*Проект*

Изображение государственного Герба Республики Казахстан

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

**Критерии оценки безопасности IT**

**Часть 5**

**ЗАРАНЕЕ ОПРЕДЕЛЕННЫЕ ПАКЕТЫ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ**

**СТ РК** **ISO/IEC 15408-4**

*(ISO/IEC 15408-5:2022 Information security, cybersecurity and privacy protection. Evaluation criteria for IT security. Part 5. Pre-defined packages of security requirements, 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 15408-5:2022 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 безопасности IT. Часть 5. Заранее определенные пакеты требований безопасности)

Международный стандарт ISO/IEC 15408-5:2022 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 | 2 |
| 3 | Термины и определения | 2 |
| 4 | Уровни гарантии оценки | 2 |
| 4.1 | Имя семейства | 2 |
| 4.2 | Обзор уровня гарантии оценки | 2 |
| 4.3 | Цели уровня гарантии оценки | 4 |
| 4.4 | Уровни гарантии оценки | 5 |
| 5 | Составные пакеты гарантий (CAP) | 15 |
| 5.1 | Имя семейства | 15 |
| 5.2 | Обзор составного пакета гарантий (CAP) | 15 |
| 5.3 | Цели составного пакета гарантий (CAP) | 16 |
| 5.4 | Пакеты в семействе CAP | 18 |
| 6 | Пакет композитного (смешанного) продукта | 21 |
| 6.1 | Имя пакета | 21 |
| 6.2 | Тип пакета | 22 |
| 6.3 | Обзор пакета | 22 |
| 6.4 | Цели | 22 |
| 6.5 | Компоненты гарантии безопасности | 22 |
| 7 | Гарантии профиля защиты | 22 |
| 7.1 | Имя семейства | 22 |
| 7.2 | Обзор семейства PPA | 23 |
| 7.3 | Цели семейства PPA | 23 |
| 7.4 | Пакеты PPA | 23 |
| 8 | Гарантии задания по безопасности | 24 |
| 8.1 | Семейство имя | 24 |
| 8.2 | Обзор семейства STA | 24 |
| 8.3 | Цели семейства STA | 25 |
| 8.4 | Пакеты STA | 25 |
| Приложение В.А *(информационное)* Сведения о соответствии стандартов ссылочным международным, региональным стандартам, стандартам иностранных государств | | 27 |

**Введение**

В настоящем стандарте представлены заранее определенные пакеты требований безопасности. Такие требования безопасности могут быть полезны для заинтересованных сторон, поскольку они стремятся к согласованности оценок. Пакеты требований безопасности также могут помочь сократить усилия по разработке профилей защиты (PP) и заданий по безопасности (ST).

ISO/IEC 15408-1 определяет термин «пакет» и описывает основные концепции.

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 гарантии безопасности соглашение касается конкретных глаголов, связанных с оценкой.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Информационная безопасность, кибербезопасность и защита конфиденциальности**

**Критерии оценки безопасности IT**

**Часть 5**

**ЗАРАНЕЕ ОПРЕДЕЛЕННЫЕ ПАКЕТЫ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ**

**Дата введения \_\_\_\_ -\_\_-\_\_**

**1 Область применения**

Настоящий стандарт устанавливает пакеты гарантий безопасности и функциональных требований безопасности, которые были определены как полезные для поддержки общего использования заинтересованными сторонами.

***Пример*** - Примеры предоставленных пакетов включают уровни гарантий оценки (EAL) и пакеты гарантий состава (CAP).

В настоящем стандарте представлены:

- семейство пакетов *уровня гарантий оценки* (*EAL*), которые определяют заранее определенные наборы компонентов гарантий безопасности, которые могут быть указаны в PP и ST и которые определяют соответствующие гарантии безопасности, которые должны быть предоставлены во время оценки задания по оценке (TOE);

- семейство пакетов *гарантий состава* (*CAP*), которые определяют наборы компонентов гарантий безопасности, используемых для указания соответствующих гарантий безопасности, которые должны быть предоставлены во время оценки составных TOE;

- пакет *составного продукта* (*COMP*), который определяет набор компонентов гарантий безопасности, используемых для указания соответствующих гарантий безопасности, которые должны быть предоставлены во время оценки составного продукта TOE;

- семейство пакетов *гарантии профиля защиты* (*PPA*), которые указывают наборы компонентов гарантий безопасности, используемых для указания соответствующих гарантий безопасности, которые должны быть предоставлены во время оценки профиля защиты;

- семейство пакетов *гарантии задания по безопасности* (STA), которые определяют наборы компонентов гарантии безопасности, используемых для указания соответствующих гарантий безопасности, которые должны быть предоставлены во время оценки задания по безопасности.

