4.5.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты распределяют по уровням на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.4.5.3 Замечания по применению

Содержимое руководства пользователя непосредственно отражает политики, правила, обязанности, процедуры и организационные меры безопасности, связанные с администратором и определенные в организационных мерах безопасности. Требование AOD_USR.1.4.C обеспечивает соответствующее представление предупреждений пользователям СОО в отношении среды безопасности СОО и целей безопасности, изложенных в ПБС/ЗБС в руководстве пользователя.

С.4.5.4 AOD_USR.1 Руководство пользователя

Зависимости: ASD_SAD.1 Описание архитектуры.

С.4.5.4.1 Элементы действий администрации

AOD_USR.1.1M Администрация должна при необходимости предоставлять руководство пользователя.

С.4.5.4.2 Элементы содержания и представления свидетельств

AOD_USR.1.1C В руководстве пользователя должны описываться функции и интерфейсы, доступные для не связанных с управлением пользователей СОО.

AOD_USR.1.2C В руководстве пользователя должны описываться организационные меры безопасности, связанные с пользователем.

AOD_USR.1.3C В руководстве пользователя должно описываться использование доступных пользователю функций безопасности, обеспечиваемых СОО.

AOD_USR.1.4C В руководстве пользователя должны содержаться предупреждения о доступных пользователю функциях и привилегиях, которые подлежат контролю в безопасной среде обработки.

AOD_USR.1.5C В руководстве пользователя должны быть четко представлены обязанности пользователя, необходимые для обеспечения безопасного функционирования СОО, включая обязанности, связанные с поведением пользователя во время эксплуатации системы.

AOD_USR.1.6C Руководство пользователя должно согласовываться с другой документацией, представленной для оценки.

С.4.5.4.3 Элементы действий оценщика

AOD_USR.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.4.5.5 Верификация руководства пользователя

Является иерархическим для: AOD_USR.1 Руководство пользователя.

Зависимости: ASD_SAD.1 Описание архитектуры.

С.4.5.5.1 Элементы действий администрации

AOD_USR.2.1M Администрация должна обеспечить наличие в организации руководства пользователя.

С.4.5.5.2 Элементы содержания и представления свидетельств

AOD_USR.2.1C В руководстве пользователя должны описываться функции и интерфейсы, доступные для не связанных с управлением пользователей СОО.

AOD_USR.2.2C В руководстве пользователя должны описываться организационные меры безопасности, связанные с пользователем.

AOD_USR.2.3C В руководстве пользователя должно описываться использование доступных пользователю функций безопасности, обеспечиваемых СОО.

AOD_USR.2.4C В руководстве пользователя должны содержаться предупреждения о доступных пользователю функциях и привилегиях, которые подлежат контролю в безопасной среде обработки.

AOD_USR.2.5C В руководстве пользователя должны быть четко представлены обязанности пользователя, необходимые для обеспечения безопасного функционирования СОО, включая обязанности, связанные с поведением пользователя во время эксплуатации системы.

AOD_USR.2.6C Руководство пользователя должно согласовываться со всей другой документацией, представленной для оценки.

С.4.5.5.3 Элементы действий оценщика

AOD_USR.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOD_USR.2.2E Оценщик должен независимо проверять посредством опросов персонала, выборки из руководства администратора, других методов практического применения спецификации руководства администратора.

С.4.6 Верификация руководств (AOD_GVR)

С.4.6.1 Цели

Целью является продемонстрировать, что документация руководства остается адекватной после внесения изменений и модификаций в компоненты системы, конфигурацию системы или среду эксплуатации.

С.4.6.2 Ранжирование компонентов

Имеется один компонент.

С.4.6.3 AOD_GVR.1 Верификация руководства

Зависимости:

AOD_OCD.1 Спецификация конфигурации автоматизированной системы;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.4.6.3.1 Цели

Назначением данного компонента является продемонстрировать, что документация руководства остается адекватной после внесения изменений и модификаций в компоненты системы, конфигурацию системы или среду эксплуатации.

С.4.6.3.2 Замечания по применению

Данный компонент рассматривает не только измененные или модифицированные части автоматизированной системы, но также части, которые могли стать недействительными (неисправными).

С.4.6.3.3 Элементы действий разработчика/интегратора

AOD_GVR.1.1D После внесения изменений и модификаций в компоненты системы, конфигурацию системы или среду эксплуатации разработчик/интегратор должен провести верифицирующий анализ для проверки, остались ли конфигурация автоматизированной системы и документация руководства правильными и согласованными.

С.4.6.3.4 Элементы содержания и представления свидетельств

AOD_GVR.1.1C По каждому документу конфигурации верифицирующий анализ должен показать его неизменность после внесения изменений или модификаций в компоненты или его правильное обновление для отражения изменений или модификаций.

AOD_GVR.1.2C По каждому руководству администратора верифицирующий анализ должен показать его неизменность после внесения изменений или модификаций в компоненты или его правильное обновление для отражения изменений или модификаций.

AOD_GVR.1.3C По каждому руководству пользователя верифицирующий анализ должен показать его неизменность после внесения изменений или модификаций в компоненты или его правильное обновление для отражения изменений или модификаций.

С.4.6.3.5 Элементы действий оценщика

AOD_GVR.1.1C Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.5 Класс ASD: документация по проектированию архитектуры автоматизированных систем и конфигурационная документация

С.5.1 Введение

Класс доверия ASD является производным класса по ИСО/МЭК 15408-3. Однако информация по разработке и интеграции, необходимая для автоматизированных систем, настолько отлична от информации в классе ADV, что возникла потребность в определении нового класса.

Целью создания этого класса является оценка решений по конфигурации, проектированию и архитектуре, принятых для обеспечения их достаточности и завершенности, исходя из соответствия функциональным требованиям, предъявляемым к автоматизированной системе. Понимание этих решений обеспечивается именно посредством ознакомления с документацией по конфигурации, проектированию и архитектуре. Второй целью данного раздела является проверка отражения в конфигурации, проектировании и архитектуре автоматизированной системы функциональных требований, предъявляемых различным подсистемам и компонентам автоматизированной системы. Для этого необходимо определить характеристики безопасности всех внутренних интерфейсов наряду с такими характеристиками безопасности (например, разделение адресного пространства), которые навязываются одним элементом архитектуры другим элементам.

С.5.2 Описание архитектуры (ASD_SAD)

С.5.2.1 Цели

Целью описания архитектуры автоматизированной системы является представление подробного обсуждения характеристик безопасности автоматизированной системы, созданных, исходя из структуры (подсистем, компонентов, интерфейсов с внешними автоматизированными системами), взаимодействия (интерфейсы, межсоединения, данные и потоки управления) и назначения (трактовка концепции безопасности операций и требований безопасности автоматизированной системы), а также присвоение различных степеней (уровней) доверия различным частям автоматизированной системы. Эта информация оказывает содействие в понимании и реализации некоторых аспектов оценки автоматизированной системы: присвоение доверия частям автоматизированной системы, концепция безопасности операций этой системы, процедуры, планы и стратегия испытаний автоматизированной системы. Назначением свидетельства описания архитектуры является предоставление описания следующих аспектов автоматизированной системы:

а) определение подсистем, составляющих автоматизированную систему;

в) внутренние и внешние интерфейсы для подсистем и выполняемые функции, предоставляемые посредством идентифицированных интерфейсов;

с) соединения между подсистемами и поток информации между подсистемами, проходящий через эти соединения;

d) внешние автоматизированные системы, с которыми сопряжена данная автоматизированная система и взаимосвязи между данной автоматизированной системой и этими внешними автоматизированными системами;

е) межсоединения для внешних автоматизированных систем и поток информации, проходящий между данной автоматизированной системой и внешними автоматизированными системами через эти межсоединения;

f) меры защиты и осуществление правильного функционирования мер обеспечения безопасности.

С.5.2.2 Ранжирование компонентов

Семейство состоит из одного компонента.

С.5.2.3 ASD_SAD.1 Описание архитектуры

Зависимости: зависимости отсутствуют.

С.5.2.3.1 Элементы действий разработчика/интегратора

ASD_SAD.1.1D Разработчик/интегратор должен обеспечить описание архитектуры.

С.5.2.3.2 Элементы содержания и представления свидетельств

ASD_SAD.1.1C Описание архитектуры должно определять автоматизированную систему, исходя из ее подсистем, интерфейсов и соединений между подсистемами.

ASD_SAD.1.2C Описание архитектуры должно определять внешние автоматизированные системы, взаимосвязанные с данной автоматизированной системой, и интерфейсы и соединения между данной автоматизированной системой и внешними автоматизированными системами.

ASD_SAD.1.3C В описании архитектуры должны излагаться назначение и функции идентифицированных подсистем, межсоединения и интерфейсы данной автоматизированной системы.

ASD_SAD.1.4C В описании архитектуры должны излагаться назначение идентифицированных межсоединений и интерфейсов от данной автоматизированной системы внешним автоматизированным системам, а также услуги, предоставляемые внешним автоматизированным системам, и услуги, предоставляемые этими системами.

ASD_SAD.1.5C В описании архитектуры должны излагаться все характеристики безопасности автоматизированной системы, которые переносятся одним элементом архитектуры на другие, включая меры защиты мер обеспечения безопасности от несанкционированного раскрытия, модификации, уничтожения или обхода.

ASD_SAD.1.6C В описании архитектуры должны излагаться механизмы самозащиты мер обеспечения безопасности.

ASD_SAD.1.7C Описание архитектуры должно быть внутренне согласованным.

С.5.2.3.3 Элементы действий оценщика

ASD_SAD.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.5.3 Функциональная спецификация интерфейсов (ASD_IFS)

С.5.3.1 Цели

Назначением функциональной спецификации интерфейсов автоматизированной системы является обеспечение описания функций безопасности автоматизированной системы, доступных на видимых интерфейсах, и их характеристики безопасности.

С.5.3.2 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.3.3 ASD_IFS.1 Функциональная спецификация интерфейсов

Зависимости: ASD_SAD.1 Описание архитектуры.

С.5.3.3.1 Элементы действий разработчика/интегратора

ASD_IFS.1.1D Разработчик/интегратор должен обеспечить функциональную спецификацию интерфейсов.

С.5.3.3.2 Элементы содержания и представления свидетельств

ASD_IFS.1.1C В функциональной спецификации интерфейсов должны идентифицироваться и излагаться все видимые интерфейсы автоматизированной системы, включая функции безопасности, доступные через эти интерфейсы, и характеристики безопасности этих интерфейсов.

ASD_IFS.1.2C Функциональная спецификация интерфейсов должна быть внутренне согласованной.

С.5.3.3.3 Элементы действий оценщика

ASD_IFS.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_IFS.1.2E Оценщик должен подтвердить соответствие функциональной спецификации интерфейсов описанию архитектуры.

С.5.4 Проект подсистем (ASD_SSD)

С.5.4.1 Цели

Целью свидетельства проектирования подсистем является обеспечение описания:

a) подсистем;

в) распределения функций безопасности по подсистемам;

c) характеристик безопасности каждой подсистемы;

d) интерфейсов каждой подсистемы и функций, выполняемых через каждый интерфейс;

e) компонентов, из которых состоит каждая подсистема.

С.5.4.2 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.4.3 ASD_SSD.1 Проектирование подсистем

Зависимости:

ASD_SAD.1 Описание архитектуры;

ASD_IFS.1 Функциональная спецификация интерфейсов.

С.5.4.3.1 Элементы действий разработчика/интегратора

ASD_SSD.1.1D Разработчик/интегратор должен обеспечить проектирование подсистемы.

ASD_SSD.1.2D Разработчик/интегратор должен обеспечить отображение проектирования подсистемы в проектирование архитектуры.

С.5.4.3.2 Элементы содержания и представления свидетельств

ASD_SSD.1.1C В проектировании подсистем должны излагаться функциональные возможности безопасности, обеспечиваемые каждой подсистемой.

ASD_SSD.1.2C В проектировании подсистем должны быть определены все аппаратные средства, программно-аппаратные средства и программное обеспечение, требуемые для выполнения функций безопасности, распределенных подсистеме.

ASD_SSD.1.3 C В проектировании подсистем должны быть определены интерфейсы к каждой подсистеме.

ASD_SSD.1.4C В проектировании подсистем должны быть определены характеристики безопасности для каждой подсистемы.

ASD_SSD.1.5C В проектировании подсистем должны быть определены интерфейсы к каждой подсистеме, исходя из их назначения и метода использования воздействий, исключений и сообщений об ошибках.

ASD_SSD.1.6C В проектировании подсистем должны быть определены компоненты, из которых состоит каждая подсистема.

ASD_SSD.1.7C Проектирование подсистемы должен быть внутренне согласовано.

ASD_SSD.1.8C Проектирование подсистем должно быть полной иллюстрацией функциональных возможностей безопасности, включая специфические для доменов функции.

ASD_SSD.1.9C Отражение проектирования подсистемы на проектирование архитектуры должно демонстрировать наличие всех элементов проектирования архитектуры в проектировании подсистемы.

С.5.4.3.3 Элементы действий оценщика

ASD_SSD.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_SSD.1.2E Оценщик должен подтвердить совместимость проектирования подсистемы с описанием архитектуры и функциональной спецификацией интерфейсов.

С.5.5 Проектирование компонентов (ASD_CMP)

С.5.5.1 Цели

Целью свидетельства проектирования компонента является обеспечение описания:

a) назначения и функций каждого компонента автоматизированной системы;

в) распределения функциональных возможностей безопасности каждому компоненту;

c) характеристик безопасности каждой подсистемы;

d) интерфейсов подсистемы, обеспечиваемых каждым компонентом;

e) функциональных возможностей, обеспечиваемых посредством идентифицированных интерфейсов для компонента;

f) способа обеспечения функциональных возможностей безопасности и характеристик безопасности каждого компонента.

С.5.5.2 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.5.3 ASD_CMP.1 Проектирование компонентов

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проектирование подсистем.

С.5.5.3.1 Элементы действий разработчика/интегратора

ASD_CMP.1.1D Разработчик/интегратор должен обеспечить проектирование компонента.

ASD_CMP.1.2D Разработчик/интегратор должен обеспечить отображение проектирования компонентов в проектирование подсистемы.

ASD_CMP.1.3D Разработчик/интегратор должен обеспечить анализ согласованности краткой спецификации СОО.

С.5.5.3.2 Элементы содержания и представления свидетельств

ASD_CMP.1.1C В проектировании компонента должны излагаться назначение и функции компонентов каждой подсистемы.

