*Проект*

Изображение государственного Герба Республики Казахстан

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

**Критерии оценки безопасности IT**

**Часть 4**

**СТРУКТУРА СПЕЦИФИКАЦИИ МЕТОДОВ И ДЕЙСТВИЙ ОЦЕНКИ**

**СТ РК** **ISO/IEC 15408-4**

*(ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 4. Framework for the specification of evaluation methods and activities, IDT)*

*Настоящий проект стандарта не подлежит применению до его утверждения*

**Комитет технического регулирования и метрологии**

**Министерства торговли и интеграции Республики Казахстан**

**(Госстандарт)**

**Астана**

**Предисловие**

**1 ПОДГОТОВЛЕН И ВНЕСЕН** РГП на ПХВ «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан

**2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ** Приказом Председателя Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан № \_\_ от « » \_\_\_\_ 202\_года

**3** Настоящий стандарт идентичен международному стандарту   
ISO/IEC 15408-4:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 4. Framework for the specification of evaluation methods and activities (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности IT. Часть 4. Структура спецификации методов и действий оценки)

Международный стандарт ISO/IEC 15408-4:2022 разработан Подкомитетом SC 27 «Информационная безопасность, кибербезопасность и защита конфиденциальности»

Перевод с английского языка (en)

Официальный экземпляр международного стандарта, на основе которого разработан настоящий стандарт имеется в Едином государственном фонде нормативных технических документов

Степень соответствия – идентичная (IDT)

**4 ВВЕДЕН ВПЕРВЫЕ**

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном каталоге «Документы по стандартизации», а текст изменений и поправок - в периодически издаваемых информационных каталогах «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в периодически издаваемом информационном каталоге «Национальные стандарты»*

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан.

**Содержание**

|  |  |  |
| --- | --- | --- |
| Введение | | IV |
| 1 | Область применения | 1 |
| 2 | Нормативные ссылки | 1 |
| 3 | Термины и определения | 1 |
| 4 | Общая модель методов оценки и мероприятия оценки | 2 |
| 4.1 | Концепции и модель | 2 |
| 4.2 | Вывод методов оценки и мероприятий оценки | 3 |
| 4.3 | Использование глаголов в описании методов оценки и мероприятий оценки | 6 |
| 4.4 | Соглашения для описания методов оценки и мероприятий оценки | 7 |
| 5 | Структура метода оценки | 7 |
| 5.1 | Обзор | 7 |
| 5.2 | Спецификация метода оценки | 8 |
| 6 | Структура мероприятия оценки | 14 |
| 6.1 | Обзор | 14 |
| 6.2 | Спецификация мероприятия оценки | 14 |
| Библиография | | 18 |
| Приложение В.А *(информационное)* Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств | | 19 |

**Введение**

Серия стандартов ISO/IEC 15408 допускает сопоставимость результатов независимых оценок безопасности, предоставляя общий набор требований к функциональности безопасности ИТ-продуктов и к мерам обеспечения безопасности, применяемым к настоящим ИТ-продуктам во время оценки безопасности. ISO/IEC 18045 предоставляет сопутствующую методологию для некоторых требований обеспечения безопасности, указанных в серии стандартов ISO/IEC 15408.

Модель оценки безопасности в ISO/IEC 15408-1 определяет, что общие мероприятия оценки высокого уровня определены в ISO/IEC 18045, но более конкретные мероприятия оценки (EA) могут быть определены как технологически-конкретные адаптации настоящих общих мероприятий для конкретных контекстов оценки, например, для функциональных требований безопасности (SFR) или требований обеспечения безопасности (SAR), применяемых к конкретным технологиям или типам целей оценки (TOE). Спецификация таких мероприятий оценки уже встречается среди практиков, и это создает потребность в спецификации для определения таких мероприятий оценки.

В настоящем стандарте описывается структура, которая может быть использована для выведения мероприятий оценки из единиц работы ISO/IEC 18045 и группировки их в методы оценки (EM). Оценочные мероприятия или методы оценки могут быть включены в профили защиты (PP) и любые поддерживающие их документы. Если PP, PP-Конфигурация, PP-Модуль, пакет или Задание по безопасности (ST) идентифицируют, что должны использоваться конкретные методы оценки/мероприятия оценки, то оценщики должны в соответствии с ISO/IEC 18045 следовать и сообщать о соответствующих методах оценки/мероприятиях оценки при назначении решений оценщиков. Как отмечено в ISO/IEC 15408-1, в некоторых случаях орган по оценке может принять решение не одобрять использование определенных методов оценки/мероприятий оценки: в таком случае орган по оценке может принять решение не проводить оценки после ST, требующего настоящих методов оценки/мероприятий оценки.

Настоящий стандарт также позволяет определять мероприятия оценки для расширенных требований обеспечения безопасности (SAR), и в настоящем случае вывод мероприятий оценки относится к эквивалентным элементам действий и единицам работы, определенным для настоящих расширенных требований обеспечения безопасности (SAR). Если в настоящем стандарте указывается ссылка на использование ISO/IEC 18045 или ISO/IEC 15408-3 для SAR (например, при определении обоснований для мероприятия оценки), то в случае расширенного SAR ссылка применяется к эквивалентным элементам действий и единицам работы, определенным для настоящего расширенного SAR.

Для ясности в настоящем стандарте указывается, как определять методы оценки и мероприятия оценки, но сам документ не указывает примеры методов оценки или мероприятия оценки.

Следующее примечание присутствует в других частях серии ISO/IEC 15408 и в ISO/IEC 18045 для описания использования полужирного шрифта и курсива в настоящих стандартах. В настоящем стандарте эти соглашения не используются, но примечание было сохранено для согласования с остальной частью серии.

Примечание - В настоящем стандарте в некоторых случаях используется полужирный шрифт и курсив, чтобы отличать термины от остального текста. Связь между компонентами в пределах семейства стандартов выделена с помощью соглашения о выделении полужирным шрифтом. Настоящее соглашение требует использования полужирного шрифта для всех новых требований. Для иерархических компонентов требования представлены полужирным шрифтом, когда они улучшены или изменены сверх требований предыдущего компонента. Кроме того, любые новые или улучшенные разрешенные операции сверх предыдущего компонента также выделены полужирным шрифтом.

Использование курсива указывает на текст, который имеет точное значение. Для требований обеспечения безопасности соглашение касается конкретных глаголов, связанных с оценкой.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

**Критерии оценки безопасности IT**

**Часть 4**

**СТРУКТУРА СПЕЦИФИКАЦИИ МЕТОДОВ И ДЕЙСТВИЙ ОЦЕНКИ**

**Дата введения \_\_\_\_ -\_\_-\_\_**

**1 Область применения**

Настоящий стандарт устанавливает стандартизированную структуру для указания объективных, повторяемых и воспроизводимых методов оценки и мероприятий оценки.

Настоящий стандарт не распространяется на способы оценивания, принятия или поддержки методов оценки и мероприятия оценки. Настоящие аспекты являются задачей тех, кто создает методы оценки и мероприятия оценки в своей конкретной области интересов.

**2 Нормативные ссылки**

Для применения настоящего стандарта необходимы, следующие ссылочные документы. Для недатированных ссылок применяют последнее издание ссылочного документа (включая все его изменения):

ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1. Introduction and general model (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 1. Введение и общая модель).

ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 2. Security functional components (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 2. Функциональные компоненты безопасности).

ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3. Security assurance components (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 3. Компоненты доверия к безопасности).

ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection. Methodology for IT security evaluation (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Методология оценки безопасности информационных технологий).

**3 Термины и определения**

В настоящем стандарте применяются термины по ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 и ISO/IEC 18045.

***Проект 1 редакция***

Примечание – ISO и IEC поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

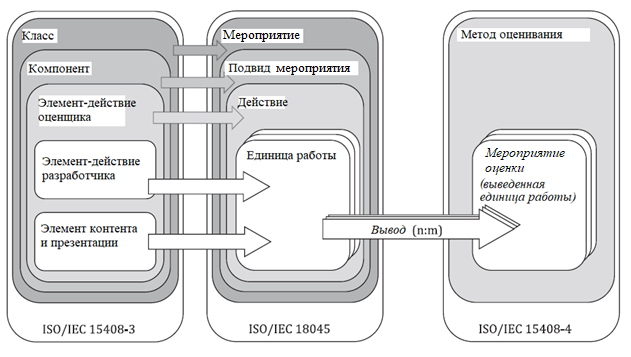
— Платформа онлайн-просмотра ISO: доступна по адресу <https://www.iso.org/obp>.

— IEC Electropedia: доступно по адресу https://[www.electropedia.org/](http://www.electropedia.org/).

**4 Общая модель методов оценки и мероприятия оценки**

**4.1 Концепции и модель**

ISO/IEC 18045 определяет общий набор единиц работы, которые оценщик выполняет для вынесения решения по большинству классов, семейств и компонентов обеспечения, определенных в ISO/IEC 15408-3. Связь между структурой SAR в   
ISO/IEC 15408-3 и единицами работы в ISO/IEC 18045 описана в ISO/IEC 18045 и обобщена на рисунке 1.



**Рисунок 1 – Сопоставление структур ISO/IEC 15408-3 и ISO/IEC 18045 со структурами настоящего стандарта**

Для целей определения новых методов оценки и мероприятия оценки главное, что следует отметить, это то, что каждое действие (представляющее элемент действия оценщика в ISO/IEC 15408-3 или подразумеваемый элемент действия оценщика) представлено в ISO/IEC 18045 как набор единиц работы, которые выполняются оценщиком.

В настоящем стандарте указаны способы, с помощью которых новые мероприятия оценки могут быть получены из общих единиц работы в ISO/IEC 18045 и объединены в метод оценивания, предназначенный для использования в некотором конкретном контексте оценивания. Типовым примером такого контекста оценки будет определенный тип TOE или определенный тип технологии.

***Пример*** - Тип TOE: сетевое устройство

Тип технологии: определенные криптографические функции

Если методы оценки и мероприятия оценки должны использоваться с определенным PP, PP-модулем, PP-конфигурацией, то PP или PP-модуль или PP-конфигурация должна идентифицировать настоящее требование в своем заявлении о соответствии. Если методы оценки и мероприятия оценки должны использоваться с определенным пакетом, то пакет должен идентифицировать это требование в разделе требований безопасности. Если методы оценки и мероприятия оценки заявляются в ST (Задание по безопасности) в результате того, что ST заявляет о соответствии PP, PP-конфигурации или пакету, то ST должен идентифицировать EM(методы оценки)/EA (мероприятия оценки), используемые в его заявлении о соответствии. Ни в одном из настоящих случаев не делается формального заявления о соответствии ISO/IEC 15408-4 (контент PP, PP-модулей, PP-конфигураций и пакетов более подробно описано в ISO/IEC 15408-1).

PP, PP-конфигурация, PP-модуль или пакет могут использовать несколько методов оценки или отдельный набор мероприятий оценки.

***Пример*** - Несколько методов оценки могут использоваться, если для криптографических операций и для протоколов защищенных каналов, используемых в PP, определены отдельные методы оценки.

Примечание - В случае использования точного соответствия ISO/IEC 15408-1 устанавливает, что методы оценки /мероприятия оценки не могут быть определены в конфигурации PP: методы оценки/мероприятия оценки, которые будут использоваться, включены в PP и PP-модули, а не в конфигурацию PP).

Когда PP, PP-модуль, PP-конфигурация или пакет идентифицируют, что должны использоваться определенные методы оценки/мероприятия оценки, то это выполняется с использованием стандартной формулировки, которая устанавливает требование и ссылается на определение методов оценки/ мероприятия оценки, которые будут использоваться. ST должен идентифицировать только требуемые методы оценки и мероприятия оценки, которые включены в PP, PP-модуль, PP-конфигурацию или пакет, на соответствие которым ST заявляет (т. е. сам ST не должен добавлять, изменять или удалять какие-либо методы оценки или мероприятия оценки). ST должен включать идентификацию всех методов оценки/мероприятия оценки, которые он требует (т. е. включая любые, которые требуются PP, PP-модулями, PP-конфигурациями или пакетами, о соответствии которым заявляет ST), так что есть единый перечень, который могут проверять и на который могут ссылаться оценщики и читатели ST.

Методы оценки и мероприятия оценки могут быть определены в документе, который их требует (например, как часть PP), или внешне в другом документе (или в комбинации того и другого). Несмотря на то, что идентификация требуется, в соответствии с описанием выше, не обязательно воспроизводить текст методов оценки/мероприятий оценки в других документах (например, ST не обязательно должен включать полный текст методов оценки/мероприятий оценки из PP, о соответствии которому он заявляет).

**4.2 Вывод методов оценки и мероприятий оценки**

В целом, определение мероприятий оценки и методов оценки может начинаться либо с SAR, стремясь сделать некоторые или все части его единиц работы более конкретными, либо с SFR, стремясь определить конкретные аспекты единиц работы, связанных с настоящим SFR.

При начале с SAR, руководство для процесса следующее.

a) Определить соответствующие единицы работы ISO/IEC 18045, из которых следует вывести, по меньшей мере, одно отдельное мероприятие оценкиили группы мероприятий оценки.

b) Для каждой рабочей единицы, из которой выводится мероприятие оценки:

1) определить новые мероприятия оценки с точки зрения конкретной работы, которая должна быть выполнена, и критериев оценки, в соответствии с описанием в 6.2 (включая, при необходимости, критерии прохождения/непрохождения, в соответствии с описанием в 6.2.8);

2) сгруппировать мероприятия оценки в метод оценки, если необходимо;

3) указать обоснование новых видов мероприятий оценки и метод оценки, по которому они группируются, в соответствии с описанием в 5.2.10 и 6.2.10.

***Пример*** - Обоснование может включать ссылку на действие разработчика, а также элементы контента и представления единиц работы, из которых они получены.

Руководство по началу работы с SFR будет следующим.

a) Определить соответствующие SFR.

b) Определить SAR (требования обеспечения безопасности) (из ISO/IEC 15408-3 или набора расширенных SAR, или оба), которые должны быть рассмотрены для настоящего конкретного SFR, и соответствующие единицы работы ISO/IEC 18045.

c) Определить новые мероприятия оценки с точки зрения конкретной работы, которая должна быть выполнена, и критериев оценки, в соответствии с описанием в 6.2 (включая, при необходимости, критерии прохождения/непрохождения, в соответствии с описанием в 6.2.8).