Пользователями настоящего стандарта могут быть потребители, разработчики и оценщики безопасных IT-продуктов.

***Проект 1 редакция***

**2 Нормативные ссылки**

Для применения настоящего стандарта необходимы, следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, 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 15408-3:2022 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).

**3 Термины и определения**

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

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 Уровни гарантии оценки**

**4.1 Имя семейства**

Имя настоящего семейства пакетов - уровни гарантии оценки (EAL).

**4.2 Обзор уровней гарантии оценки**

4.2.1 Общие положения

EAL предоставляют возрастающую шкалу, которая уравновешивает уровень полученной гарантии с затратами и осуществимостью получения этой степени гарантии. Подход ISO/IEC 15408-1 определяет отдельные концепции гарантии в TOE в конце оценки и поддержания этой гарантии во время операционного использования TOE.

Примечание - Не все семейства и компоненты, приведенные в ISO/IEC 15408-3, включены в EAL. Это не означает, что они не предоставляют значимых и заданных гарантий. Вместо этого ожидается, что настоящие семейства и компоненты могут рассматриваться для расширения EAL в тех профилях защиты (PP) и заданиях по безопасности (ST), для которых они обеспечивают полезность. Кроме того, некоторые классы, найденные в ISO/IEC 15408-3, не имеют отношения к EAL. Примерами таких классов являются классы APE и ACO.

Для каждого EAL был выбран набор компонентов гарантии.

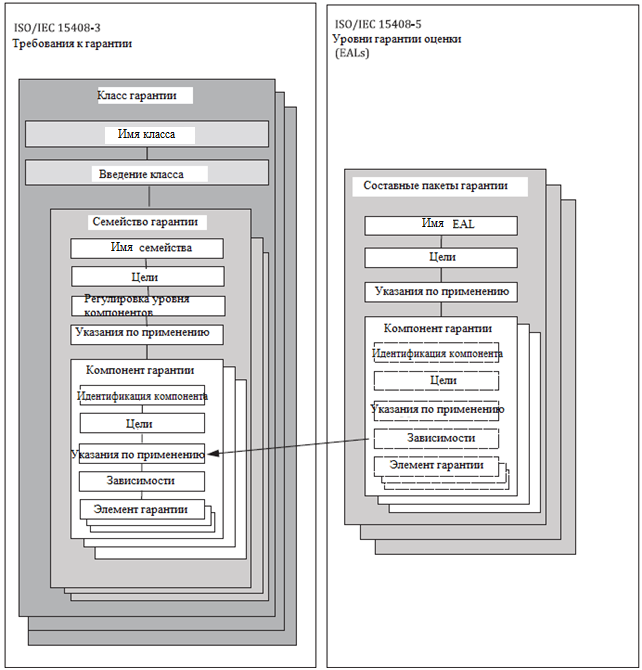
Более высокий уровень гарантии, чем тот, который предоставляется заданным EAL, может быть достигнут путем:

a) включения дополнительных компонентов гарантии из других семейств гарантии; или

b) замены компонента гарантии на компонент гарантии более высокого уровня из того же семейства гарантии.

4.2.2 Связь между гарантиями и уровнями гарантии

На рисунке 1 показана связь между требованиями гарантии безопасности (SAR), содержащимися в ISO/IEC 15408-3, и уровнями гарантии, определенными в настоящем стандарте. Несмотря на то, что компоненты гарантии далее разлагаются на элементы гарантии, элементы гарантии не могут быть индивидуально указаны уровнями гарантии.



Примечание - Стрелка на рисунке представляет собой ссылку из EAL на компонент гарантии в пределах класса, где он определен.

**Рисунок 1 – Связь гарантии и уровня гарантии**

Таблица 1 представляет собой краткое содержание EAL. Столбцы представляют иерархически упорядоченный набор EAL, а строки представляют семейства гарантии. Каждое число в результирующей матрице идентифицирует конкретный компонент гарантии, где это применимо.

Элементы, отмеченные серым цветом, неприменимы в спецификации EAL. Тем не менее, их можно использовать для дополнения пакета EAL.