ASD_CMP.1.2C В проектировании компонента должны быть определены взаимосвязи между компонентами в каждой подсистеме.

ASD_CMP.1.3C В проектировании компонента должны идентифицироваться интерфейсы для подсистемы автоматизированной системы, которым соответствует каждый компонент.

ASD_CMP.1.4C В проектировании компонента должны описываться интерфейсы для подсистемы автоматизированной системы, которым соответствует каждый компонент, исходя из их назначения и метода использования.

ASD_CMP.1.5C В проектировании компонента должны излагаться функциональные возможности безопасности, обеспечиваемые каждым компонентом.

ASD_CMP.1 6C В проектировании компонента должны идентифицироваться характеристики безопасности каждого компонента.

ASD_CMP.1.7C В проектировании компонента должно излагаться то, как обеспечиваются функциональные возможности безопасности и характеристики безопасности каждого компонента.

ASD_CMP.1.8C Проектирование компонентов каждой подсистемы должно быть внутренне согласованным.

ASD_CMP.1.9C Проектирование компонентов каждой подсистемы должно обеспечить полную иллюстрацию функциональных возможностей безопасности, назначенных этой подсистеме, включая специфические для доменов функции.

ASD_CMP.1.10C Отражение проектирования компонентов на проектирование подсистемы должно демонстрировать наличие всех элементов проектирования подсистемы в проектировании компонентов.

ASD_CMP.1.11C Анализ согласованности краткой спецификации СОО должен продемонстрировать согласованность проектирования компонентов с описанием внедрения ФБС и ДБС в краткую спецификацию СОО и все краткие спецификации доменов СОО.

С.5.5.3.3 Элементы действий оценщика

ASD_CMP.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_CMP.1.2E Оценщик должен определить согласованность проектирования компонентов с проектированием подсистемы и функциональной спецификацией интерфейса.

С.5.6 Представление реализации (ASD_IMP)

С.5.6.1 Цели

Целью описания реализации является оказание поддержки при оценке критически важных функций автоматизированной системы, созданных исключительно для интегрирования компонентов в эту систему. Критически важные функции автоматизированной системы не являются функциями, присущими компоненту как уже заданные или оцененные. Однако может возникнуть необходимость пересмотра некоторых оцененных частей компонента в контексте оценки автоматизированной системы вследствие специфических проблем, связанных с конфигурацией или интеграцией, обнаруженных перед оценкой автоматизированной системы или во время ее.

С.5.6.2 Замечания по применению

Описание реализации (например, исходный текст) не предполагается применять для всех компонентов автоматизированной системы, а только для тех, которые конфигурируют другие части системы или реализуют критически важные функции безопасности, поддерживающие другие компоненты. Заданием для этого семейства могут быть программы интеграции или выходные вспомогательные программы, созданные исключительно для автоматизированной системы.

С.5.6.3 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.6.4 ASD_IMP.1 Описание реализации

Зависимости: ASD_CMP.1 Проектирование компонентов.

С.5.6.4.1 Элементы действий разработчика/интегратора

ASD_IMP.1D Разработчик/интегратор должен обеспечить описание реализации проектирования компонентов.

С.5.6.4.2 Элементы содержания и представления свидетельств

ASD_IMP.1.1C В описании реализации должна быть приведена полная реализация проектирования компонентов, включая все выполняемые функции безопасности и характеристики безопасности, назначенные этому компоненту.

ASD_IMP.1.2C В описании реализации должны быть определены выполняемые функции безопасности, обеспечиваемые каждым компонентом, исходя из его конкретных требований к конфигурации.

ASD_IMP.1.3C Описание реализации должно быть внутренне согласованным.

С.5.6.4.3 Элементы действий оценщика

ASD_IMP.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.5.7 Концепция безопасности функционирования (ASD_CON)

С.5.7.1 Цели

Назначением концепции безопасности функционирования является описание политик, свойств и характеристик безопасности автоматизированной системы в том виде, в каком они представляются и выполняются в поддержку деловой оперативной деятельности или выполняемой целевой задачи, что позволяет провести анализ свидетельства архитектурного проектирования для подтверждения осуществления СОО необходимых политик и свойств.

С.5.7.2 Замечания по применению

Обычно для обеспечения эффективности технических и организационных мер безопасности, реализующих ФБС, применяются различные методы. В случае с техническими средствами безопасности часто реализуют необходимые широкомасштабные механизмы на уровне аппаратных средств (например, механизмы управления памятью). В случае организационных мер безопасности часто применяются процедурные механизмы в масштабе организации (например, разделение обязанностей).

С.5.7.3 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.7.4 ASD_CON.1 Концепция безопасности операций

Зависимости: ASD_SAD.1 Описание архитектуры.

С.5.7.4.1 Элементы действий разработчика/интегратора

ASD_CON.1.1D Разработчик/интегратор должен обеспечить документацию концепции безопасности операций, охватывающую все ФБС.

С.5.7.4.2 Элементы содержания и представления свидетельств

ASD_CON.1.1C Концепция безопасности операций должна обладать степенью детализации, сопоставимой со степенью детализации описания интерфейсов, свойств и механизмов безопасности, предусмотренных в архитектурном проектировании.

ASD_CON.1.2C В документацию концепции безопасности операций должны быть включены все режимы работы автоматизированной системы (например, режим архивации или ухудшенный режим работы).

ASD_CON.1.3C Документация концепции безопасности операций должна быть внутренне согласованной.

ASD_CON.1.4C В документации концепции безопасности операций должно быть описано поддержание доменов безопасности автоматизированной системы способом, согласующимся с требованиями безопасности системы.

ASD_CON.1.5C Документация концепции безопасности операций должна демонстрировать предотвращение процессом инициализации ФБС обхода, создания помех или умышленного нанесения ущерба при установлении функций выполнения требований безопасности системы.

ASD_CON.1.6C Документация концепции безопасности операций должна демонстрировать самозащиту ФБС от помех и фальсифицирования.

ASD_CON.1.7C Документация концепции безопасности операций должна демонстрировать предотвращение обхода функций выполнения требований безопасности системы.

ASD_CON.1.8C Документация концепции безопасности операций должна демонстрировать то, что потоки информации между доменами безопасности автоматизированной системы и между данной автоматизирован-

ной системой и внешними автоматизированными системами не обходят, не создают помехи или не наносят ущерб функций выполнения требований безопасности системы.

С.5.7.4.3 Элементы действий оценщика

ASD_CON.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_CON.1.2E Оценщик должен определить, является ли архитектурное проектирование полной и правильной реализацией концепции безопасности функционирования автоматизированной системы в поддержку выполняемой целевой задачи.

С.5.8 Верификация проектной документации (ASD_GVR)

С.5.8.1 Цели

Целью является демонстрация правильности проектной документации по безопасности после внесения изменений в компоненты системы или их модификации.

С.5.8.2 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.5.8.3 ASD_GVR.1 Проверка проектной документации

Зависимости:

ASD_SAD.1 Описание архитектуры;

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проектирование подсистем;

ASD_CMP.1 Проектирование компонентов;

ASD_CON.1 Концепция безопасности компонентов.

С.5.8.3.1 Цели

Назначением данного компонента является демонстрация того, что документация по безопасности остается правильной после внесения изменений в компоненты системы или их модификации.

С.5.8.3.2 Замечания по применению

Данный компонент взаимодействует не только с измененными или модифицированными частями автоматизированной системы, но также с другими частями, которые могли стать недействительными.

С.5.8.3.3 Элементы действий разработчика/интегратора

ASD_GVR.1.1D После внесения изменений или модификаций в компоненты системы, ее конфигурацию или среду эксплуатации разработчик/интегратор должен провести верификационный анализ для проверки того, осталась ли проектная документация автоматизированной системы правильной и согласованной.

С.5.8.3.4 Элементы содержания и представления свидетельств

ASD_GVR.1.1C По каждому проектному документу верификационный анализ должен показать, не подвергался ли документ воздействию изменений или модификаций или был ли должным образом обновлен для отражения изменений или модификаций.

С.5.8.3.5 Элементы действий оценщика

ASD_GVR.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6 Класс AOC: управление конфигурацией автоматизированных систем

С.6.1 Введение

Целью управления конфигурацией во время оценки является обеспечение доверия к тому, что у оценщика имеется правильная версия всех компонентов автоматизированной системы для других действий по оценке. Следовательно, это управление применимо к мерам в пределах среды разработки и интеграции, но не среды эксплуатации, где она имеет отличия. После разворачивания и интегрирования автоматизированной системы оцененная система управления конфигурацией остается в среде разработки и интеграции.

Управление конфигурацией может осуществлять контроль за оцененными и неоцененными продуктами в автоматизированных системах.

Данный класс обеспечивает не связанные с ИТ меры, позволяющие персоналу управлять аспектами безопасности автоматизированной системы и связанной с ней конфигурацией(ями) в ходе эксплуатации и контролировать изменения в автоматизированной системе, связанные с мерами обеспечения ее безопасности. Управление конфигурацией безопасности определяет и описывает компоненты автоматизированной системы, как определено ее конфигурацией разработки, любые специализированные функции межоперабельности, как определено конфигурацией интеграции, а также установки параметров для конфигурации рабочего цикла компонентов, как определено эксплуатационной конфигурацией. Управление конфигурацией безопасности также предусматривает наличие политик и процедур контроля за изменениями и их эффективную реализацию для контроля за изменениями в автоматизированной системе, включая ограничения доступа к контролю за изменениями.

Семейства данного класса определяют процессы и процедуры, позволяющие персоналу, ответственному за безопасность, определять, из чего состоит конфигурация автоматизированной системы, что позволяет осуществлять прослеживание процессов и обслуживание автоматизированной системы и каждого из критически важных компонентов, составляющих систему в различных конфигурациях. Определения конфигурации включают в себя процессы разработки, интеграции, организации и учет непредвиденных ситуаций. Семейства обязательно определяют меры, не связанные с ИТ, задействованные в обеспечении безопасности автоматизированной

системы, и обеспечивают необходимый контроль за конфигурацией и след аудита, связанный с изменениями в действиях по обеспечению безопасности автоматизированной системы.

С.6.2 (AOC_OBM) Базовая конфигурация автоматизированной системы

С.6.2.1 Цели

Данное семейство определяет оцененную конфигурацию автоматизированной системы и ее компоненты безопасности, а также меры, посредством которых планы и процедуры управления конфигурацией безопасности отслеживают базовую конфигурацию и контролируют изменения в этой базе. Данное семейство по существу отслеживает оцененную базу, управляет ею и осуществляет контроль за ней. Данное семейство определяет и отслеживает как технические, так и организационные меры безопасности, выполняющие функции безопасности автоматизированной системы, и их взаимосвязи. База автоматизированной системы обновляется при каждой повторной оценке для получения самой последней оцененной базы, на которую будут ссылаться при всех последующих модификациях, анализе воздействия или повторных оценках.

С.6.2.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются на основе подтверждения описания документации и проверок в автоматизированной системе.

С.6.2.3 AOC_OBM.1 Базовая конфигурация автоматизированной системы

Зависимости: зависимости отсутствуют.

С.6.2.3.1 Элементы действий разработчика/интегратора

AOC_OBM.1.1D Для исходной/самой последней оцененной системы разработчик/интегратор должен использовать систему управления конфигурацией (УК), которая называется «База».

AOC_OBM.1.2D Система УК должна отслеживать и контролировать каждое изменение, предлагаемое для Базы и внесенное в нее, и состояние ее оценки.

AOC_OBM.1.3D Система УК должна сообщать о текущей конфигурации Базы автоматизированной системы.

AOC_OBM.1.4D Разработчик/интегратор/владелец системы должен предоставлять документацию по УК Базы системы.

С.6.2.3.2 Элементы содержания и представления свидетельств

AOC_OBM.1.1C Система УК должна однозначно определять Базу СОО, каждое связанное с ней изменение и состояние ее оценки.

AOC_OBM.1.2C В плане УК должно излагаться то, как поддерживается База системы и как отслеживаются и управляются изменения в Базе.

С.6.2.3.3 Элементы действий оценщика

ASD_OBM.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6.2.4 ASD_OBM.2 Проверка базовой конфигурации автоматизированной системы

Является иерархической для: AOC_OBM.1 Базовая конфигурация автоматизированной системы.

Зависимости: зависимости отсутствуют.

С.6.2.4.1 Элементы действий разработчика/интегратора

AOC_OBM.2.1D Для исходной/самой последней оцененной системы разработчик/интегратор должен использовать систему УК, которая называется «База».

AOC_OBM.2.2D Система УК должна отслеживать и контролировать каждое изменение, предлагаемое для Базы и внесенное в нее, и состояние ее оценки.

AOC_OBM.2.3D Система УК должна сообщать о текущей конфигурации Базы автоматизированной системы.

AOC_OBM.2.4D Разработчик/интегратор/владелец системы должен предоставлять документацию по УК Базы системы.

С.6.2.4.2 Элементы содержания и представления свидетельств

AOC_OBM.2.1C Система УК должна однозначно определять Базу СОО, каждое связанное с ней изменение и состояние ее оценки.

AOC_OBM.2.2C В плане УК должно излагаться то, как поддерживается База системы и как отслеживаются и управляются изменения в Базе.

С.6.2.4.3 Элементы действий оценщика

ASD_OBM.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_OBM.2.1E Оценщик должен независимо проверять посредством опросов персонала, выборки изменений, других методов достоверности системы УК.

С.6.3 Оцененные продукты компонентов (AOC_ECP)

С.6.3.1 Цели

Данное семейство определяет пакет доверия и требования к эксплуатационным параметрам компонентов автоматизированной системы, которые составлены из оцененных продуктов. При создании автоматизированной системы из компонентов, составленных из продуктов, возникает необходимость установления требуемого доверия из аспектов работ по разработке и интеграции. При использовании готовых продуктов деятельность по разработке специально для автоматизированной системы не проводится. Следовательно, доверие должно быть получено из оценки продукта и сертификации, такой как наличие официального сертификата, подтверждающего сертификацию продукта, например, в EAL4, как определено в стандартах серии ИСО/МЭК 15408.

С.6.3.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются на основе подтверждения описания документации и проверок в автоматизированной системе.

С.6.3.3 AOC_ECP.1 Оцененные продукты компонентов

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы

С.6.3.3.1 Элементы действий разработчика/интегратора

AOC_ECP.1.1D Разработчик/интегратор должен определять оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_ECP.1.2D Разработчик/интегратор должен устанавливать эксплуатационные параметры для каждого продукта компонентов.