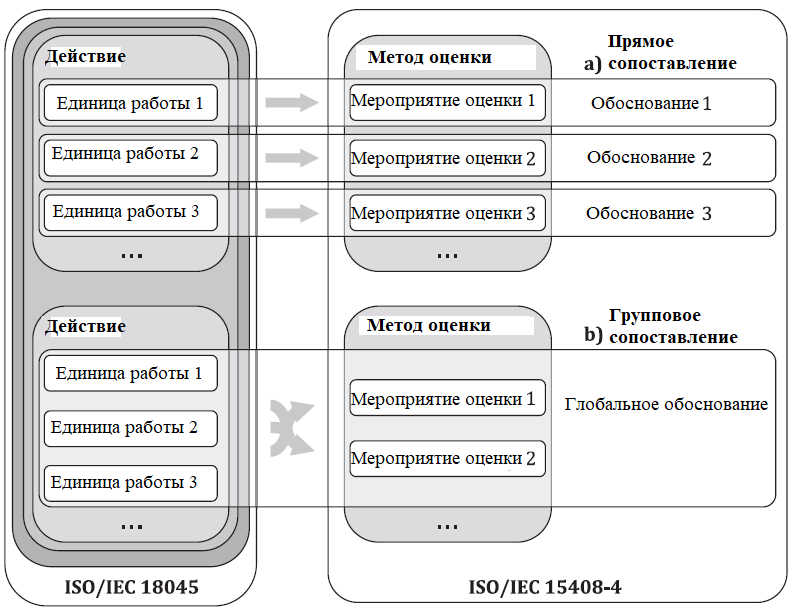
***Пример*** - Мероприятия оценки могут быть определены для проверки представления конкретного SFR в спецификации краткого содержания TOE (полученной из ASE), для проверки представления SFR в руководящей документации (полученной из AGD) и для проведения определенных тестов SFR (полученных из ATE).

d) Сопоставить затронутые единицы работы для требований обеспечения безопасности с новыми мероприятиями оценки.

e) Указать обоснование для новых мероприятий оценки и метода оценки, по которому они сгруппированы, в соответствии с описанием в 5.2.10 и 6.2.10.

Несмотря на то, что автор может выбрать, начинать ли с SAR или SFR, отмечается, что SAR в конечном итоге охватывают все SFR. Начинать с SFR, в соответствии с описанием выше, - это метод, который может быть полезен при уточнении деталей того, как SAR применяется к конкретному SFR, и который может быть полезен для представления SFR вместе с описанием их мероприятия оценки.

Не требуется иметь сопоставление 1:1 между единицами работы и новыми мероприятиями оценки, и фактическое соответствие документируется в обосновании (в соответствии с описанием в 5.2.10). Вывод может быть выполнен относительно отдельных единиц работы или групп единиц работы, и это изображено на рисунке 2. В случае а) рисунка 2 автор сопоставляет каждую единицу работы из ISO/IEC 18045 с соответствующим мероприятием оценки, тогда как в случае b) автор сопоставляет различное количество единиц работы и мероприятий оценки, при этом по-прежнему рассматривая все аспекты мероприятия (т. е. совокупность единиц работы).



**Рисунок 2 – Альтернативные подходы к сопоставлению ISO/IEC 18045 с выведенными мероприятиями оценки**

Возможны другие подходы в зависимости от контента конкретных единиц работы и мероприятий оценки: даже если существует одинаковое количество единиц работы и мероприятий оценки, простое сопоставление 1:1 иногда невозможно, и поэтому сопоставление на уровне действия может быть целесообразным. Некоторые более подробные ситуации сопоставления приведены в примерах ниже.

Примечание - Настоящие примеры предполагают, что описанные мероприятия оценки определяются сообществом, которое может судить о пригодности обоснования для полноты мероприятий оценки. Примеры касаются только формы и структуры сопоставлений, а не характера или принятия обоснования полноты.

***Примеры***

1 Для типа TOE, включающего как программное обеспечение, так и оборудование, могут быть определены дополнительные мероприятия оценки для работы с производственной средой и ее процессами. Рассматривая семейство ALC\_DVS, возможным подходом было бы принятие всех существующих единиц работы ALC\_DVS для среды разработки программного обеспечения и определение дополнительных мероприятий оценки для каждого из соответствующих аспектов оборудования и производства. Настоящие аспекты могут включать расширения обычной области применения ALC\_DVS на дополнительные элементы, такие как защита проектирования оборудования в среде разработки, безопасная передача программного обеспечения из среды разработки в производственную среду, безопасность производственного участка и защита произведенного продукта в ожидании поставки. Они также могут включать новые аспекты, связанные с объектами и процессами, которые возникают только в производственной среде, такие как:

- подтверждение того, что программа ПЗУ (прошивка), используемая на производственной линии, надежно получена из авторизованной версии, созданной в системе сборки прошивки;

- проверка управления конфигурацией тестовых программ для тестирования TOE на производственной линии;

- подтверждение того, что процессы отключения тестовых или отладочных интерфейсов на TOE работают правильно и надежно;

- проверка физической и логической безопасности систем управления ключами, используемых для внедрения ключей или сертификатов в TOE во время производства.

В настоящем примере исходное действие ALC\_DVS.1.1E сопоставляется с включением всех новых мероприятий оценки, но альтернативный подход будет заключаться в определении дополнительных мероприятий оценки для каждой отдельной единицы работы для ALC\_DVS.1E, определяя дополнительные действия для покрытия производственной среды для настоящей единицы работы.

2 Если анализ уязвимости AVA\_VAN.1 применяется к определенному типу TOE, где есть конкретная необходимость в достижении согласованности в используемых источниках уязвимости в общедоступном домене, то возможным подходом будет определение мероприятия оценки, которое охватывает единицу работы AVA\_VAN, занимающуюся поиском источников в общедоступном домене, путем указания конкретных источников, которые будут использоваться, возможно, вместе с конкретными поисками, которые будут выполнены, и критериями принятия решений для выбора результирующего списка потенциальных уязвимостей для анализа и тестирования. В настоящем примере исходная рабочая единица AVA\_VAN.1-3 сопоставляется с новым мероприятием оценки.

3 Для метода оценки, который будет использоваться с оборудованием, таким как интегральная схема, можно определить мероприятия оценки для проверки архитектуры схемы, определяя требуемые входные данные, которые предоставляют оценщику конкретные сведения об операциях и информации, доступной через интерфейсы схемы. Определение настоящих требуемых входных данных может затем прояснить, что соответствующие интерфейсы включают физическую поверхность схемы, ее исполняемые программные инструкции и ее интерфейсы связи.

Дополнительные мероприятия оценки в рамках метода оценки могут исследовать устойчивость схемы к физическому зондированию, чтобы предотвратить манипулирование или отключение функций TSF.

Для мероприятий по тестированию мероприятия оценки в рамках метода оценки могут определять требуемые входные данные, которые представляют конструкцию схемы в виде блок-схемы функций безопасности, пронизывающих подсистемы схемы. Затем блок-схема может использоваться оценщиком для создания тестовых случаев и подтверждения полного охвата теста схемы.