С.6.3.3.2 Элементы содержания и представления свидетельств

AOC_ECP.1.1C В плане УК должны описываться оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_ECP.1.2C Должны быть определены отчет о результатах оценки или уведомление о независимой сертификации и ЗБ для оцененных продуктов.

AOC_ECP.1.3C В плане УК должны быть указаны эксплуатационные параметры для каждого продукта компонента.

С.6.3.3.3 Элементы действий оценщика

ASD_ECP.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6.3.4 AOC_ECP.2 Проверка оцененных продуктов компонентов

Является иерархическим для: AOC_ECP.1 Оцененные продукты компонентов.

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы.

С.6.3.4.1 Элементы действий разработчика/интегратора

ASD_ECP.2.1D Разработчик/интегратор должен определять оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_ECP.2.2D Разработчик/интегратор должен устанавливать эксплуатационные параметры для каждого продукта компонентов.

С.6.3.4.2 Элементы содержания и представления свидетельств

AOC_ECP.2.1C В плане УК должны быть указаны оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_ECP.2.2C. Должны быть определены отчет о результатах оценки или уведомление о независимой сертификации и ЗБ для оцененных продуктов.

AOC_ECP.2.3C В плане УК должны быть указаны эксплуатационные параметры для каждого продукта компонента.

С.6.3.4.3 Элементы действий оценщика

ASD_ECP.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_ECP.2.2E Оценщик должен подтвердить соответствие условий эксплуатации, изложенных в отчете о результатах оценки или отчете о независимой сертификации, требованиям среды эксплуатации автоматизированной системы.

С.6.4 Соответствие ПЗ (AOC_PPC)

С.6.4.1 Цели

Данное семейство определяет требования доверия к согласованию с конкретным ПЗ. Предъявляемым свидетельством является уведомление о сертификации, включая приемлемое ЗБ. В среде эксплуатации продукты компонентов могут иметь специфические параметры. Такие параметры должны быть четко определены.

С.6.4.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются на основе подтверждения описания документации и проверок автоматизированной системы.

С.6.4.3 AOC_PPC.1 Согласование с ПЗ

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы.

С.6.4.3.1 Элементы действий разработчика/интегратора

AOC_PPC.1.1D Разработчик/интегратор должен обозначить ПЗ для продуктов компонентов, с которыми они должны быть согласованы.

AOC_PPC.1.2D Разработчик/интегратор должен устанавливать эксплуатационные параметры для каждого продукта компонента.

ASD_ECP.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6.4.3.2 Элементы содержания и представления свидетельств

AOC_PPC.1.1C В плане УК должны быть определены ПЗ для продуктов компонентов, с которыми они должны быть согласованы.

AOC_PPC.1.2C Должны быть определены отчет о результатах оценки или уведомление о независимой сертификации и ЗБ для оцененных продуктов.

AOC_PPC.1.3C В плане УК должны быть определены эксплуатационные параметры для каждого продукта компонентов.

С.6.4.3.3 Элементы действий оценщика

ASD_PPC.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6.4.4 AOC_PPC Согласование с проверкой ПЗ

Является иерархическим для: AOC_PPC.1. согласование с ПЗ.

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы.

С.6.4.4.1 Элементы действий разработчика/интегратора

AOC_PPC.2.1D Разработчик/интегратор должен обозначить ПЗ для продуктов компонентов, с которыми они должны быть согласованы.

AOC_PPC.2.2D Разработчик/интегратор должен устанавливать эксплуатационные параметры для каждого продукта компонента.

С.6.4.4.2 Элементы содержания и представления свидетельств

AOC_PPC.2.1C В плане УК должны быть определены ПЗ для продуктов компонентов, с которыми они должны быть согласованы.

AOC_PPC.2.2C Должны быть определены отчет о результатах оценки или уведомление о независимой сертификации и ЗБ для оцененных продуктов.

AOC_PPC.2.3C В плане УК должны быть определены эксплуатационные параметры для каждого продукта компонентов.

С.6.4.4.3 Элементы действий оценщика

ASD_PPC.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASD_PPC.2.2E Оценщик должен подтвердить соответствие условий эксплуатации, изложенных в отчете о результатах оценки или отчете о независимой сертификации, требованиям среды эксплуатации автоматизированной системы.

С.6.5 Неоцененные продукты компонентов (AOC_NCP)

С.6.5.1 Цели

Семейство описывает пакет доверия и требования к оперативным параметрам компонентов автоматизированной системы, составленных из неоцененных продуктов. При создании автоматизированной системы из компонентов существует необходимость определения требуемого доверия из аспектов действий по разработке и интеграции. Для таких продуктов, как программы для коммерческого применения, разработанных специально для автоматизированной системы, в ходе разработки разработчик продукта может создавать свидетельство доверия, аналогичное свидетельству, требуемому для оценки продукта.

В среде эксплуатации компоненты, состоящие из продуктов, могут иметь специфические параметры. Подобные параметры должны быть четко определены.

С.6.5.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Компоненты семейства распределяются на основе подтверждения описания документации и проверки автоматизированной системы.

С.6.5.3 AOC_NCP.1 Неоцененные продукты компонентов

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы.

С.6.5.3.1 Элементы действий разработчика/интегратора

AOC_NCP.1.1D Разработчик/интегратор/владелец системы должен определять необходимые пакеты доверия для продуктов компонентов или доменов безопасности, содержащих подобные продукты.

AOC_NCP.1.2D Разработчик/интегратор/оператор системы должен устанавливать эксплуатационные параметры для каждого продукта компонента.

С.6.5.3.2 Элементы содержания и представления свидетельств

AOC_NCP.1.1C В плане УК должны описываться оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_NCP.1.2C В плане УК должны быть определены эксплуатационные параметры для каждого продукта компонентов.

С.6.5.3.3 Элементы действий оценщика

AOC_NCP.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.6.5.4 AOC_NCP.2 Проверка неоцененных продуктов компонентов

Является иерархическим для: AOC_NCP.1 Неоцененные продукты компонентов.

Зависимости: AOC_OBM.1 Конфигурация базы автоматизированной системы.

С.6.5.4.1 Элементы действий разработчика/интегратора

AOC_NCP.2.1D Разработчик/интегратор/владелец системы должен определять необходимые пакеты доверия для продуктов компонентов или доменов безопасности, содержащих подобные продукты.

AOC_NCP.2.2D Разработчик/интегратор/оператор системы должен устанавливать эксплуатационные параметры для каждого продукта компонента.

С.6.5.4.2 Элементы содержания и представления свидетельств

AOC_NCP.2.1C В плане УК должны описываться оцененные пакеты доверия для продуктов компонентов или доменов безопасности, содержащих такие продукты.

AOC_NCP.2.2C В плане УК должны быть определены эксплуатационные параметры для каждого продукта компонентов.

С.6.5.4.3 Элементы действий оценщика

AOC_NCP.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOC_NCP.2.2E Оценщик должен провести оценку и подтвердить, что продукты соответствуют требуемым пакетам доверия в среде эксплуатации автоматизированной системы.

С.7 Класс AOT: тестирование автоматизированных систем

С.7.1 Введение

Назначением данного класса является проверка соответствия компонентов автоматизированной системы, установленных, интегрированных и конфигурированных в соответствии с архитектурой и свидетельством конфигурации автоматизированной системы, функциональным требованиям безопасности, определенным в ЗБС, и эффективности выполнения концепции безопасности функционирования автоматизированной системы. Архитектура, интеграция и проектная документация автоматизированной системы содействуют в планировании и проведении испытаний. Это содействие определяется тем, что ФБС были сконфигурированы в соответствии со спецификацией конфигурации, испытаны в отношении к соответствующей архитектуре и свидетельству проекта при помощи выборки испытаний разработчика/интегратора и независимого испытания подгруппы (подмножества) ФБС.

С.7.2 Функциональное тестирование автоматизированной системы (AOT_FUN)

С.7.2.1 Цели

Назначением данного компонента является демонстрация разработчиком должного выполнения всех функций безопасности. Разработчик требуется также для проведения тестирования и обеспечения тестовой документации.

При функциональном тестировании, проводимом разработчиком и/или интегратором, устанавливается наличие у ФБС свойств, необходимых для удовлетворения функциональных требований ее ПЗ/ЗБ. Подобное функциональное тестирование обеспечивает доверие к тому, что ФБС соответствует, по крайней мере, функциональным требованиям безопасности, хотя ФБС не может установить, что ФБС не делает более того, что было установлено для нее. Семейство «Функциональные тесты» сфокусировано на типе или объеме документации или на необходимых инструментальных средствах поддержки, а также на том, что должно быть выявлено посредством тестирования разработчика. Функциональное тестирование не ограничивается положительным заключением о предоставлении требуемых функций безопасности, а может также включать в себя негативное тестирование для проверки отсутствия определенного нежелательного поведения (часто основанное на инверсии функциональных требований).

Семейство способствует обеспечению доверия к тому, что вероятность необнаруженных дефектов относительно мала.

Семейства AOT_COV, AOT_DPT и AOT_FUN используются в комбинации для определения свидетельства тестирования, представляемого разработчиком и/или интегратором. Независимое функциональное тестирование, проводимое оценщиком, определяется семейством AOT_IND.

С.7.2.2 Ранжирование компонентов

Данное семейство состоит из одного компонента.

С.7.2.3 Замечания по применению

Предполагается, что в процедурах проведения тестов предусмотрены инструкции тестовых программ и тестовых комплексов, включая тестовую среду, условия тестов, параметры и значения тестовых данных. Тестовые процедуры должны также демонстрировать получение результатов тестирования из входных данных тестов.

Данное семейство устанавливает требования к представлению всех планов, процедур и результатов тестов. Количество информации, предназначенной для проведения тестирования, изменяется в соответствии с использованием семейств AOT_COV и AOT_DPT.

Зависимости упорядочения являются значимыми, когда успешное выполнение определенного теста зависит от наличия определенного состояния другого теста. Например, может потребоваться выполнение теста А непосредственно перед тестом В, поскольку состояние успешного выполнения теста А является предпосылкой успешного выполнения теста В, следовательно, сбой во время теста В может быть связан с проблемой, касающейся зависимостей упорядочения. В вышеприведенном примере отказ теста В мог быть результатом выполнения теста С (а не теста А) непосредственно перед ним, или сбой в тесте В мог быть связан со сбоем в тесте А.

С.7.2.4 AOT_FUN Функциональное тестирование

Зависимости: зависимости отсутствуют.

С.7.2.4.1 Элементы действий разработчика/интегратора

AOT_FUN.1.1D Разработчик/интегратор должен тестировать ФБС и документировать результаты.

AOT_FUN.1.2D Разработчик/интегратор должен обеспечивать тестовую документацию.

AOT_FUN.1.3D Разработчик/интегратор должен обеспечивать анализ уровня детализации и комплексного тестирования мер обеспечения безопасности.

С.7.2.4.2 Элементы содержания и представления свидетельств

AOT_FUN.1.1C Тестовая документация должна состоять из планов тестов, описания тестовых процедур, предполагаемых и фактических результатов тестов.

AOT_FUN.1.2C Анализ проверки мер обеспечения безопасности должен демонстрировать абсолютное соответствие между мерами обеспечения безопасности, определенными в ЗБ, и тестами, изложенными в тестовой документации.

AOT_FUN.1.3C В планах тестов должны быть определены функции безопасности, предназначенные для тестирования, и изложена цель тестов, предназначенных для выполнения.

AOT_FUN.1.4C В описаниях тестовых процедур должны быть определены тесты, предназначенные для выполнения, и изложены сценарии тестирования каждой функции безопасности. Эти сценарии должны включать в себя все зависимости упорядочения по результатам других тестов.

AOT_FUN.1.5C В предполагаемых результатах тестов должны быть отражены ожидаемые выходные данные после успешного выполнения тестов.

AOT_FUN.1.6C Результаты тестов, выполненных разработчиком/интегратором, должны демонстрировать заданное поведение каждой тестируемой функции безопасности.

AOT_FUN.1.7C Тестовая документация должна включать в себя анализ зависимостей упорядочения тестовых процедур.

С.7.2.4.3 Элементы действий оценщика

AOC_FUN 1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.3 Покрытие тестами автоматизированной системы (AOT_COV)

С.7.3.1 Цели

Данное семейство рассматривает аспекты тестирования, связанные с полнотой покрытия тестами. То есть, оно рассматривает степень тестирования ФБС и достаточность этой степени для демонстрации работы ФБС заданным образом.

С.7.3.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе возрастающей строгости испытания интерфейсов и возрастающей строгости анализа достаточности тестов для демонстрации действия ФБС в соответствии с функциональной спецификацией ее интерфейса.

С.7.3.3 AOT_COV.1 Свидетельство покрытия тестами

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейса;

AOT_FUN.1 Функциональное тестирование.

С.7.3.3.1 Цели

Назначением данного компонента является установление факта, что ФБС была тестирована по отношению к функциональной спецификации интерфейса систематическим образом. Это достигается посредством изучения анализа соответствия, проведенного разработчиком и/или интегратором.

С.7.3.3.2 Замечания по применению

В то время как целью тестирования является покрытие ФБС, требование по предоставлению чего-либо для проверки этого утверждения, кроме неформального отображения тестов в функциональной спецификации интерфейса и самих испытательных данных, отсутствует.

Для данного компонента требуется разработчик/интегратор для демонстрации того, что идентифицированные тесты включают в себя тестирование всех видимых функций безопасности, как описано в функциональной спецификации интерфейса. Анализ должен не только показывать соответствие между тестами и функциями безопасности, но также обеспечивать оценщика информацией, достаточной для определения способа выполнения функций. Данная информация может применяться в планировании дополнительных тестов оценщика. Хотя на этом уровне разработчику/интегратору приходится демонстрировать, что каждая из функций в функциональной спецификации интерфейса была тестирована, объем тестирования не обязательно должен быть исчерпывающим.

С.7.3.3.3 Элементы действий разработчика/интегратора

AOT_COV.1.1D Разработчик/интегратор должен обеспечивать анализ покрытия тестами.

С.7.3.3.4 Элементы содержания и представления свидетельств

AOT_COV.1.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и ФБС, доступными посредством видимых интерфейсов автоматизированной системы, описанных в функциональной спецификации интерфейсов.

AOT_COV.1.2C Анализ покрытия тестами должен демонстрировать полноту соответствия между ФБС, доступными посредством видимых интерфейсов автоматизированной системы, описанных в функциональной спецификации интерфейсов, и тестами, идентифицированными в тестовой документации.

С.7.3.3.5 Элементы действий оценщика

AOC_COV1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.3.4 AOC_COV.2 Строгий анализ покрытия тестами

Является иерархическим для: AOC_COV.1 Свидетельство покрытия тестами.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

AOT_FUN.1 Функциональное тестирование.

С.7.3.4.1 Цели

Назначением данного компонента является установление факта, что ФБС была тестирована по отношению к функциональной спецификации интерфейса систематическим и исчерпывающим образом. Установление вышеупомянутого факта достигается посредством изучения анализа соответствия, проведенного разработчиком и/или интегратором.

С.7.3.4.2 Замечания по применению

Разработчик/интегратор требуется для предоставления убедительного аргумента — идентифицированные тесты охватывают все видимые функции безопасности, и тестирование каждой функции является полным. Для оценщика остается малое поле деятельности для разработки дополнительных функциональных тестов интерфейсов ФБС, основанных на функциональной спецификации интерфейса, иначе они были бы тестированы исчерпывающим образом. Тем не менее оценщик должен стремиться к созданию таких тестов.

С.7.3.4.3 Элементы действий разработчика/интегратора

AOC_COV.2.1D Разработчик/интегратор должен обеспечивать анализ покрытия тестами.

С.7.3.4.4 Элементы содержания и представления свидетельств

AOT_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами, идентифицированными в тестовой документации, и ФБС, доступными посредством видимых интерфейсов автоматизированной системы, описанных в функциональной спецификации интерфейсов.

AOT_COV.2.2C Анализ покрытия тестами должен демонстрировать полноту соответствия между ФБС, доступными посредством видимых интерфейсов автоматизированной системы, описанных в функциональной спецификации интерфейсов, и тестами, идентифицированными в тестовой документации.

AOT_COV.2.3C Анализ покрытия тестами должен строго демонстрировать, что все видимые интерфейсы для ФБС, указанные в функциональной спецификации интерфейсов, были полностью тестированы.

С.7.3.4.5 Элементы действий оценщика

AOC_COV2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.4 Глубина тестирования автоматизированной системы (AOT_DPT)

С.7.4.1 Цели

Назначением компонентов данного семейства является установление степени детализации тестирования ФБС. Тестирование функций безопасности основано на растущей глубине информации, полученной из анализа представлений.

Целью тестирования является противодействие риску пропуска ошибки при разработке и интеграции СОО. Кроме того, вероятность обнаружения вредоносного кода компонентами этого семейства больше, особенно если тестирование связано с внутренней структурой ФБС.

Тестирование специфических внутренних интерфейсов может обеспечить доверие не только к тому, что ФБС демонстрирует нужное внешнее поведение в области безопасности, но также к тому, что это поведение основано на правильно функционирующих внутренних механизмах.

С.7.4.2 Ранжирование компонентов

Данное семейство состоит из трех компонентов. Компоненты распределяются на основе повышения детализации, установленной в представлениях ФБС, от проекта архитектуры до представления реализации. Это распределение отражает представления ФБС, установленные в классе ASD.

С.7.4.3 Замечания по применению

Конкретный объем, тип документации и свидетельство в общем определяются выбранным компонентом из AOT_FUN.

Тестирование на уровне функциональной спецификации интерфейсов осуществляется с помощью AOT_COV.

Принцип, принятый в данном семействе, заключается в том, чтобы уровень тестирования соответствовал уровню искомого доверия. При применении компонентов более высокого уровня результаты тестов должны демонстрировать соответствие реализации ФБС ее проекту. Например, в проекте подсистем должны быть изложены каждая из подсистем, а также интерфейсы между этими подсистемами достаточно подробно для четкого определения назначения, действий и возможных погрешностей каждого интерфейса. Свидетельство тестирования на уровне проекта подсистемы должно показывать, что были выполнены внутренние интерфейсы между подсистемами. Выполнение внутренних интерфейсов между подсистемами можно осуществить посредством тестирования через внешние интерфейсы ФБС или тестирования интерфейсов подсистем в изоляции, иногда с применением средств испытания. Целью компонентов более высокого уровня является проверка правильности функционирования внутренних интерфейсов, которые становятся видимыми по мере того, как проект становится

менее абстрактным. При применении этих компонентов предоставление адекватного свидетельства глубины тестирования с помощью только внешних интерфейсов ФБС становится более затруднительным.

С.7.4.4 AOT_DPT.1 Тестирование: функциональная спецификация интерфейсов

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

AOT_FUN.1 Функциональное тестирование.

С.7.4.4.1 Цели

В функциональной спецификации интерфейсов определяются и излагаются все ФБС, доступные через внешне видимые интерфейсы. Тестирование на уровне видимых интерфейсов обеспечивает доверие к тому, что непосредственно доступные ФБС были реализованы правильно.

С.7.4.4.2 Элементы действий разработчика/интегратора

AOT_DPT.1.1D Разработчик/интегратор должен обеспечивать анализ глубины тестирования.

С.7.4.4.3 Элементы содержания и представления свидетельств

AOT_DPT.1.1C Анализ глубины тестирования должен демонстрировать, что тестов, указанных в тестовой документации, достаточно для демонстрации функционирования ФБС в соответствии с ее функциональной спецификацией интерфейсов.

С.7.4.4.4 Элементы действий оценщика

AOT_DPT.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.4.5 AOT_DPT.2 Тестирование: проект подсистем

Является иерархическим для: AOT_DPT.1 Тестирование: функциональная спецификация интерфейсов.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

AOT_FUN.1 Функциональное тестирование.

С.7.4.5.1 Цели

Проект подсистем обеспечивает высокоуровневое описание внутренних действий ФБС. Тестирование на уровне подсистем обеспечивает доверие к правильности реализации подсистем ФБС.

С.7.4.5.2 Элементы действий разработчика/интегратора

AOT_DPT.2.1D Разработчик/интегратор должен обеспечивать анализ глубины тестирования.

С.7.4.5.3 Элементы содержания и представления свидетельств

AOT_DPT.2.1C Анализ глубины тестирования должен демонстрировать, что тестов, указанных в тестовой документации, достаточно для демонстрации функционирования ФБС в соответствии с ее функциональной спецификацией интерфейсов и проектом подсистем.

С.7.4.5.4 Элементы действий оценщика

AOT_DPT.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.4.6 AOT_DPT.3 Тестирование: проект компонентов

Является иерархическим для: AOT_DPT.2 Тестирование: проект подсистем.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_CMP.1 Проект компонентов;

AOT_FUN.1 Функциональное тестирование.

С.7.4.6.1 Цели

Проект компонентов обеспечивает подробное описание внутренних действий ФБС. Тестирование на уровне компонентов обеспечивает доверие к правильности реализации рабочего проекта ФБС.

С.7.4.6.2 Элементы действий разработчика/интегратора

AOT_DPT.3.1D Разработчик/интегратор должен обеспечивать анализ глубины тестирования.

С.7.4.6.3 Элементы содержания и представления свидетельств

AOT_DPT.3.1C Анализ глубины тестирования должен демонстрировать, что тестов, указанных в тестовой документации, достаточно для демонстрации функционирования ФБС в соответствии с ее функциональной спецификацией интерфейсов, с проектом подсистем и проектом компонентов.

С.7.4.6.4 Элементы действий оценщика

AOT_DPT.3.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.4.7 AOT_ DPT.4 Тестирование: представление реализации

Является иерархическим для: AOT_DPT.3 Тестирование: проект компонентов.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_CMP.1 Проект компонентов;

ASD_IMP.1 Представление реализации;

AOT_FUN.1 Функциональное тестирование.

С.7.4.7.1 Цели

Представление реализации ФБС обеспечивает ее фактическое поведение. Тестирование на уровне представления реализации обеспечивает доверие к правильности всесторонней реализации релевантных ФБС.

С.7.4.7.2 Замечания по применению

Представление реализации используется для создания самой ФБС (например, исходный код, который затем компилируется).

С.7.4.7.3 Элементы действий разработчика/интегратора

AOT_DPT.4.1D Разработчик/интегратор должен обеспечивать анализ глубины тестирования.

С.7.4.7.4 Элементы содержания и представления свидетельств

AOT_DPT.4.1C Анализ глубины тестирования должен демонстрировать, что тестов, указанных в тестовой документации, достаточно для демонстрации функционирования ФБС в соответствии с ее функциональной спецификацией интерфейсов, с проектом подсистем, проектом компонентов и представлением реализации.

С.7.4.7.5 Элементы действий оценщика

AOT_DPT.4.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.7.5 Независимое тестирование (AOT_IND)

С.7.5.1 Цели

Целью независимсмого тестирования является демонстрация должного выполнения функций безопасности.

Дополнительной целью является противодействие риску неправильной оценки выходных данных тестов разработчиком, что приводит к неправильной реализации спецификаций или пропуску кода, который не согласуется со спецификациями.

С.7.5.2 Ранжирование компонентов

Данное семейство состоит из трех компонентов. Распределение основано на объеме тестовой документации, тестового обеспечения и объема тестирования оценщиком.

С.7.5.3 Замечания по применению

Тестирование, указанное в данном семействе, может обеспечиваться стороной, обладающей специальными знаниями, отличными от знаний оценщика (например, независимой лабораторией, объективной организацией заказчика). Для тестирования требуется понимание СОО, согласующееся с выполнением других действий по обеспечению доверия, а за оценщиком сохраняется обязанность по соблюдению требований этого семейства при использовании подобного обеспечения.

Данное семейство определяет степень независимости функционального тестирования ФБС. Независимое функциональное тестирование может принимать форму повторения функциональных тестов разработчика в целом или частично, а также форму дополнения к функциональным тестам разработчика с целью расширения области действия этих тестов, их углубления или проверки очевидных слабых мест безопасности общедоступных доменов безопасности, которые могут быть применены к СОО. Эти действия являются вспомогательными, а для каждого СОО должна быть запланирована соответствующая комбинация тестов, в которой учитывается доступность и охват результатов тестов, а также функциональная сложность ФБС. Необходимо разработать план тестов, согласующийся с уровнем других действий по обеспечению доверия, который в случае потребности в более высоком уровне доверия, будет включать в себя более масштабные выборки повторных тестов и более независимые положительные и отрицательные функциональные тесты, выполненные оценщиком.

Целью выборочного контроля за тестами разработчика должно быть подтверждение выполнения разработчиком своей запланированной программы испытаний ФБС и правильности регистрации им результатов испытаний. На число выбранных образцов тестов влияют детализация и качество результатов функциональных тестов разработчика. Оценщику также надо учитывать область разработки дополнительных тестов и относительную пользу, которую можно получить от деятельности в этих двух доменах. Общепризнанно, что в одних случаях повторение всех тестов разработчика может быть полезно и желательно, но весьма затруднительно и менее продуктивно — в других. Таким образом, компонент самого высокого уровня должен использоваться с осторожностью. Выборочный контроль проводится из большой совокупности имеющихся результатов тестов, включая результаты, отвечающие требованиям семейств AOT_COV и AOT_DPT.

Существует также необходимость в рассмотрении различных конфигураций СОО, включенных в оценку. Оценщик должен оценить приемлемость предоставленных результатов и соответствующим образом планировать собственное тестирование.

Независимое функциональное тестирование отличается от испытания на проникновение, если оно основывается на информированном и систематическом поиске уязвимостей в проекте и/или реализации. Испытание на проникновение осуществляется с помощью семейства AOV_VLA.

Пригодность СОО для тестирования основывается на доступе к СОО, вспомогательной документации и информации, требуемой (включая любое испытательное ПО или инструментальные средства) для проведения тестов. Потребность в такой поддержке определяется зависимостями для других семейств для обеспечения доверия.

Кроме того, пригодность СОО для тестирования может основываться на других соображениях. Например, версия СОО, представленная разработчиком, может не быть последней.

Ссылки на подмножество ФБС предназначены для оказания помощи оценщику при проектировании соответствующего набора тестов, согласующихся с целями проводимой оценки.

С.7.5.4 AOT_IND.1 Независимое тестирование-соответствие

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.7.5.4.1 Цели

В данном компоненте целью является демонстрация должного выполнения функций безопасности.

С.7.5.4.2 Замечания по применению

Данный компонент не занимается использованием результатов тестов разработчика. Компонент применим в случае отсутствия таких результатов, а также в случаях, если тестирование разработчика принимается без проверки достоверности. Оценщик требуется для разработки и проведения тестов с целью подтверждения соответствия функциональным требованиям безопасности СОО. Метод проведения тестов заключается в приобретении уверенности в правильности функционирования посредством репрезентативного тестирования вместо проведения каждого возможного теста. Число тестов, планирующихся для подтверждения соответствия фунцкиональным требованиям безопасности СОО, является методологической проблемой, и потребности в тестах должны рассматриваться в контексте конкретного СОО и равновесия и других действий по оценке.

С.7.5.4.3 Элементы действий разработчика/интегратора

AOT_IND.1.1D Разработчик/интегратор должен предоставлять СОО для тестирования.

С.7.5.4.4 Элементы содержания и представления свидетельств

AOT_IND.1.1C СОО должен быть пригодным для тестирования.

С.7.5.4.5 Элементы действий оценщика

AOT_IND.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOT_IND.2.1E Оценщик должен протестировать подгруппу ФБС на правильность для подтверждения должного функционирования СОО.

С.7.5.5 AOT_IND.2 Независимое тестирование-выборка

Является иерархическим для: AOT_IND.1 Независимое тестирование-соответствие.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя;

AOT_FUN.1 Функциональное тестирование.

С.7.5.5.1 Цели

Целью является демонстрация должного выполнения функций безопасности.

Тестирование оценщиком включает в себя отбор и повторение выборки из тестов разработчика.

С.7.5.5.2 Замечания по применению

Предполагается, что разработчик предоставляет оценщику материалы, необходимые для эффективного воспроизведения своих тестов. Материалы могут включать в себя машинно-считываемую тестовую документацию, текстовые программы и т.д.

В данном компоненте содержится требование предоставления оценщику результатов тестов разработчика для дополнения к программе тестирования. Оценщик повторяет выборку из тестов разработчика для приобретения уверенности в полученных результатах.

Получив такую уверенность, оценщик расширяет тестирование разработчика путем проведения дополнительных тестов, в которых СОО используется иным образом.