4 Для типа TOE, такого как сетевое устройство, которое предоставляет криптографически проверяемые обновления прошивки, мероприятия оценки могут предоставить конкретные сведения о том, как оценщик должен просматривать документацию по целям безопасности и руководству для подтверждения определенных конкретных характеристик, требуемых для процесса криптографического обновления.

Другие мероприятия оценки могут определять конкретные тестовые случаи, охватывающие верификацию текущей прошивки, доступность обновлений, получение обновлений, проверку источника обновлений с использованием криптографических подписей и использование определенных типов недействительных обновлений для тестирования функций принятия TOE.

**4.3 Использование глаголов в описании методов оценки и мероприятий оценки**

Если глагол определен в ISO/IEC 15408-1, то описание мероприятий оценки должно использовать настоящие глаголы только в соответствии с определениями. Альтернативные глаголы могут использоваться в методе оценки для использования в его мероприятиях оценки при условии, что альтернативные глаголы определены в методе оценки. Любое такое определение глагола должно четко указывать, в какой степени задействовано суждение оценщика (в отличие от простой проверки).

***Пример*** - Метод оценки, включающий автоматическую генерацию тестов для протокола, может определять глагол «покрыть», применяемый к перечисляемым типам в параметре протокола, что означает попытку всех определенных и неопределенных значений параметра в пределах доступной длины параметра. Затем мероприятия оценки могут быть записаны в таких формах, как «Оценщик должен охватить поле PaymentMode (СпособПлатежа)».

Глаголы действия оценщика, такие как check (проверять), exam (осмотреть), report (сообщать в отчете) и record (регистрировать), используются в настоящем документе со значениями, определенными в ISO/IEC 15408-1.

**4.4 Соглашения для описания методов оценки и мероприятий оценки**

В следующих пунктах описываются соглашения, используемые в ISO/IEC 15408-3 и ISO/IEC 18045, которые поддерживают последовательность в описании методов оценки и мероприятий оценки.

Всем глаголам единиц работы и подзадач предшествует вспомогательный глагол «должен» (shall) а также и глагол, и «должен» выделяются полужирным курсивом. Вспомогательный глагол «должен» используется только в том случае, если предоставленный текст является обязательным, и, следовательно, только в единицах работы и подзадачах. Единицы работы и подзадачи содержат обязательные мероприятия, которые оценщик должен выполнить для вынесения решений.

Текст руководства, сопровождающий единицы работы и подзадачи, приводит дополнительные пояснения о том, как применять единицы работы и подзадачи в оценке.

**5 Структура метода оценки**

**5.1 Обзор**

Метод оценки и его составляющие мероприятия оценки определяются для использования в определенном контексте оценки. Например, отдельные методы оценки могут быть определены для специальных технологических областей, которые могут варьироваться от определенных функций до определенных типов продуктов или даже, в крайних случаях, для конкретного продукта, когда продукт оценивается по уникальным характеристикам, но когда есть требование, чтобы продукт оценивался с использованием отдельно определенного метода, который поддерживает наглядность, повторяемость и воспроизводимость оценки.

***Пример*** - Контексты оценки, для которых могут быть определены отдельные методы оценки:

- определенные типы продуктов, такие как сетевые устройства, смарт-карты, биометрические устройства, мобильные устройства;

- определенные функции безопасности, повторно используемые для нескольких типов продуктов, такие как криптографические функции, криптографические протоколы, проверка цифровых сертификатов, схемы идентификации и аутентификации.

Метод оценки включает в себя набор отдельных мероприятий оценки с дополнительной информацией о том, как мероприятия оценки в совокупности достигают цели, связанной с определенным контекстом оценки.

Описание метода оценки включает:

a) идентификацию субъекта, который отвечает за определение и поддержание метода оценки;

b) предполагаемую область применения метода оценки, определяющую цель для получения мероприятий оценки в методе оценки, контекст оценки, в котором он должен применяться, и любые известные ограничения или аспекты, которые не должны охватываться методом оценки;

c) любые типы инструментов и/или компетенции оценщика, необходимые для выполнения мероприятия оценки, содержащихся в методе оценки;

d) любые требования к отчетности о результатах применения метода оценки;

e) идентификация каждой единицы работы в ISO/IEC 18045 (или эквивалент для расширенного SAR), которая рассматривается мероприятиями оценки в методе оценки;

f) идентификация любых расширенных SAR, из которых выводится метод оценки (если применимо);

g) любые дополнительные глаголы, используемые в описании мероприятий оценки вместо глаголов, определенных в ISO/IEC 15408-1.

Дальнейшее описание контента, включая определение того, какие элементы контента являются обязательными, и как элементы контента могут быть распределены между методом оценки и мероприятиями оценки, приведено в 5.2 и 6.2 и обобщено в Таблице 1. Если элемент контента является необязательным (например, определение конкретных компетенций оценщика или требуемых типов инструментов), то эта часть может быть просто пропущена из соответствующего определения: нет необходимости включать пустой раздел.

**5.2 Спецификация метода оценки**

5.2.1 Обзор

Метод оценки определяется относительно информации, указанной в 5.2.2-5.2.12. Для предоставления или представления настоящей информации не требуется никакого определенного формата, за исключением случаев, когда настоящее указано для отдельных элементов в 5.2.2-5.2.12. Целью указания описания метода оценки в 5.2.2-5.2.12 является обеспечение того, чтобы методы обеспечения, используемые при оценке, могли быть однозначно идентифицированы, и чтобы метод оценки использовался надлежащим образом (в контексте, для которого он был предназначен) и таким образом, чтобы поддерживать согласованные результаты оценки.

В целом, описание метода оценки может быть принято как включающее описания отдельных мероприятий оценки, которые он содержит. Это означает, что аспекты описания метода оценки могут быть выведены из описаний мероприятия оценки.

Рисунок 3 иллюстрирует контент, описанный в настоящем документе для метода оценки. Он не определяет обязательную структуру для описания метода оценки.



**Рисунок 3 – Контент метода оценки**

Контент, показанный на рисунке 3, более подробно описан в 5.2 и 6.2, а краткое описание обязательных и необязательных требований для указания методов оценки и мероприятия оценки приведено в таблице 1.

**Таблица 1 – Распределение контента между методом оценки (EM) и мероприятиями оценки (EA)**

|  |  |  |
| --- | --- | --- |
| Элемент контента | Метод оценки | Мероприятие оценки |
| Идентификатор | Обязательный | Обязательный |
| Ответственный субъект | Обязательный | N/A |
| Область | Обязательный | N/A |
| Зависимости | Необязательно на уровне EM или EA | |
| Требуемые входные данные | Обязательный на уровне EM или EA | |
| Требуемые типы инструментов | Необязательно на уровне EM или EA | |
| Требуемые компетенции оценщика | Необязательно на уровне EM или EA | |
| Требования к отчетности | Необязательно на уровне EM или EA | |
| Обоснование | Обязательный на уровне EM или EA | |
| Мероприятия оценки | Обязательный | N/A |
| Дополнительные определения глаголов | Необязательно | N/A |
| Цель | N/A | Обязательно |
| Мероприятие оценки связано с SFR, SAR и другими мероприятиями оценки | N/A | Необязательно |
| Стратегия оценки | N/A | Обязательно |
| Критерии прохождения / непрохождения | N/A | Необязательно |
| N/A: не применимо к методу оценки или мероприятию оценки. | | |

5.2.2 Идентификация методов оценки

Определение метода оценки должно включать уникальный идентификатор для того, чтобы однозначно идентифицировать набор мероприятий оценки, которые будут применяться в любой заданной оценке. Идентификатор должен быть назначен на уровне метода оценки (а не только на уровне мероприятий оценки, которые он содержит), отражая тот факт, что метод оценки предназначен для применения в целом и подлежит обоснованию и определенным целям и задачам на настоящем уровне. Если набор мероприятий оценки был сгруппирован в метод оценки, то он должен быть идентифицирован как тот же метод оценки, только когда используется полный набор мероприятий оценки в методе оценки с тем же обоснованием, которое содержится в исходном методе оценки. Если необходимо разделить метод оценки на более мелкие наборы мероприятий оценки, то для каждого мелкого набора должен быть определен отдельный метод оценки со своим собственным обоснованием.

***Примеры***

1 Уникальный идентификатор, выраженный названием и номером версии подтверждающего документа или PP, содержащего метод оценки.

2 Идентификатор, полученный от регистрирующего органа.

В соответствии с описанием в 5.2.10, метод оценки может быть перекрыт другим методом оценки (например, для использования в других PP или PP-модулях). В таком случае, если исходное обоснование метода оценки все еще остается в силе (в соответствии с описанием в 5.2.10), то должен использоваться идентификатор исходного метода оценки. Тем не менее, если обоснование изменяется как часть наложения, то должен использоваться отдельный идентификатор, определенный в соответствующем PP-модуле, PP-конфигурации или PP. Цель здесь заключается в том, чтобы обеспечить, что значительное изменение обоснования приведет к использованию другого идентификатора.

5.2.3 Субъект, ответственный за метод оценки

Определение метода оценки должно указывать субъект, который несет ответственность за определение и поддержание метода оценки.

***Пример -*** Примерами ответственных субъектов являются органы оценки, органы стандартизации, отраслевые рабочие группы или технические сообщества.

5.2.4 Область применения метода оценки

Определение метода оценки должно описывать его область применения, включая:

a) цель метода оценки в виде краткого заявления, обобщающего цели обеспечения, и заявление на высоком уровне о том, как они реализуются с помощью мероприятий оценки в рамках метода оценки;

b) контекст оценки, в котором предполагается применять метод оценки. Например, это может описывать тип TOE, такой как смарт-карта или сетевое устройство, или тип функции, такой как криптографические функции, использующие определенные алгоритмы и режимы, применяемые к определенным типам передачи и хранения данных;

c) любое известное ограничение метода оценки или аспекты, не предназначенные для охвата методом оценки.

Мероприятия оценки могут быть определены для применения конкретно к одному или нескольким SFR. Когда метод оценки включает такие конкретные для SFR мероприятия оценки, то подраздел области применения должен идентифицировать отдельные SFR, для которых определен метод оценки, и место, где определены SFR (например, ISO/IEC 15408-2 или расширенные SFR, определенные в PP). Для расширенных SFR, которые не определены в ISO/IEC 15408-2, идентификация местоположения особенно важна, поскольку одно и то же название SFR может использоваться в разных источниках для ссылки на SFR с различным контентом (если метод оценки не является конкретным для каких-либо SFR, то настоящий подраздел не требуется).

Аналогичным образом, мероприятия оценки могут быть определены для применения конкретно к одному или нескольким расширенным SAR (т. е. SAR, которые не определены в ISO/IEC 15408-3). Когда метод оценки включает такие мероприятия оценки, то подраздел области применения должен идентифицировать соответствующие расширенные SAR и место, где они определены (например, в PP). Как и в случае с расширенными SFR, идентификация местоположения особенно важна, поскольку одно и то же имя SAR может использоваться в разных источниках для ссылки на SAR с разным контентом (если метод оценки не применяется ни к одному расширенному SAR, то настоящий подраздел не требуется).

Примечание - Обоснование полноты метода оценки (см. 5.2.10) может дать дополнительную информацию, относящуюся к области применения метода оценки.

5.2.5 Зависимости

Определение метода оценки должно описывать любые зависимости от других методов оценки, мероприятий оценки или от некоторых общих действий в ISO/IEC 18045.

***Пример -*** Метод оценки, который опирается на информацию, полученную из какого-либо другого элемента действия разработчика в ISO/IEC 15408-3 или какого-либо действия в ISO/IEC 18045.

Зависимости могут быть идентифицированы либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки, содержащегося в методе оценки.

5.2.6 Требуемые входные данные от разработчика или других субъектов

Определение метода оценки должно идентифицировать любые входные данные разработчика, необходимые для выполнения мероприятий оценки. Это может быть выполнено либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки, включенной в метод оценки. Описание входных данных также может быть выполнено путем ссылки на те, которые определены для общего SAR, из которого выводятся мероприятия оценки, в соответствии с определением в ISO/IEC 15408-3 (или эквивалентном общем определении, если речь идет о расширенном SAR).

***Пример -*** Входные данные для метода оценки, работающего с шифрованием TOE, могут определять требование к описанию конкретных деталей иерархии ключей.

5.2.7 Требуемые типы инструментов

Если для мероприятий оценки требуются какие-либо типы инструментов, то они должны быть перечислены как часть определения метода оценки. Типы инструментов могут быть определены либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки, содержащегося в методе оценки.

5.2.8 Требуемые компетенции оценщика

Метод оценки может определять конкретные компетенции оценщика, необходимые для его мероприятий оценки (см. [3]). Если определены конкретные компетенции оценщика, то это может быть выполнено либо на уровне метода оценки, либо на уровне отдельных мероприятий оценки, содержащихся в методе оценки (или в комбинации того и другого).

5.2.9 Требования к отчетности

Описание метода оценки может включать описание требований к отчетности. Настоящее описание может быть дано на уровне метода оценки, на уровне отдельных мероприятий оценки или на обоих уровнях.

***Пример*** - Уровень метода оценки может задавать общие требования к отчетности, но с некоторыми мероприятиями оценки, также требующими включения конкретных наблюдений, обоснований или ответов на конкретные вопросы.

Любые заявленные требования к отчетности должны соответствовать требованиям к техническому отчету по оценке в ISO/IEC 18045 и любым другим стандартам, требуемым для проведения оценки.

***Пример*** - Примером другого стандарта, который может потребоваться для проведения оценки, является ISO/IEC 17025.

Требования к отчетности могут указывать отчетность, которая должна быть включена в технический отчет по оценке (ETR), в соответствии с описанием в   
ISO/IEC 18045, но также могут определять контент других результатов отчетов, которые должны быть созданы.

***Пример*** - Могут быть отдельные отчеты, определенные для публичного распространения и для более ограниченного распространения (например, разработчик, оценщик и орган оценки).

Если таким образом определено несколько отчетов, требования к отчетности для метода оценки (включая требования для отдельных мероприятий оценки) могут затем указывать аспекты, которые должны быть представлены в каждом из результатов отчетов.

Если метод оценки не требует отчетов или подробностей об отчете, отличных от тех, которые приведены в единицах работы, из которых он выведен (или если все дополнительные требования к отчетности указаны в мероприятиях оценки), то настоящий раздел не требуется.