На основе утвержденных результатов тестов разработчика оценщик может быть уверен в правильном функционировании СОО в более широком диапазоне условий, чем это было возможно при использовании лишь собственных действий разработчика при условии наличия постоянного уровня ресурсов. Будучи уверенным, что разработчик протестировал СОО, оценщик обладает большей свободой для концентрации тестирования на тех участках, где проверка документации или знания специалиста вызывают особую озабоченность.

С.7.5.5.3 Элементы действий разработчика/интегратора

AOT_IND.2.1D Разработчик/интегратор должен предоставлять СОО для тестирования.

С.7.5.5.4 Элементы содержания и представления свидетельств

AOT_IND.2.1C СОО должен быть пригодным для тестирования.

AOT_IND.2.2C Разработчик/интегратор должен предоставлять набор ресурсов, эквивалентный тем, которые были использованы в функциональном тестировании ФБС разработчиком.

С.7.5.5.5 Элементы действий оценщика

AOT_IND.2.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOT_IND.2.2E Оценщик должен протестировать подгруппу ФБС на правильность для подтверждения должного функционирования СОО.

AOT_IND.2.3E Оценщик должен провести выборку тестов в тестовой документации для проверки достоверности результатов тестов разработчика.

С.7.5.6 AOT_IND.3 Независимое тестирование-полнота

Является иерархическим для: AOT_IND.2 Независимое тестирование-выборка.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя;

AOT_FUN.1 Функциональное тестирование.

С.7.5.6.1 Цели

Целью является демонстрация должного выполнения функций безопасности.

Тестирование оценщиком включает повторение всех тестов разработчика.

С.7.5.6.2 Замечания по применению

Предполагается, что разработчик предоставляет оценщику материалы, необходимые для эффективного воспроизведения тестов разработчика/интегратора. Материалы могут включать в себя машинно-считываемую тестовую документацию, текстовые программы и т.д.

В данном компоненте оценщик должен повторить все тесты разработчика как часть программы тестирования. Как и в предыдущем компоненте, оценщик должен также провести тесты, предназначенные для использования СОО, способом, отличным от способа, применявшегося разработчиком. В случаях исчерпывающего тестирования разработчиком необходимость в этом может отсутствовать.

С.7.5.6.3 Элементы действий разработчика/интегратора

AOT_IND.3.1D Разработчик/интегратор должен предоставлять СОО для тестирования.

С.7.5.6.4 Элементы содержания и представления свидетельств

AOT_IND.3.1C СОО должен быть пригодным для тестирования.

AOT_IND.3.2C Разработчик/интегратор должен предоставлять набор ресурсов, эквивалентный тем, которые были использованы в функциональном тестировании ФБС разработчиком.

С.7.5.6.5 Элементы действий оценщика

AOT_IND.3.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOT_IND.3.2E Оценщик должен протестировать подгруппу ФБС на правильность для подтверждения должного функционирования СОО.

AOT_IND.3.3E Для проверки достоверности результатов тестов разработчика оценщик должен выполнить все тесты из тестовой документации.

С.7.6 Регрессионное тестирование (AOT_REG)

С.7.6.1 Цели

Целью является демонстрация должного выполнения функций безопасности после внесения изменений и модификаций в компоненты или конфигурацию системы или среду эксплуатации.

С.7.6.2 Ранжирование компонентов

Состоит из одного компонента.

С.7.6.3 AOT_REG.1 Регрессионное тестирование

Зависимости: зависимости отсутствуют.

С.7.6.3.1 Цели

Целью данного компонента является демонстрация должного выполнения функций безопасности после внесения изменений или модификаций в компоненты и конфигурацию системы или среду эксплуатации.

С.7.6.3.2 Замечания по применению

Этот компонент относится не только к проверке измененных или модифицированных частей автоматизированной системы.

С.7.6.3.3 Элементы действий разработчика/интегратора

AOT_REG.1.1D Разработчик/интегратор должен протестировать выборку тестов разработчика для ФБС и документировать результаты.

AOT_REG.1.2D Разработчик/интегратор должен предоставлять тестовую документацию.

AOT_REG.1.3D Разработчик/интегратор должен обеспечивать анализ степени детализации регрессионного тестирования.

С.7.6.3.4 Элементы содержания и представления свидетельств

AOT_REG.1.1C Тестовая документация должна состоять из планов тестов, описаний тестовых процедур, предполагаемых результатов тестов и фактических результатов.

AOT_REG.1.2C В планах тестов должны быть определены воздействия, вызванные изменениями или модификациями, функции безопасности, предназначенные для тестирования, и изложена цель предполагаемых тестов.

AOT_REG.1.3C В описаниях тестовых процедур должны определяться тесты для измененных или модифицированных частей и излагаться сценарии тестирования каждой функции безопасности. Сценарии тестирования должны включать в себя любые зависимости упорядочения от измененных частей и результаты других тестов.

AOT_REG.1.4C Результаты тестов, выполненных разработчиком/интегратором, должны демонстрировать должное функционирование каждой тестированной функции безопасности и отсутствие воздействия изменений или модификаций на ФБС.

AOT_REG.1.5C Тестовая документация должна включать в себя анализ зависимостей упорядочения тестовых процедур.

С.7.6.3.5 Элементы действий оценщика

AOT_REG.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.8 Класс AOV: анализ уязвимостей автоматизированных систем

С.8.1 Введение

Целью действий по оценке уязвимостей является определение наличия и эксплуатируемости, дефектов и слабых мест автоматизированной системы, сконфигурированной в предназначенной ей среде. Определение наличия и эксплуатируемости, дефектов и слабых мест автоматизированной системы основано на анализе, проведенном разработчиком/интегратором и оценщиком, входных данных заказчика и результатах тестирования со стороны оценщика.

В своей основе действия по анализу уязвимостей тесно связаны с политикой и процедурами безопасности автоматизированной системы, физическими мерами безопасности, безопасностью персонала и наличием инфраструктуры безопасности для эффективного противодействия любым уязвимостям автоматизированной системы. Стойкость функций безопасности автоматизированной системы охватывает аспекты управления безопасностью (в особенности человеческие) для обеспечения сохранения защиты автоматизированной системы и противодействия любым нарушениям этой защиты.

С.8.2 Неправильное применение автоматизированной системы (AOV_MSU)

С.8.2.1 Цели

Целями неправильного применения автоматизированной системы является минимизация возможности конфигурирования или установки СОО, компонентов ИТ и компонентов, не относящихся к ИТ, способом, не обеспечивающим защиту, без пользователя или обсуживающего персонала, способных определить его, а также минимизировать риски человеческих или других ошибок при эксплуатации, которые могут дезактивировать, заблокировать или вызвать отказ при активации функций безопасности и привести к состоянию необнаруживаемой незащищенности.

С.8.2.2 Замечания по применению

Противоречивое, дезориентирующее, неполное, неудобное для пользователя или необоснованное руководство может привести к формированию у пользователя СОО или любой из его подсистем или компонентов мнения о достаточной защищенности СОО или любой из его подсистем или компонентов, которая фактически отсутствует, и появлению вследствие этого уязвимостей.

Примером противоречивого руководства являются две инструкции руководства, которые предполагают разные выходные данные при применении тех же входных данных.

Примером дезориентирующего руководства является описание одной инструкции, которая может толковаться по-разному, и одно из толкований может привести к состоянию незащищенности.

Примером неполного руководства является перечень значимых требований физической безопасности, в котором опущен критически важный пункт, что приводит к невыполнению этого пункта администратором, пользователем или обслуживающим персоналом, которые считают этот перечень полным.

Примером неудобного для пользователя руководства являются нечетко или слишком подробно написанные инструкции, что делает их излишне сложными и трудно воспринимаемыми для администратора, пользователя или обслуживающего персонала, и что может привести к неправильному выполнению какого-либо действия или, возможно, к невыполнению действия совсем, или к неправильным или ненужным действиям, результатом чего может стать незащищенность автоматизированной системы.

Примером необоснованного руководства является рекомендация выполнять слишком обременительную процедуру для администратора, пользователя или обслуживающего персонала.

Руководство является необходимым и может содержаться в существующей документации по СОО либо предоставляться отдельно. В последнем случае оценщик должен подтвердить поставку документации с СОО.

С.8.2.3 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты ранжированы на основе подтверждения описания документации и проверке автоматизированной системы.

С.8.2.4 AOV_MSU.1 Проверка руководств автоматизированной системы

Зависимости:

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.8.2.4.1 Цели

Цель проверки руководств автоматизированной системы заключается в обеспечении отсутствия дезориентирующего, необоснованного и противоречивого руководства в документации руководств и указаний процедур защиты для всех режимов функционирования. Состояния незащищенности должны быть легко обнаруживаемыми.

С.8.2.4.2 Элементы действий разработчика/интегратора

AOV_MSU.1.1.D Разработчик/интегратор должен предоставлять документацию руководств.

AOV_MSU.1.2.D Разработчик/интегратор должен документировать анализ документации руководств.

С.8.2.4.3 Элементы содержания и представления свидетельств

AOV_MSU.1.1.C В документации руководств должны быть определены все возможные режимы функционирования СОО (включая операцию, следующую за отказом или эксплуатационной ошибкой), их последствия и воздействия для поддержания безопасного функционирования.

AOV_MSU.1.2.C Документация руководств должна быть полной, ясной, последовательной и обоснованной.

AOV_MSU.1.3.C В документации руководств должны быть указаны все организационные меры обеспечения безопасности.

AOV_MSU.1.4.C В документации руководств должны быть указаны все зависимости от безопасного функционирования внешних автоматизированных систем.

AOV_MSU.1.5.C В документации по анализу должна быть отражена степень полноты документации.

С.8.2.4.4 Элементы действий оценщика

AOT_MSU.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOT_MSU.1.2E Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения, что СОО можно конфигурировать и использовать безопасно, только пользуясь поставленной документацией руководств.

AOT_MSU.1.3E Оценщик должен определить, что использование документации руководств позволяет выявлять все состояния незащищенности и восстанавливать их до состояния защищенности.

AOT_MSU.1.4E Оценщик должен подтвердить, что в документации анализа отражено предназначение руководств для безопасной работы во всех режимах функционирования СОО.

С.8.2.5 AOT_MSU.2 Анализ и тестирование незащищенных состояний

Является иерархическим для: AOV_MSU.1 Проверка руководства по автоматизированной системе.

Зависимости:

AOD_ADM.1 Руководство администраторов;

AOD_USR.1 Руководство пользователя.

С.8.2.5.1 Цели

Цель анализа и тестирования незащищенных состояний заключается в обеспечении отсутствия дезориентирующего, необоснованного и противоречивого руководства в документации по руководству и указания процедур защиты для всех режимов функционирования. Состояния незащищенности должны легко обнаруживаться. В данном компоненте анализ документации руководств оценщиком требуется для обеспечения дополнительного доверия к соответствию цели; этот анализ проверяется и его достоверность подтверждается посредством тестирования со стороны оценщика.

С 8.2.5.2 Замечания по применению

В данном компоненте оценщик нужен для проведения тестирования с целью обеспечения быстрого обнаружения вхождения СОО в состояние незащищенности.

С.8.2.5.3 Элементы действий разработчика/интегратора

AOV_MSU.2.1.D Разработчик/интегратор должен предоставлять документацию руководства.

AOV_MSU.2.2.D Разработчик/интегратор должен документировать анализ документации руководства.

С.8.2.5.4 Элементы содержания и представления свидетельств

AOV_MSU.1.1.C В документации руководства должны быть определены все возможные режимы функционирования СОО (включая операцию, следующую за отказом или эксплуатационной ошибкой), их последствия и воздействия для поддержания безопасного функционирования.

AOV_MSU.1.2.C Документация руководств должна быть полной, ясной, последовательной и обоснованной.

AOV_MSU.1.3.C В документации руководств должны быть указаны все организационные меры безопасности.

AOV_MSU.1.4.C В документации руководств должны быть указаны все зависимости от безопасного функционирования внешних автоматизированных систем.

AOV_MSU.1.5.C В документации по анализу должна быть отражена степень полноты документации.

С.8.2.5.5 Элементы действий оценщика

AOT_MSU.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOT_MSU.2.2E Оценщик должен повторить все процедуры конфигурирования и установки для подтверждения, что СОО можно конфигурировать и использовать безопасно, только пользуясь поставленной документацией руководств.

AOT_MSU.2.3E Оценщик должен определить, что использование документации руководств позволяет выявлять все состояния незащищенности и восстанавливать их до состояния защищенности.

AOT_MSU.2.4E Оценщик должен подтвердить, что в документации анализа отражено предназначение руководств для обеспечения безопасной работы во всех режимах функционирования СОО.

AOT_MSU.2.5E Оценщик должен проводить независимое тестирование для определения обоснованной способности администратора или пользователя, ознакомленного с документацией руководств, определять, конфигурирован ли и функционирует ли СОО безопасным образом.

С.8.3 Анализ уязвимостей (AOV_VLA)

С.8.3.1 Цели

Анализом уязвимостей является оценка того, способны ли уязвимости, выявленные во время оценки структуры и предполагаемого функционирования СОО или другими методами (например гипотеза дефектов) в течение жизненного цикла автоматизированной системы, мешать ФБС или изменять их, или создавать помехи санкционированным возможностям других пользователей.

С.8.3.2 Замечания по применению

Анализ уязвимостей проводится разработчиком/интегратором с целью определения наличия уязвимостей безопасности, и при анализе должно учитываться содержимое комплектующих узлов СОО. Расположение идентифицированных уязвимостей должно документироваться с тем, чтобы оценщик мог воспользоваться этой информацией при независимом тестировании на проникновение и/или проведении анализа уязвимостей.

Анализ уязвимостей предназначен для подтверждения того, что выявленные уязвимости безопасности не могут быть использованы в предполагаемой среде СОО, и, что СОО невосприимчив к очевидным атакам на проникновение.

Очевидными уязвимостями являются уязвимости открытые для применения, требующего минимального знания СОО, его связанных и не связанных с ИТ компонентами, и минимальных технических навыков, мастерства и ресурсов. Их наличие можно предположить из описания интерфейсов ФБС. Очевидными уязвимостями являются также находящейся в общедоступном домене безопасности, подробности которых должны быть известны разработчику/интегратору или организации пользователя или доступны из органа оценки.

Для систематического поиска уязвимостей требуется структурированная и повторяемая работа разработчика/интегратора в противоположность выявлению уязвимостей безструктурным (произвольным) методом.

Основным назначением независимого анализа уязвимостей оценщиком и связанного с ним тестирования на проникновение является сопротивляемость СОО атакам на проникновение, осуществляемым нарушителем, имеющим низкий (AOV_VLA.2), средний (AOV_VLA.3) или высокий (AOV_VLA.4) потенциал атаки. Оценщик должен предположить роль нарушителя с низким, средним или высоким (соответственно AOV_VLA.2, AOV_VLA.3 или AOV_VLA.4) потенциалами атаки. Использование уязвимостей автоматизированной системы таким нарушителем должно рассматриваться оценщиком как «очевидные атаки проникновения» (по отношению к элементам AOV_VLA.*.2C) в контексте компонентов от AOV_VLA.2 до AOV_VLA.4.

С.8.3.3 Ранжирование компонентов

Данное семейство состоит из четырех компонентов. Эти компоненты распределяются на основе подтверждения анализа разработчиком/интегратором и глубины независимого анализа.

С.8.3.4 Анализ уязвимостей разработчиком_интегратором

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_CON.1 Концепция безопасности функционирования;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.8.3.4.1 Цели

Анализ уязвимостей проводится разработчиком/интегратором для выявления наличия очевидных уязвимостей и подтверждения невозможности их использования в предполагаемой среде СОО.

С.8.3.4.2 Замечания по применению

Оценщик должен учитывать возможность проведения дополнительных тестов потенциально используемых уязвимостей, выявленных в ходе других этапов оценки.

С.8.3.4.3 Элементы действий разработчика/интегратора

AOV_VLA.1.1D Разработчик/интегратор должен проводить и документировать анализ комплектующих узлов СОО для поиска очевидных путей, которыми пользователь может нарушить функции обеспечения безопасности.

AOV_VLA.1.2D Разработчик/интегратор должен документировать расположение очевидных уязвимостей.

С.8.3.4.4 Элементы содержания и представления свидетельств

AOV_VLA.1.1C В документации по всем выявленным уязвимостям должно быть указано о невозможности использования уязвимости в предполагаемой среде СОО.

С.8.3.4.5 Элементы действий оценщика

AOV_VLA.1.1E Оценщик должен подтверждать соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOV_VLA.1.2E Оценщик должен проводить тестирование на проникновение, построенное на анализе уязвимостей, проведенном разработчиком/интегратором, для обеспечения выявления очевидных уязвимостей.

С.8.3.5 AOV_VLA.2 Независимый анализ уязвимостей

Является иерархическим для: AOV_VLA.1 Анализ уязвимостей, проведенный разработчиком/интегратором.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_IMP.1 Представление реализации;

ASD_CON.1 Концепция безопасности функционирования;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.8.3.5.1 Цели

Анализ уязвимостей проводится разработчиком/интегратором для установления наличия очевидных уязвимостей и подтверждения невозможности их использования в предполагаемой среде СОО.

Оценщик проводит независимое тестирование на проникновение, сопровождаемое независимым анализом уязвимостей оценщика, с целью определения сопротивляемости СОО атакам на проникновение, осуществляемым нарушителем с низким потенциалом атаки.

С.8.3.5.2 Элементы действий разработчика/интегратора

AOV_VLA.2.1D Разработчик/интегратор должен проводить и документировать анализ комплектующих узлов СОО для поиска очевидных путей, которыми пользователь может нарушить функции обеспечения безопасности.

AOV_VLA.2.2D Разработчик/интегратор должен документировать расположение очевидных уязвимостей.

С.8.3.5.3 Элементы содержания и представления свидетельств

AOV_VLA.2.1C В документации по всем выявленным уязвимостям должно быть указано о невозможности использования уязвимости в предполагаемой среде СОО.

AOV_VLA.2.2C.В документации должно быть обоснование сопротивляемости СОО со всеми выявленными уязвимостями очевидным атакам на проникновение.

С.8.3.5.4 Элементы действий оценщика

AOV_VLA.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOV_VLA.2.2E Оценщик должен провести тестирование на проникновение, построенное на анализе уязвимостей, проведенном разработчиком/интегратором, для обеспечения указания выявленных уязвимостей.

AOV_VLA.2.3E Оценщик должен провести независимый анализ уязвимостей.

AOV_VLA.2.4E Оценщик должен провести независимое тестирование на проникновение, основанное на независимом анализе уязвимостей, для определения возможности использования дополнительно выявленных уязвимостей в предполагаемой среде.

AOV_VLA 2.5E Оценщик должен определять сопротивляемость СОО атакам на проникновение, осуществляемым нарушителем с низким потенциалом атаки.

С.8.3.6 AOT_VLA.3 Средняя сопротивляемость

Является иерархическим для: AOV_VLA.2 Независимый анализ уязвимостей.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_IMP.1 Представление реализации;

ASD_CON.1 Концепция безопасности функционирования;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.8.3.6.1 Цели

Анализ уязвимостей проводится разработчиком/интегратором для установления наличия очевидных уязвимостей и подтверждения невозможности их использования в предполагаемой среде СОО.

Оценщик проводит независимое тестирование на проникновение, сопровождаемое независимым анализом уязвимостей оценщика, с целью определения сопротивляемости СОО атакам на проникновение, осуществляемым нарушителем со средним потенциалом атаки.

С.8.3.6.2 Элементы действий разработчика/интегратора

AOV_VLA.3.1D Разработчик/интегратор должен проводить и документировать анализ комплектующих узлов СОО для поиска очевидных путей, которыми пользователь может нарушить функции обеспечения безопасности.

AOV_VLA.3.2D Разработчик/интегратор должен документировать расположение очевидных уязвимостей.

С.8.3.6.3 Элементы содержания и представления свидетельств

AOV_VLA.3.1C В документации по всем выявленным уязвимостям должно быть указано о невозможности использования уязвимости в предполагаемой среде СОО.

AOV_VLA.3.2C.В документации должно быть обоснование сопротивляемости СОО со всеми выявленными уязвимостями очевидным атакам на проникновение.

AOV_VLA.3.3C В свидетельстве должна быть отражена систематичность поиска уязвимостей.

С.8.3.6.4 Элементы действий оценщика

AOV_VLA.3.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOV_VLA.3.2E Оценщик должен провести тестирование на проникновение, построенное на анализе уязвимостей, проведенном разработчиком/интегратором, для обеспечения указания выявленных уязвимостей.

AOV_VLA.3.3E Оценщик должен провести независимый анализ уязвимостей.

AOV_VLA.3.4E Оценщик должен провести независимое тестирование на проникновение, основанное на независимом анализе уязвимостей, для определения возможности использования дополнительно выявленных уязвимостей в предполагаемой среде.

AOV_VLA 3.5E Оценщик должен определять сопротивляемость СОО атакам на проникновение, осуществляемым нарушителем со средним потенциалом атаки.

С.8.3.7 AOT_VLA.4 Высокая сопротивляемость

Является иерархическим для: AOV_VLA.3 Средняя сопротивляемость.

Зависимости:

ASD_IFS.1 Функциональная спецификация интерфейсов;

ASD_SSD.1 Проект подсистем;

ASD_IMP.1 Представление реализации;

ASD_CON.1 Концепция безопасности функционирования;

AOD_ADM.1 Руководство администратора;

AOD_USR.1 Руководство пользователя.

С.8.3.7.1 Цели

Анализ уязвимостей проводится разработчиком/интегратором для установления наличия очевидных уязвимостей и подтверждения невозможности их использования в предполагаемой среде СОО.

Оценщик проводит независимое тестирование на проникновение, сопровождаемое независимым анализом уязвимостей оценщика, с целью определения сопротивляемости СОО атакам на проникновение, осуществляемым нарушителем с высоким потенциалом атаки.

С.8.3.7.2 Элементы действий разработчика/интегратора

AOV_VLA.4.1D Разработчик/интегратор должен проводить и документировать анализ комплектующих узлов СОО для поиска очевидных путей, которыми пользователь может нарушить функции обеспечения безопасности.

AOV_VLA.4.2D Разработчик/интегратор должен документировать расположение очевидных уязвимостей.

С.8.3.7.3 Элементы содержания и представления свидетельств

AOV_VLA.4.1C В документации по всем выявленным уязвимостям должно быть указано о невозможности использования уязвимости в предполагаемой среде СОО.

AOV_VLA.4.2C.В документации должно быть обоснование сопротивляемости СОО со всеми выявленными уязвимостями очевидным атакам на проникновение.

AOV_VLA.4.3C В свидетельстве должна быть отражена систематичность поиска уязвимостей.

AOV_VLA.4.4C В документации анализа должно содержаться обоснование полного охвата анализом комплектующих узлов СОО.

С.8.3.7.4 Элементы действий оценщика

AOV_VLA.4.1.E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOV_VLA.4.2E Оценщик должен провести тестирование на проникновение, построенное на анализе уязвимостей, проведенном разработчиком/интегратором, для обеспечения указания выявленных уязвимостей.

AOV_VLA.4.3E Оценщик должен провести независимый анализ уязвимостей.

AOV_VLA.4.4E Оценщик должен провести независимое тестирование на проникновение, основанное на независимом анализе уязвимостей, для определения возможности использования дополнительно выявленных уязвимостей в предполагаемой среде.

AOV_VLA.4.5E Оценщик должен определять сопротивляемость СОО атакам на проникновение, осуществляемым нарушителем с высоким потенциалом атаки.

С.9 Класс AOL: поддержка жизненного цикла автоматизированных систем

С.9.1 Введение

Целью поддержки жизненного цикла автоматизированной системы является определение адекватности процедур, использованных во время интеграции и эксплуатационных жизненных циклов автоматизированной системы. Эти процедуры включают в себя меры обеспечения безопасности, применявшиеся в ходе разработки автоматизированной системы (т.е. интеграции), модель жизненного цикла, применявшуюся интегратором, и инструментальные средства, применявшиеся интегратором на протяжении жизненного цикла автоматизированной системы.

С.9.2 Определение мер обеспечения безопасности автоматизированной системы (AOL_DVS)

С.9.2.1 Цели

Данное семейство обеспечивает меры обеспечения безопасности во время разработки автоматизированной системы. При опытно-конструкторских работах должны соблюдаться конфиденциальность и целостность материалов, задействованных для разработки.

С.9.2.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.9.2.3 AOL_DVS.1 Определение мер обеспечения безопасности

Зависимости: зависимости отсутствуют.

С.9.2.3.1 Элементы действий разработчика/интегратора

AOL_DVS.1.1D Разработчик/интегратор должен создавать документацию по безопасности разработки.

С.9.2.3.2 Элементы содержания и представления свидетельств

AOL_DVS.1.1C В документации по безопасности разработки должны быть изложены все физические, процедурные, относящиеся к персоналу, и другие меры обеспечения безопасности, необходимые для защиты конфиденциальности, аутентичности, надежности и целостности проекта и реализации СОО в его среде разработки и интеграции.

AOL_DVS.1.2C Документация по безопасности разработки должна предоставлять доказательство соблюдения этих мер обеспечения безопасности во время разработки и обслуживания СОО.

С.9.2.3.3 Элементы действий оценщика

AOL_DVS.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.9.2.4 AOL_DVS.2 Проверка мер обеспечения безопасности

Является иерархическим для: AOL_DVS.1 Определение мер обеспечения безопасности.

Зависимости: зависимости отсутствуют.

С.9.2.4.1 Элементы действий разработчика/интегратора

AOL_DVS.2.1D Разработчик/интегратор должен создавать документацию по безопасности разработки.

С.9.2.4.2 Элементы содержания и представления свидетельств

AOL_DVS.2.1C В документации по безопасности разработки должны быть изложены все физические, процедурные, относящиеся к персоналу и другие меры обеспечения безопасности, необходимые для защиты конфиденциальности, аутентичности, надежности и целостности проекта и реализации СОО в его среде разработки и интеграции.

AOL_DVS.2.2C Документация по безопасности разработки должна предоставлять доказательство соблюдения этих мер обеспечения безопасности во время разработки и обслуживания СОО.

С.9.2.4.3 Элементы действий оценщика

AOL_DVS.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

AOL_DVS.2.2E Оценщик должен осуществлять независимую проверку посредством опросов персонала, выборки мер обеспечения безопасности и других методов применения мер обеспечения безопасности.

С.10 Класс ASI: безопасная установка (внедрение) систем

С.10.1 Введение

Во время внедрения системы необходимо создать структуру руководства обеспечением безопасности, назначением которого является пропагандирование и распространение политики безопасности в организации. Руководство должно способствовать безопасности и поддерживать ее посредством активного участия во внедрении безопасности в организации. Действия руководства включают в себя подробное изложение целей безопасности, соответствующих требованиям безопасности, и интегрированы в соответствующие бизнес-процессы. Эти действия включают в себя формулирование, анализ и утверждение политики безопасности, обеспечение четкой и явной поддержки руководства, а также предоставление программ по обучению и обеспечению осведомленности в поддержку политики безопасности организации. Руководство также назначает менеджера в качестве уполномоченного по безопасности организации.

Необходимо также подтверждать адекватность процедур конфигурирования автоматизированной системы как при установке, так и при контрольном запуске.

С.10.2 Осведомленность (ASI_AWA)

С.10.2.1 Цели

В соответствии с данным семейством от руководства требуется обеспечение обучения персонала его ролям и обязанностям в области обеспечения безопасности в процессе своей деловой деятельности в организации.

С.10.2.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.10.2.3 ASI_AWA.1 Обучение с целью повышения осведомленности

Зависимости: зависимости отсутствуют.

С.10.2.3.1 Элементы действий руководства

ASI_AWA.1.1M Руководство должно проводить обучение с целью повышения осведомленности с формальным вводным курсом, предназначенным для ознакомления со всеми организационными мерами безопасности и ожидаемыми от них результатами, предоставляя персоналу доступ к активам автоматизированной системы до периода обучения во время или периодически.

С.10.2.3.2 Элементы содержания и представления свидетельств

ASI_AWA.1.1C Обучение с целью повышения осведомленности должно регистрироваться.

ASI_AWA.1.2C Записи должны содержать дату и время, персонал с правом доступа, обучаемый персонал, содержание и результаты обучения.

С.10.2.3.3 Элементы действий оценщика

ASI_AWA.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.10.2.4 ASI_AWA.2 Проверка обучения с целью повышения осведомленности

Является иерархическим для: ASI_AWA.1 Обучение с целью повышения осведомленности.