5.2.10 Обоснование метода оценки

Необходимо привести обоснование, чтобы показать, что выведение мероприятия оценки в методе оценки из исходных единиц работы в ISO/IEC 18045 является целесообразным (в случае расширенного SAR вместо настоящей ссылки на единицы работы в ISO/IEC 18045 применяются к единицам работы в соответствующем определении методологии для расширенного SAR). Это может быть задано либо на уровне метода оценки, либо на уровне отдельных мероприятий оценки. Если мероприятия оценки, содержащиеся в методе оценки, не имеют индивидуальных обоснований согласно 6.2.10, то метод оценки должен включать обоснование для выведения мероприятий оценки из единиц работы в ISO/IEC 18045. Настоящее обоснование может содержать объяснение того, почему единицы работы были переработаны для области применения и глубины оценки конкретной технологии или типа TOE. Обоснование должно далее указывать, как мероприятия оценки, которые оно содержит, рассматривает все аспекты элементов действий в ISO/IEC 15408-3, к которым они применяются. Оно также должно обосновывать, что способ, которым рассматриваются элементы действий или единицы работы, является полным по отношению к контексту оценки, в котором предполагается применение метода оценки.

Если мероприятия оценки были получены из расширенного SAR, обоснование должно аргументировать, что мероприятия оценки соответствует описанию единиц работы для настоящего расширенного SAR (методология, определенная в ISO/IEC 18045 для оценки расширенных определений компонентов (семейства APE\_ECD, ACE\_ECD и ASE\_ECD в ISO/IEC 15408-3), требует, чтобы единицы работы были включены как часть определения расширенного SAR).

Обоснование может, если это уместно, идентифицировать конкретные предположения, которые выполнены для контекста оценки.

В случаях, когда объединяются различные источники требований, например, когда модули PP используются с базовым PP в конфигурации PP, мероприятия оценки из каждого источника (например, мероприятия оценки для каждого базового PP/модуля PP и мероприятия оценки для каждого компонента конфигурации PP) объединяются и применяются ко всему полученному TOE. В рамках комбинации метод оценки может быть перекрыт другим методом оценки, при условии обоснования любых изменений, внесенных наложением, таким образом, чтобы обоснование для результирующего метода оценки все еще было задано. Наложение существует, когда область применения более чем одной оценки из разных источников одинакова. Причина наложения заключается в том, чтобы сделать результирующий метод оценки более конкретным для TOE, когда две части используются вместе (в настоящем примере части являются базовым PP и PP-модулем, но могут возникнуть и другие случаи, например, когда пакет используется в PP, и более конкретный метод оценки, определенный для PP, накладывает более общий метод оценки, определенный для пакета).

Примечание - Несмотря на то, что автоматически мероприятия оценки применяются ко всему результирующему TOE, определение методов оценки или мероприятий оценки может определять ограничения для их применения. Например, мероприятия оценки могут быть определены специально для криптографических операций, которые используются в контексте определенных протоколов защищенного канала: настоящие мероприятия оценки затем не будут применяться к тем же криптографическим операциям при использовании в контексте защиты хранящихся данных.

***Пример*** - Метод оценки может быть определен в базовом PP для сетевого устройства TOE, включая мероприятия оценки для общих защищенных каналов, поддерживаемых TOE. PP-модуль может быть определен для определенных операций удаленного управления на сетевых устройствах, используя определенный тип защищенного канала (например, указав определенные операции или определенные протоколы). Мероприятия оценки для PP-модуля затем накладываются на метод оценки для базового PP, что означает, что мероприятия оценки PP-модуля заменяют базовые мероприятия оценки PP для определенных действий удаленного управления, охватываемых в PP-модуле (другие возможности безопасного канала по-прежнему будут подлежать мероприятиям оценки в методе оценки для базового PP).

Эффект наложения заключается в том, что одно или несколько из следующих изменений вносятся в базовый метод оценки:

a) базовое мероприятие оценки может быть удалено – как правило, это происходит, потому что мероприятие оценки больше не актуально (например, когда некоторые из доступных значений выбора в базовом PP SFR удаляются PP-модулем);

b) базовое мероприятие оценки может быть уточнено путем добавления более конкретных деталей (что может сделать мероприятие более строгим) - обычно это будет отражать дополнительные детали в контексте оценки (например, когда детали добавляются в контекст PP функциональным пакетом);

c) определяется дополнительное мероприятие оценки – как правило, это будет отражать дополнительный контекст оценки (например, из дополнительных деталей, добавленных в контекст PP функциональным пакетом, или дополнительного SAR, добавленного в PP-конфигурацию).

Возникает особый случай, когда базовое мероприятие оценки изменяется, чтобы соответствовать приращению связанного SAR – как правило, это будет отражать замену существующего SAR на иерархически более высокий SAR в PP-конфигурации. В таком случае, в зависимости от нового контента иерархического SAR, может быть комбинация добавления деталей, как в b), и добавления дополнительных мероприятий оценки, как в c).

Обоснование полученного метода оценки может основываться на допущениях, уже выполненных для наложения в обосновании исходного метода оценки (т. е. когда обоснование для наложения уже включено в определение исходного метода оценки), или же на более конкретном методе оценки (например, в PP-модуле) может включать отдельное обоснование, касающееся его влияния на исходный метод оценки (например, в базовом PP). Если наложенный метод оценки (например, PP-модуль) включает отдельное обоснование, это должно показать, что полученный метод оценки сохраняет соответствующие аспекты наложенного метода оценки, принимая во внимание контекст, в котором должны использоваться объединенные части. В случае PP, используемых в сочетании, применяется тот же принцип: либо исходный метод оценки описывает разрешенные изменения в соответствии с контекстом, в котором он применяется, либо полученный наложенный метод оценки рассматривает влияние на исходный метод оценки.

Обоснование для наложенных мероприятий оценки может быть отдельным разделом или может быть включено как часть обоснования гарантий или обоснования требований безопасности, в соответствии с описанием в ISO/IEC 15408-1.

5.2.11 Дополнительные определения глаголов

В соответствии с описанием в 4.3 выше, в спецификации мероприятий оценки могут использоваться альтернативные глаголы, отличные от определенных в ISO/IEC 15408-1, но любые такие альтернативные глаголы должны быть определены как часть метода оценки, который содержит мероприятия оценки, и должны четко указывать, в какой степени задействовано суждение оценщика (в отличие от простой проверки).

5.2.12 Набор мероприятий оценки

Мероприятия оценки, содержащиеся в методе оценки, должны быть определены с использованием структуры, определенной в разделе 6.

**6 Структура мероприятий оценки**

**6.1 Обзор**

На уровне отдельного мероприятия оценки акцент спецификации делается на обеспечении того, чтобы мероприятие оценки имело четкую цель, четкие критерии прохождения/не прохождения (при необходимости) и чтобы были определены любые зависимости от других мероприятий оценки. Это предназначено для того, чтобы помочь в понимании оценки и, следовательно, последовательного применения мероприятия в каждой оценке.

В соответствии с указанием в 5.2 и обобщением в таблице 1, некоторые детали, которые должны быть указаны для мероприятий оценки, могут быть включены либо на уровне метода оценки, либо на уровне отдельных мероприятий оценки.

Предполагается, что контент мероприятий оценки может быть предоставлен в различных форматах, включая формат, который состоит, например, только из краткого повествовательного описания теста или аналитической деятельности (например, для подтверждения того, что документация пользователя приводит описание безопасного создания учетных данных для использования с протоколом). Кроме того, некоторые мероприятия оценки могут быть сгруппированы вместе, а элементы контента описаны для группы в целом, а не повторяются для каждого отдельного мероприятия оценки. Каждый элемент контента мероприятия оценки описан более подробно в 6.2.1 – 6.2.10, а сводка обязательного и необязательного статуса каждого элемента обобщена в таблице 1.

**6.2 Спецификация мероприятия оценки**

6.2.1 Уникальная идентификация мероприятия оценки

Мероприятия оценки должны быть уникально идентифицированы в исходном документе. Сам исходный документ должен быть уникально идентифицирован. Если мероприятия оценки были сгруппированы в метод оценки, то отдельные идентификаторы мероприятий оценки определяются в дополнение к идентификатору для метода оценки в целом (см. 5.2.2).

6.2.2 Цель мероприятия оценки

Цель выполнения мероприятия оценки должна быть указана. Она может быть указана со ссылкой на SFR и SAR, в соответствии с обсуждением в 6.2.3, и на критерии прохождения/непрохождения в 6.2.8. Тем не менее, также важно, чтобы указание цели помогало оценщику понимать гибкость и ограничения при изменении мероприятия оценки для соответствия определенному TOE.

6.2.3 Связи мероприятия оценки с SFR, SAR и другими мероприятиями оценки

Если мероприятие оценки связано с конкретными SFR (возможно, с конкретными примерами SFR в другом документе, таком как пакет, PP или PP-Module), то это должно быть указано как часть определения мероприятия оценки.

***Пример*** - Мероприятие оценки может быть связано с SFR, указанным в конкретном PP с частичным выполнением задания для ограничения приемлемых значений, которые могут использоваться в соответствующем ST.

Аналогичным образом должна быть указана связь с конкретными SAR [это может быть достигнуто посредством обоснования вывода из единиц работы исходного   
SAR (см. 5.2.10 и 6.2.10), если нет дополнительной информации, которая должна быть предоставлена об этой связи].

Если мероприятие оценки зависит от выполнения другого мероприятия оценки, то зависимость и другое мероприятие оценки должны быть идентифицированы как часть определения зависимого мероприятия оценки (зависимости могут быть идентифицированы либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки).

6.2.4 Требуемые входные данные от разработчика или других субъектов

В соответствии с указанием в 5.2.6, могут быть указаны дополнительные сведения относительно требуемого формата и контента входных данных для мероприятия оценки. Настоящие дополнительные сведения обычно используются для поддержки точной спецификации мероприятия оценки и ее критериев прохождения/непрохождения (это может быть выполнено либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки).

Если мероприятия оценки не требует других входных данных, кроме тех, которые определены в единице работы, из которой она получена, то настоящий раздел не требуется.

6.2.5 Требуемые типы инструментов

Если для выполнения мероприятия оценки требуются какие-либо типы инструментов для выполнения мероприятия, то настоящие типы инструментов должны быть определены как часть определения мероприятия оценки. Определение типа инструмента должно включать достаточно подробностей, чтобы инструмент настоящего типа можно было получить или воссоздать, чтобы мероприятие оценки могло быть последовательно выполнено в отношении описания мероприятия оценки и ее критериев прохождения/непрохождения (это может быть выполнено либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки).

Если мероприятия оценки не требует определенных типов инструментов, отличных от тех, которые заданы или подразумеваются в единице работы, из которой она получена, то настоящий раздел не требуется.

6.2.6 Требуемые компетенции оценщика

В соответствии с указанием в 5.2.8, метод оценки может определять конкретные компетенции оценщика, необходимые для его мероприятия оценки (см. [3]). Если определены конкретные компетенции оценщика, то это может быть выполнено либо на уровне метода оценки, либо на уровне отдельных мероприятий оценки, содержащихся в методе оценки (или комбинации того и другого).

6.2.7 Стратегия оценки

Настоящий раздел мероприятия оценки должен содержать руководство и подробную информацию о том, как выполнять деятельность. Он включает в себя, в зависимости от контента мероприятия оценки, следующее:

a) как оценить входные данные разработчика или других субъектов на предмет полноты в отношении мероприятия оценки;

b) как использовать любые требуемые типы инструментов (потенциально включая руководство по калибровке или настройке инструментов);

c) пошаговое руководство по выполнению действия.

Предоставление некоторого пространства для адаптации, конкретной для технологий, важно для большинства мероприятий оценки. Нахождение правильного баланса между точной спецификацией стратегии оценки и допустимым пространством для такой адаптации важно для обеспечения объективных и воспроизводимых результатов, с одной стороны, и значимых результатов, с другой стороны. Когда у разработчика больше гибкости в отношении того, как реализовать функциональное требование(я), то определение мероприятия оценки должно предоставлять больше места для адаптации оценки к различным потенциальным реализациям. В настоящих случаях стратегия оценки должна предоставлять общее руководство о том, как выполнять уточнение и адаптацию, конкретные для TOE, а не указывать каждую деталь действий, которые должен выполнить оценщик. В целом, отклонения/уточнения от мероприятия оценки (т. е. пропуск моментов, требуемых в оценочном действии) не допускаются.

Стратегия оценки может состоять из нескольких этапов, которые должен выполнить оценщик, и в этом случае настоящие этапы должны быть указаны с ожидаемым результатом каждого этапа. Некоторые этапы могут зависеть от результата предыдущих этапов, и в настоящем случае стратегия оценки должна также определять, что оценщику необходимо сделать, если один из этапов не дает ожидаемого результата. Примерами таких случаев являются возврат к предыдущему этапу с некоторыми измененными входными данными, выполнение мероприятия оценки с указанием того, что документировать в качестве результата деятельности, или продолжение с другим этапом.

В зависимости от потребностей контекста оценки и характера самого мероприятия оценки стратегия оценки может быть краткой и может составлять часть общего описания мероприятия оценки (например, описание того, как проводить конкретное испытание или анализ).

6.2.8 Критерии прохождения/непрохождения

Настоящий раздел мероприятия оценки позволяет определить критерии, которые оценщик использует для определения того, продемонстрировало ли мероприятие оценки, что TOE соответствует надлежащим требованиям или что он не соответствует надлежащим требованиям. В некоторых случаях может быть целесообразно положиться на описание исходной единицы работы, из которой выведено мероприятие оценки, но в других случаях автор мероприятия оценки может решить, что необходимо или полезно указать более конкретные критерии. В конечном счете, критерии прохождения/непрохождения касаются определения того, была ли достигнута цель, заявленная для мероприятия оценки (см. 6.2.2). Если мероприятие оценки требует отдельных критериев прохождения/непрохождения, то настоящие критерии должны приблизить максимальную согласованность результатов от выполнения мероприятия оценки в разных оценках. Четкое изложение конкретных критериев таким образом сводит к минимуму вероятность того, что другой оценщик придет к другому выводу для мероприятия оценки, учитывая те же доказательства. В целом, поэтому критерии прохождения/непрохождения должны быть максимально конкретными.

Способы достижения конкретных критериев прохождения/непрохождения для анализа документов включают выражение критериев с точки зрения наличия или отсутствия определенных характеристик, например, наличия подробной конфигурации стека связи или набора триггеров сбоев среды выполнения, и с точки зрения ответов «да/нет» на определенные «закрытые» вопросы (возможно, подкрепленные ответами, полученными на другие «открытые» вопросы).