Зависимости: зависимости отсутствуют.

С.10.2.4.1 Элементы действий руководства

ASI_AWA.1.1M Руководство должно проводить обучение с целью повышения осведомленности с формальным вводным курсом, предназначенным для ознакомления со всеми организационными мерами безопасности и ожидаемыми от них результатами, предоставляя персоналу доступ к активам автоматизированной системы до периода обучения во время или периодически.

С.10.2.4.2 Элементы содержания и представления свидетельств

ASI_AWA.2.1C Обучение с целью повышения осведомленности должно документироваться.

ASI_AWA.2.2C Записи должны содержать дату и время, персонал с правом доступа, обучаемый персонал, содержание и результаты обучения.

С.10.2.4.3 Элементы действий оценщика

ASI_AWA.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_AWA.2.2E Оценщик должен осуществлять независимую проверку посредством проведения опроса персонала, выборочной проверки прохождения курсов повышения квалификации и других методов проверки результативности проведения подготовки по повышению компетентности персонала.

С.10.3 Доведение (ASI_CMM)

С.10.3.1 Цели

Данное семейство требует от руководства наличия определенных средств передачи документации руководства по эксплуатации, определяющую и предписывающую ФБС для соответствующего персонала.

С.10.3.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.10.3.3 ASI_CMM.1 Информация о мерах обеспечения безопасности

Зависимости: зависимости отсутствуют.

С.10.3.3.1 Элементы действий руководства

ASI_CMM.1.1M Руководство должно передавать все ФБС всему персоналу, имеющему отношение к организационным мерам безопасности, перед предоставлением им доступа к активам автоматизированной системы.

С.10.3.3.2 Элементы содержания и представления свидетельств

ASI_CMM.1.1C Обучение осведомленности должно документироваться.

ASI_CMM.1.2C Записи должны содержать дату и время, персонал с правом доступа, обучаемый персонал, содержание и результаты обучения.

С.10.3.3.3 Элементы действий оценщика

ASI_CMM.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.10.3.4 ASI_CMM.2 Проверка достоверности информации о мерах обеспечения безопасности

Является иерархическим для: ASI_CMM.1 Информация о мерах обеспечения безопасности

Зависимости: зависимости отсутствуют.

С.10.3.4.3 Элементы действий руководства

ASI_CMM.2.1M Руководство должно передавать соответствующие ФБС персоналу, имеющему отношение к организационным мерам безопасности, перед предоставлением им доступа к конкретным активам автоматизированной системы.

С.10.3.4.2 Элементы содержания и представления свидетельств

ASI_CMM.2.1C Обучение осведомленности должно документироваться.

ASI_CMM.2.2C Записи должны содержать дату и время, персонал с правом доступа, обучаемый персонал, содержание и результаты обучения.

С.10.3.4.3 Элементы действий оценщика

ASI_CMM.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_CMM.2.2E Оценщик должен независимым образом проверять посредством опросов персонала, выборки из организационных мер безопасности и других методов достоверность передачи организационных мер безопасности.

С.10.4 Проверка безопасной установки (ASI_SIC)

С.10.4.1 Цели

Данное семейство предоставляет средства проверки установки и пуска СОО. Осуществление установки, пуска СОО и управление ими, должны быть правильными и эффективными в соответствии с политикой безопасности автоматизированной системы.

С.10.4.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.10.4.3 ASI_SIC.1 Проверка безопасной установки

Зависимости: зависимости отсутствуют.

С.10.4.3.1 Элементы действий руководства

ASI_SIC.1.1M Разработчик/интегратор должен документировать процедуры безопасной установки, необходимые для обеспечения возможности безопасной инсталляции, пуска и взаимодействия компонентов и интерфейсов, составляющих СОО, особенно связанных с унаследованными мерами обеспечения безопасности и интерфейсами.

С.10.4.3.2 Элементы содержания и представления свидетельств

ASI_SIC.1.1C В документации по безопасной установке должны излагаться шаги, необходимые для проверки безопасной установки, пуска и взаимодействия СОО в его среде.

С.10.4.3.3 Элементы действий оценщика

ASI_SIC.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.10.4.4 ASI_SIC.2 Верификация проверки безопасной установки

Является иерархическим для: ASI_SIC.1 Проверка безопасной установки.

Зависимости: зависимости отсутствуют.

С.10.4.4.1 Элементы действий руководства

ASI_SIC.2.1M Разработчик /интегратор должен документировать процедуры безопасной установки, необходимые для обеспечения возможности безопасной инсталляции, пуска и взаимодействия компонентов и интерфейсов, составляющих СОО, особенно связанных с унаследованными мерами обеспечения безопасности и интерфейсами.

С.10.4.4.2 Элементы содержания и представления свидетельств

ASI_SIC.2.1C В документации по безопасной установке должны излагаться шаги, необходимые для проверки безопасной установки, пуска и взаимодействия СОО в его среде.

С.10.4.4.3 Элементы действий оценщика

ASI_.SIC.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_.SIC.2.2E Оценщик должен верифицировать, что результатом процедур безопасной установки является безопасная конфигурация.

С.11 Класс ASO: Регистрация и запись в автоматизированных системах

С.11.1 Введение

Автоматизированная система может постоянно находиться в процессе изменения и модификации. Изменения и модификации включают в себя запросы на изменения, пакеты обновлений, патчи прикладного ПО и специальные требования к межоперабельности и совместимости, вызванные добавлением имеющегося внутреннего или внешнего интерфейса или его изменением.

В данном классе содержатся семейства, определяющие правильность и эффективность действий ФБС в ходе функционирования системы. Основным назначением безопасности системы является определение безопасного функционирования автоматизированной системы без нарушения ее политики безопасности. Данный класс также определяет действия, предпринимаемые в случае появления событий, связанных с безопасностью, а также обеспечивает выполнение соответствующих действий по обнаружению и регистрации событий, способных нарушить политику безопасности автоматизированной системы, и реагированию на них.

Семейства данного класса определяют для руководства средства мониторинга и проверки организационных мер безопасности.

С.11.2 Записи об организационных мерах безопасности (ASO_RCD)

С.11.2.1 Цели

Данное семейство обеспечивает записи о функционировании ФБС во время эксплуатации. Организационные меры безопасности должны реализовываться и осуществляться правильно и эффективно в соответствии с политикой безопасности автоматизированной системы.

С.11.2.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.11.2.3 ASO_RCD.1 Запись о функционировании организационных мер безопасности

Зависимости: зависимости отсутствуют.

С.11.2.3.1 Элементы действий руководства

ASO_RCD.1.M Руководство должно регистрировать свидетельства эксплуатации, определенные всеми организационными мерами безопасности.

С.11.2.3.2 Элементы содержания и представления свидетельств

ASO_RCD.1.1C Информация, связанная со свидетельством эксплуатации, должна регистрироваться.

ASO_RCD.1.2C В записях должны указываться дата и время, ответственное лицо, задействованные организационные меры безопасности и результаты функционирования.

С.11.2.3.3 Элементы действий оценщика

ASO_RCD.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.11.2.4 ASO_RCD.2 Проверка записей эксплуатации

Является иерархическим для: ASO_RCD.1 Запись о функционировании организационных мер безопасности.

Зависимости: зависимости отсутствуют.

С.11.2.4.1 Элементы действий менеджмента

ASO_RCD.2.1M Руководство должно регистрировать свидетельства эксплуатации, определенные (все или по выбору) организационные меры безопасности.

С.11.2.4.2 Элементы содержания и представления свидетельств

ASO_RCD.2.1C Информация, связанная со свидетельством эксплуатации, должна регистрироваться.

ASO_RCD.2.2C В записях указывают дату и время, ответственное лицо, задействованные организационные меры безопасности и результаты функционирования.

С.11.2.4.3 Элементы действий оценщика

ASI_.RCD.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_RCD.2.2E Оценщик должен осуществлять независимую проверку посредством опросов персонала, выборок из записей эксплуатации и других методов, правильность регистрации информации, относящейся к функционированию организационных мер безопасности.

С.11.3 Верификация организационных мер безопасности (ASO_VER)

С.11.3.1 Цели

Данное семейство обеспечивает средства проверки организационных мер безопасности в ходе их функционирования. Организационные меры безопасности должны реализовываться и эксплуатироваться правильно и эффективно в соответствии с политикой безопасности автоматизированной системы.

С.11.3.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.11.3.3 ASO_VER.1 Проверка организационных мер безопасности

Зависимости: зависимости отсутствуют.

С.11.3.3.1 Элементы действий руководства

ASO_VER.1.1M Руководство должно проверять все организационные меры безопасности на правильность и эффективность установки и функционирования.

С.11.3.3.2 Элементы содержания и представления свидетельств

ASO_VER.1.1C Информация, связанная с проверкой, должна регистрироваться.

ASO_VER.1.2C В записях должны указываться дата и время и ответственное лицо, задействованные организационные меры безопасности и результаты проверки.

С.11.3.3.3 Элементы действий оценщика

ASI_VER.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.11.3.4 ASO_VER.2 Независимая проверка организационных мер безопасности

Является иерархическим для: ASO_VER. Проверка организационных мер безопасности.

Зависимости: зависимости отсутствуют.

С.11.3.4.1 Элементы действий руководства

ASO_VER.2.1M Руководство должно проверять (все или по выбору) организационные меры безопасности на правильность и эффективность установки и функционирования.

С.11.3.4.2 Элементы содержания и представления свидетельств

ASO_VER.2.1C Информация, связанная с проверкой, должна регистрироваться.

ASO_VER.2.2C В записях должны указываться дата и время и ответственное лицо, а также запланированные организационые меры безопасности и результаты проверки.

С.11.3.4.3 Элементы действий оценщика

ASI_VER.2.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_VER.2.2E Оценщик должен осуществлять независимую проверку посредством опросов персонала, выборки из организационных мер безопасности и других методов, правильность и эффективность установки и функционирования организационных мер безопасности.

С.11.4 Мониторинг организационных мер безопасности (ASO_MON)

С.11.4.1 Цели

Данное семейство обеспечивает средства мониторинга организационных мер безопасности во время функционирования. Основной целью мониторинга является установление того, что организационные меры безопасности функционируют безопасным образом и отсутствуют нарушения политик безопасности автоматизированной системы. Организационные меры безопасности должны реализовываться и функционировать правильно и эффективно в соответствии с политикой безопасности автоматизированной системы. Мониторинг организационных мер безопасности также определяет действия, предпринимаемые при появлении любых изменений в автоматизированной системе.

С.11.4.2 Ранжирование компонентов

Данное семейство состоит из двух компонентов. Эти компоненты распределяются на основе подтверждения описания в документации и проверок в автоматизированной системе.

С.11.4.3 ASO_MON.1 Мониторинг организационных мер безопасности руководством

Зависимости: зависимости отсутствуют.

С.11.4.3.1 Элементы действий руководства

ASO_MON.1.1M Руководство должно через одинаковые промежутки времени контролировать средства обеспечения и уровни производительности всех организационных мер безопасности.

ASO_MON.1.2M Руководство должно контролировать внесение изменений в предоставление услуг, включая поддержание и усовершенствование политик, процедур и мер обеспечения безопасности с учетом критичности задействованных бизнес-систем и бизнес-процессов и повторной оценки рисков.

С.11.4.3.2 Элементы содержания и представления свидетельств

ASO_MON.1.1C Информация, связанная с мониторингом, должна регистрироваться.

ASO_MON.1.2C В записях должны указываться дата и время и ответственное лицо, а также запланированные организационые меры безопасности и результаты проверки.

С.11.4.3.3 Элементы действий оценщика

ASO_MON.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

С.11.4.4 ASO_MON.2 Верификация мониторинга организационных мер безопасности

Является иерархическим для: ASO_MON.1 Мониторинг организационных мер безопасности руководством.

Зависимости: зависимости отсутствуют.

С.11.4.4.1 Элементы действий руководства

ASO_MON.2.1M Руководство должно через одинаковые промежутки времени контролировать средства обеспечения и уровни производительности всех организационных мер безопасности.

ASO_MON.2.2M Руководство должно контролировать внесение изменений в предоставление услуг, включая поддержание и усовершенствование политик, процедур и мер обеспечения безопасности с учетом критичности задействованных бизнес-систем, бизнес-процессов и повторной оценки рисков.

С.11.4.4.2 Элементы содержания и представления свидетельств

ASO_MON.1.1C Информация, связанная с мониторингом, должна регистрироваться.

ASO_MON.1.2C В записях должны указываться дата и время и ответственное лицо, а также запланированные организационые меры безопасности и результаты проверки.

С.11.4.4.3 Элементы действий оценщика

ASO_MON.1.1E Оценщик должен подтвердить соответствие представленной информации всем требованиям к содержанию и представлению свидетельств.

ASI_MON 2.2E Оценщик должен осуществлять независимую проверку (посредством опросов персонала, выборки изменений и другими методами) соответствия проведения мониторинга политике безопасности.

Приложение D
(справочное)

Взаимосвязь с разработкой Общих критериев

В настоящем приложении определены очевидные различия между критериями оценки автоматизированных систем и критериями проекта для комментариев Общих критериев (версия 3.0) [14], а также определена необходимость пересмотра настоящего стндарта при распространении изменений в Общих критериях на новую версию ИСО/МЭК 15408.

В основной части данного стандарта нет ничего специфического для версии Общих критериев и, похоже, что изменения не потребуются после пересмотра ИСО/МЭК 15408 в соответствии с [13].

В приложении А настоящего стандарта определены схема и содержание ПЗС и ЗБС. Приложение А было подготовлено с учетом предлагаемых изменений в схеме и содержании ПЗС и ЗБС стандартов серии ИСО/МЭК 15408, имея в виду [14]. В данном приложении по мере возможности эти предлагаемые изменения приняты. Существует одно основное различие между структурами, используемыми для оценки автоматизированных систем, и структурами, предлагаемыми в [14], которое заключается в возможности оценки специфических для доменов требований и мер обеспечения безопасности. Это различие является преднамеренным и сохранится после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14].

В приложении А рассматриваются функциональные требования автоматизированной системы. Оно структурировано иначе, чем в стандартах серии ИСО/МЭК 15408, основываясь на структурах, заимствованных из НИСТ СП 800-53 [9] и ИСО/МЭК 17799 [8]. Таким образом, основные изменения в функциональных требованиях стандартов серии ИСО/МЭК 15408 и [14] не оказали влияния на содержание настоящего стандарта; новые компоненты для технических мер безопасности автоматически включаются обновленной ссылкой. Для совместимости с терминологией [14] название приложения А следует изменить на «Функциональные компоненты автоматизированной системы».