Способами достижения конкретных критериев прохождения/непрохождения тестов было бы выражение критериев в терминах конкретного видимого результата, например, наблюдение за успешной связью по каналу или получение сообщения об ошибке, указывающего на то, что настройка канала не удалась, или наблюдение за доступом/настройкой памяти. Такая фраза, как «TOE удаляет данные», как правило, было бы плохим выбором в качестве критерия прохождения/непрохождения, поскольку неясно, как это удаление должно определяться оценщиком: лучшим выбором было бы «TOE возвращает ошибку «файл не найден»» или «оценщик использует <именованный вызов интерфейса> и подтверждает, что файл отсутствует в возвращенном списке файлов». Другой метод выражения конкретных критериев прохождения/непрохождения для мероприятия оценки был бы относительно определения соответствия конкретным положениям определенного стандарта или относительно сравнения с эталонной моделью или набором примеров, таких как модель потенциала атаки в ISO/IEC 18045 или конкретная модель потенциала атаки, определенная для некоторых типов ИТ-продуктов.

Тем не менее, также известно, что критерии, как правило, должны учитывать различия в деталях реализации между различными TOE. Поэтому критерии прохождения/непрохождения также могут быть описаны относительно цели, определенной для мероприятия оценки (см. 6.2.2).

Если мероприятие оценки не требует результатов прохождения/непрохождения, отличных от тех, которые указаны в единице работы, из которой она выведена, то настоящий раздел не требуется.

6.2.9 Требования к отчетности

В соответствии с указанием в 5.2.9, для мероприятия оценки могут быть указаны особые требования к отчетности (в ETR и, возможно, в других выходных данных). Требования могут быть указаны на уровне метода оценки или на уровне отдельных мероприятий оценки. На настоящем уровне определенные требования к отчетности, как правило, направлены на поддержку наглядности и воспроизводимости суждения о прохождении/непрохождении путем документирования ответов на конкретные вопросы, обоснования выводов или предоставления четкого описания результата конкретного теста. В частности, если ожидается, что критерии прохождения/непрохождения потребуют суждений оценщика, то требования к отчетности должны включать запись конкретных факторов, определенных для участия в принятии суждения и достижении заключения о прохождении/непрохождении.

Если мероприятие оценки не требует отчетов или подробностей отчета, отличных от тех, которые указаны в единице работы, из которой оно выведено, то настоящий раздел не требуется.

6.2.10 Обоснование для мероприятия оценки

Мероприятие оценки должно включать обоснование вывода из одной или нескольких единиц работы в ISO/IEC 18045 (или эквивалентного определения единицы работы для расширенного SAR). Настоящее обоснование может содержать объяснение, почему единицы работы должны быть переработаны для области применения и глубины оценки конкретной технологии или типа TOE. Сочетание обоснования на уровнях метода оценки (см. 5.2.10) и мероприятия оценки должно обосновывать, что метод оценки рассматривает все аспекты элементов действий в ISO/IEC 15408-3, к которым он применяется. Кроме того, объединенное обоснование должно описывать, как вывод из исходных элементов действий или единиц работы обеспечивает полноту мероприятия оценки по отношению к контексту оценки, в котором предполагается применение мероприятия оценки.

Примечание – Обоснование может определять и обосновывать, что некоторые аспекты неприменимы для конкретного контекста оценки.

Если мероприятие оценки определяет критерии прохождения/непрохождения, которые отличаются от единиц работы, из которых оно выведено, то обоснование должно содержать причины осуществимости и эффективности новых критериев.

Обоснование может, если это уместно, определять конкретные предположения, которые выполнены для контекста оценки.

Обоснование может быть дано либо на уровне метода оценки, либо на уровне отдельного мероприятия оценки.

**Библиография**

[1] ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 5. Pre-defined packages of security requirements (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 5. Заранее определенные пакеты требований безопасности).

[2] ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories (Общие требования к компетентности испытательных и калибровочных лабораторий).

[3] ISO/IEC 19896-3 IT security techniques. Competence requirements for information security testers and evaluators. Part 3. Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators (Информационная технология. Методы и средства обеспечения безопасности. Требования к компетенции тестировщиков и оценщиков защищенности информации. Часть 3. Требования к знаниям, квалификации и эффективности оценщиков, использующих ISO/IEC 15408).

**Приложение В.А**

*(информационное)*

**Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств**

**Таблица В.А.1 – Сведения о соответствии стандартов, ссылочным международным, региональным стандартам, стандартам иностранных государств другого года издания**

|  |  |  |  |
| --- | --- | --- | --- |
| Обозначение и наименование ссылочного международного, регионального стандартов, стандартов иностранного государств документа | Обозначение и наименование международного, регионального стандартов, стандартов иностранного государств | Степень соответствия | Обозначение и наименование национального стандарта, межгосударственного стандарта |
| ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 1. Introduction and general model (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 1. Введение и общая модель) | ISO/IEC 15408-1:2009 Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель) | IDT | СТ РК ISO/IEC 15408-1-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» |
| ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 2. Security functional components (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 2. Функциональные компоненты безопасности) | ISO/IEC 15408-2:2008 Information technology. Security techniques. Evaluation criteria for IT security. Part 2. Security functional components (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности) | IDT | СТ РК ISO/IEC 15408-2-2017 Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности |

*Продолжение таблицы В.А.1*

|  |  |  |  |
| --- | --- | --- | --- |
| Обозначение и наименование ссылочного международного, регионального стандартов, стандартов иностранного государств документа | Обозначение и наименование международного, регионального стандартов, стандартов иностранного государств | Степень соответствия | Обозначение и наименование национального стандарта, межгосударственного стандарта |
| ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 3. Security assurance components (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Часть 3. Компоненты доверия к безопасности) | ISO/IEC 15408-3:2008 Information technology. Security techniques. Evaluation criteria for IT security. Part 3. Security assurance components (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности) | IDT | СТ РК ISO/IEC 15408-3-2017 Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты |
| ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection. Methodology for IT security evaluation (Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки ИТ-безопасности. Методология оценки безопасности информационных технологий) | ISO/IEC 18045:2008 Information technology. Security techniques. Methodology for IT security evaluation (Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий) | IDT | СТ РК ИСО/МЭК 18045-2009 Технологии информационные. Методы защиты. Методология оценки защиты информационных технологий |

|  |
| --- |
| **МКС 35.030 (IDT)** |
| **Ключевые слова:** информационная безопасность, кибербезопасность, защита конфиденциальности, критерии оценки безопасности, структура, методы оценки, спецификация |

|  |
| --- |
| **МКС 35.030 (IDT)** |
| **Ключевые слова:** информационная безопасность, кибербезопасность, защита конфиденциальности, критерии оценки безопасности, структура, методы оценки, спецификация |

**РАЗРАБОТЧИК**

РГП на ПХВ «Казахстанский институт стандартизации и метрологии» Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан

**Заместитель**

**Генерального директора Е. Амирханова**

**Руководитель**

**Департамента разработки стандартов А. Сопбеков**

**Ведущий специалист**

**Департамента разработки стандартов Ж. Туяков**