Требования доверия к автоматизированной системе рассматриваются в приложении С настоящего стандарта. В нем определены девять новых классов требований доверия. Некоторые из них являются совершенно новыми, некоторые основаны на классах и семействах по стандартам серии ИСО/МЭК 15408. Следовательно, необходимо рассмотреть каждое семейство отдельно. Для совместимости с терминологией [14] название приложения А следует изменить на «Компоненты доверия к автоматизированной системе».

Оценка ПЗС рассматривается в классе ASP, подобного классу APE [14], приложения С настоящего стандарта. Семейство ASP_INT имеет различия, обусловленные наличием взаимосвязей с внешними автоматизированными системами и необходимостью обозначения доменной организации. Ссылка на аппаратные и программно-аппаратные средства, не связанные с ОО, не делается, поскольку во всех случаях они образуют часть автоматизированной системы. Имеются два компонента семейства, разделенных на уровни в зависимости от степени значимости предоставленной информации, касающейся целей безопасности для каждого домена. У семейства ASP_CCL отсутствует утверждение соответствия, поскольку профили защиты системы охватывают все аспекты взаимосвязанных автоматизированных систем. Семейство ASP_SPD рассматривает не угрозы, а риски, и не допускает предположений о среде эксплуатации, поскольку среда эксплуатации является частью оцененной автоматизированной системы. Семейство ASP_OBJ допускает использование цели для внешних автоматизированных систем, но не для среды эксплуатации, поскольку оно является частью оцененной автоматизированной системы. Следовательно, семейство ASP_OBJ имеет только один компонент. Семейство ASP_REQ допускает соответствие внешних автоматизированных систем целям данного семейства. Существует много дополнительных семейств, касающихся специфических для доменов требований. Все они являются преднамеренными различиями и остаются после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14]. Существует некоторое число второстепенных различий, таких как проверка согласованности определений проблем безопасности и целей, которые могут представлять проблемы в [14].

Оценка ЗБС рассматривается в классе ASP, подобного классу APE [14], приложения С настоящего стандарта. Различия между ними аналогичны различиям между классами ASP и APE по профилям защиты. Семейство ASS_INT имеет различия, обусловленные наличием взаимосвязей с внешними автоматизированными системами и необходимостью обозначения доменной организации и средами разработки. Ссылка на не связанные с ОО аппаратные и программно-аппаратные средства отсутствует, поскольку во всех случаях они образуют часть автоматизированной системы. Имеются два компонента семейства, разделенных на уровни в зависимости от степени значимости предоставленной информации, касающейся целей безопасности для каждого домена. У семейства ASP_CCL отсутствует утверждение соответствия, поскольку профили защиты системы охватывают все аспекты обеспечения безопасности взаимосвязанных автоматизированных систем. Семейство ASP_SPD рассматривает не угрозы, а риски, и не допускает предположений о среде эксплуатации, поскольку она является частью оцененной автоматизированной системы. Семейство ASP_OBJ допускает цели для внешних автоматизированных систем, но не для среды эксплуатации, поскольку она является частью оцененной автоматизированной системы. Следовательно, оно имеет только один компонент. Семейство ASP_REQ допускает соответствие внешних авто-

матизированных систем целям данного семейства. Семейство ASE_TSS запрашивает подробности удовлетворения требований доверия. Это необходимо, поскольку разные домены соответствуют требованиям по-разному. Существует много дополнительных семейств, касающихся специфических для доменов требований. Все они являются преднамеренными различиями и остаются после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14]. Существует некоторое число второстепенных различий, таких как проверка согласованности определений проблем безопасности и целей, которые могут представлять проблемы в [14].

Класс AOD приложения С рассматривает документацию руководства по эксплуатации. Семейства AOD_OCD и AOD_GVR являются уникальными для оценки автоматизированной системы. Однако семейства AOD_ADM и AOD_USR основаны на семействах AGD_ADM и AGD_USR стандартов серии ИСО/МЭК 15408. В [14] они заменены одним семейством AGD_OPE. Подобная реорганизация требуется и для автоматизированных систем, что приводит к незначительным изменениям в AOD_GVR.

Класс ASD приложения С рассматривает проект и архитектуру системы. Его основой является класс ADV стандартов серии ИСО/МЭК 15408, но со значительными изменениями, связанными с дополнительной информацией об автоматизированных системах и их внутренней структурой. Семейство ASD_SAD не имеет аналога в стандартах серии ИСО/МЭК 15408, но оно охватывается частью нового семейства ADV_TDS [14]. Семейство ASD_IFS основано на ADV_FSP, но ограничено по спецификациям интерфейсов, когда другие характеристики безопасности проверяются через различные уровни документации проекта. ASD_HLD основано на ADV_SSD, ASD_CMP на ADV_LLD и ASD_IMP на ADV_IMP, но во всех случаях они расширены с целью охвата всех аспектов автоматизированных систем с одним уровнем информации. Наконец, семейство ASD_CON является новым, идентичным по замыслу новому семейству ADV_ARC [13].

Согласование между классом ADV ИСО/МЭК 15408 и классом ADV [13] является очень сложным. Для распространения изменений на данную серию стандартов требуется полная переработка текущего класса ASD.

Класс управления конфигурацией AOC приложения С является скорее дополнением, а не заменой класса ACM по стандартам серии ИСО/МЭК 15408. Семейство AOC_OBM связано с управлением эксплуатационной конфигурацией. Семейства AOC_ECP, AOC_PPC и AOC_NCP связаны с доверием к покупным продуктам. В [14] класс ACM был поглощен классом ACL. Компонент ALC.CMC.5, Передовая поддержка, реализует ограниченную форму AOC_OBM. Однако AOC_OBM является более общим и будет все еще нужен после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14].

Класс тестирования AOT приложения С в большей степени основан на классе ATE стандартов серии ИСО/МЭК 15408 с дополнительным семейством AOT_REG для выполнения регрессионного тестирования во время функционирования системы. AOT_FUN заимствовано из ATE_FUN с дополнительными требованиями для тестирования интегрированных мер обеспечения безопасности, и только один уровень в качестве упорядоченного уровня считается значимым для автоматизированной системы. AOT_COV заимствовано из ATE_COV с незначительными изменениями в различных требованиях к документации и не аналогично уровню ATE.COV.1. AOT_DPT заимствовано из ATE_DPT с незначительными изменениями, являющихся следствием различных требований к документации. Это относится и к AOT_IND. В [14] все эти четыре семейства по существу неизменны. Были внесены изменения в некоторые требования для разъяснения их значения. Некоторые части документации имеют различные названия. После пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14] эти редакционные изменения должны быть повсеместно распространены. Дополнительное семейство AOT_REG остается неизменным.

Класс AOV приложения С занимается анализом уязвимостей. Класс AOV получен из нескольких семейств класса AVA ИСО/МЭК. Аналог семейства AVA_SOF отсутствует, поскольку реализация организационных мер безопасности вероятностными или перестановочными механизмами очень маловероятна. Аналогичным образом отсутствует эквивалент AVA_CCA, поскольку крайне маловероятна реализация скрытых каналов через побочные эффекты организационных мер безопасности. Семейство AOV_MSU основано на AVA_MSU, но без эквивалента самому нижнему уровню AVA.MSU.1. Семейство AOV_MSU рассматривает случаи неправильного использования организационных мер безопасности, а не предположения среды эксплуатации AVA_MSU. В [14] семейство AVA_MSU включено в класс AGD. Подобный подход можно использовать в автоматизированных системах. Последнее семейство AOV_VLA основано на AVA_VLA, но реструктуировано с намерением сделать явной цель анализа уязвимостей. В [14] аналогичное семейство AVA_VAN имеет совершенно другой подход — он возлагает ответственность за анализ уязвимостей на оценщика и увеличивает число уровней по сравнению с AVA_VLA. Эту новую философию в основном следует перенести на AOV_VLA с редакционными изменениями для работы с различными составными частями документации.

Класс поддержки жизненного цикла AOL приложения С состоит из одного семейства AOL_DVS, рассматривающего меры обеспечения безопасности для защиты среды разработки. Данное семейство почти идентично ALC_DVS [14], гораздо ближе к этой версии, чем семейство ALC_DVS стандартов серии ИСО/МЭК 15408. Поскольку семейство связано только с безопасностью среды разработки, возможно его удаление после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14] и замена пересмотренной версией ADV_DVS.

Два последних класса ASI и ASO приложения С связаны с организационными мерами безопасности соответственно при установке и функционировании. Классы ASI и ASO являются новыми и не связаны ни с каким классом по стандартам серии ИСО/МЭК 15408, и, следовательно, существует вероятность того, что изменения не понадобятся после пересмотра стандартов серии ИСО/МЭК 15408 в соответствии с [14].

Приложение Е
(справочное)

Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам

Таблица Е.1

Обозначение ссылочного международного стандарта	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 15408-1:2005	ГОСТ Р ИСО/МЭК 15408-1—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
ИСО/МЭК 15408-2:2005	ГОСТ Р ИСО/МЭК 15408-2—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
ИСО/МЭК 15408-3:2005	ГОСТ Р ИСО/МЭК 15408-3—2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
ИСО/МЭК 13335-1:2004	ГОСТ Р ИСО/МЭК 13335-1—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ИСО/МЭК ТО 13335-3:1998	ГОСТ Р ИСО/МЭК ТО 13335-3—2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
ИСО/МЭК ТО 13335-4:2000	ГОСТ Р ИСО/МЭК ТО 13335-4—2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
ИСО/МЭК ТО 13335-5:2001	ГОСТ Р ИСО/МЭК ТО 13335—2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
ИСО/МЭК 17799:2005	ГОСТ Р ИСО/МЭК 17799—2006 Информационная технология. Методы и средства обеспечения безопасности. Практические правила менеджмента информационной безопасности
ИСО/МЭК 27005	*
ИСО/МЭК 18045	ГОСТ Р ИСО/МЭК 18045—2008 Информационная безопасность. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
ИСО/МЭК ТО 15446:2004	*
ИСО/МЭК 21827:2002	*
ИСО/МЭК ТО 15443 (все части)	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

Библиография

[1] ИСО/МЭК 13335-1:2004* Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
(ISO/IEC 13335-1:2004) (Information technology. Security techniques. Part 1: Concepts and models for information and communications technology security management)

[2] ИСО/МЭК ТО 13335-3:1998* Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы управления безопасностью информационных технологий
(ISO/IEC TR 13335-3):1998 (Information technology. Security techniques. Part 3: Techniques for information technology security)

[3] ИСО/МЭК ТО 13335-4:2000* Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
(ISO/IEC TR 13335-4):2000 (Information technology. Security techniques. Part 4: Selection of safeguards)

[4] ИСО/МЭК 13335-5:2001* Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
(ISO/IEC 13335-5):2001 (Information technology. Security techniques. Part 5: Management guidance on network security)

[5] ИСО/МЭК 27005:2008 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
(ISO/IEC 27005):2008 (Information technology. Security techniques. Information security risk management)

[6] Руководство по сертификации и аккредитации безопасности федеральных информационных систем, Специальная публикация НИСТ СП 800-37, Министерство торговли, США
(Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication SP 800-37, Department of Commerce, United States)

[7] ИСО/МЭК ТО 15443 (все части) Информационная технология. Методы и средства обеспечения безопасности. Основа доверия к безопасности ИТ
[(ISO/IEC TR 15443 (all parts)] (Information technology. Security techniques. A framework for IT security assurance)

[8] ИСО/МЭК 17799:2005 Информационная технология. Методы и средства обеспечения безопасности. Свод правил по управлению информационной безопасностью
(ISO/IEC 17799):2005 (Information technology. Security techniques. Code of practice for information security management)

[9] Рекомендуемые средства обеспечения безопасности для федеральных информационных систем, Специальная публикация НИСТ СП 800-53, Второй публичный проект, сентябрь 2004 года, Министерство торговли, США
(Recommended Security Controls for Federal Information Systems, NIST Special Publication SP 800-53, Second Public Draft, September 2004, Department of Commerce, United States)

[10] ИСО/МЭК 21827:2002 Информационная технология. Проектирование безопасности систем. Модель зрелости
(ISO/IEC 21827):2002 (Information technology. Security techniques. System security engineering. Capability maturity model)

[11] ИСО/МЭК ТО 15446:2004 Информационная безопасность. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности
(ISO/IEC/TR 15446):2004 (Information technology. Security techniques. Guide for the production of protection profiles and security targets)

* Стандарты серии ИСО/МЭК 13335 заменяются стандартами из серии ИСО/МЭК 27000.

[12] Руководство по оценке средств обеспечения безопасности в федеральных информационных системах, Специальная публикация НИСТ СП 800-53А, Министерство торговли, США
(Guide for Assessing the Security Controls in Federal Information Systems, NIST Special Publication. SP 800-53A, Department of Commerce, United States)

[13] Руководство по защите базы ИТ, Федеральное ведомство по безопасности технологии сбора, обработки и передачи информации, Германия, 3-88784-915-9
(IT Baseline Protection Manual, Bundesamt für Sicherheit in der Informationstechnik, Germany. ISBN 3-88784-915-9)

[14] Общие критерии оценки безопасности информационных технологий, Версия 3.0, редакция 2, июнь 2005 г., Совет по разработке общих критериев
(Common criteria for Information technology security evaluation, Version 3.0, Revision 2, June 2005, Common criteria development board)

[15] ИСО/МЭК 18045:2005 — Информационная безопасность. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий
(ISO/IEC 18045):2005 — (Information technology. Security techniques. Methodology for IT security evaiuation)

УДК 351.864.1:004:006.354 ОКС 35.040 Т00

Ключевые слова: автоматизированная система, обеспечение безопасности автоматизированных систем, оценка автоматизированных систем

Редактор *В. Н. Колысов*
Технический редактор *Н. С. Гришанова*
Корректор *Н. И. Гаврищук*
Компьютерная верстка *Т. Ф. Кузнецовой*

Сдано в набор 09.03.2010. Подписано в печать 05.05.2010. Формат 60×84 1/8. Бумага офсетная. Гарнитура Ариал. Печать офсетная. Усл. печ. л. 14.42. Уч.-изд. л. 16,10. Тираж 251 экз. Зак. 440

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru
Набрано и отпечатано в Калужской типографии стандартов, 248021 Калуга, ул. Московская, 256.