Примечание - Несмотря на то, что семейства ALC\_FLR и ALC\_TDA не показаны в таблице 1, они часто используются в качестве дополнения к EAL.

**Таблица 1 - Краткое содержание уровней гарантии оценки**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Класс гарантии | Семейство гарантии | Компоненты гарантии по уровню гарантии оценки | | | | | | |
| EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Разработка | ADV\_ARC |  | **1** | 1 | 1 | 1 | 1 | 1 |
| ADV\_FSP | **1** | **2** | **3** | **4** | **5** | 5 | **6** |
| ADV\_IMP |  |  |  | **1** | 1 | **2** | 2 |
| ADV\_INT |  |  |  |  | **2** | **3** | 3 |
| ADV\_SPM |  |  |  |  |  | **1** | 1 |
| ADV\_TDS |  | **1** | **2** | **3** | **4** | **5** | **6** |
| Руководящие документы | AGD\_OPE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| AGD\_PRE | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Поддержка жизненного цикла | ALC\_CMC | **1** | **2** | **3** | **4** | 4 | **5** | 5 |
| ALC\_CMS | **1** | **2** | **3** | **4** | **5** | 5 | 5 |
| ALC\_DEL |  | **1** | 1 | 1 | 1 | 1 | 1 |
| ALC\_DVS |  |  | **1** | 1 | 1 | **2** | 2 |
| ALC\_LCD |  |  | **1** | 1 | 1 | 1 | **2** |
| ALC\_TAT |  |  |  | **1** | **2** | **3** | 3 |
| Оценка ST | ASE\_CCL | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| ASE\_ECD | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| ASE\_INT | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| ASE\_OBJ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| ASE\_REQ | **1** | **2** | 2 | 2 | 2 | 2 | 2 |
| ASE\_SPD |  | **1** | 1 | 1 | 1 | 1 | 1 |
| ASE\_TSS | **1** | 1 | 1 | 1 | 1 | 1 | 1 |
| Тесты | ATE\_COV |  | **1** | **2** | 2 | 2 | **3** | 3 |
| ATE\_DPT |  |  | **1** | 1 | **3** | 3 | **4** |
| ATE\_FUN |  | **1** | 1 | 1 | 1 | **2** | 2 |
| ATE\_IND | **1** | **2** | 2 | 2 | 2 | 2 | **3** |
| Оценка уязвимости | AVA\_VAN | **1** | **2** | 2 | **3** | **4** | **5** | 5 |

**4.3 Цели уровня гарантии оценки**

В соответствии с 4.4, в настоящем стандарте определены семь иерархически упорядоченных уровней гарантии оценки для рейтинга гарантий TOE. Они иерархически упорядочены, поскольку каждый EAL представляет большую гарантию, чем все более низкие EAL. Повышение гарантии от одного EAL до другого EAL достигается путем замены иерархически более высокого компонента гарантии из того же семейства гарантий (т. е. увеличения строгости (точности), области применения и/или глубины) и добавления компонентов гарантии из других семейств гарантий (т. е. добавления новых требований).

Настоящие EAL состоят из соответствующей комбинации компонентов гарантии, в соответствии с описанием в ISO/IEC 15408-3. Точнее, каждый EAL включает не более одного компонента из каждого семейства гарантий, и рассматриваются все зависимости гарантий каждого компонента.

Понятие «расширение» позволяет добавлять компоненты гарантии (из семейств гарантии, еще не включенных в EAL) или заменять компоненты гарантии (другим иерархически более высоким компонентом гарантии в том же семействе гарантии) в EAL. Из структур гарантии, определенных в ISO/IEC 15408-1, только EAL могут быть расширены. Понятие «EAL минус составной компонент гарантии» не признается в ISO/IEC 15408-1 как допустимое утверждение. Расширение влечет за собой обязательство со стороны заявителя обосновать полезность и добавленную ценность добавленного компонента гарантии в EAL. EAL также может быть расширен повышенными требованиями к гарантии.

Примечание - EAL не может быть расширен, если он включен в ST, который заявляет о точном соответствии PP.

**4.4 Уровни оценки гарантии**

4.4.1 Общие положения

В настоящем подразделе приводятся определения EAL, подчеркивающие различия между конкретными требованиями и прозаическими характеристиками настоящих требований с использованием полужирного шрифта.

4.4.2 Уровень гарантии оценки 1 (EAL1). Функционально протестирован

4.4.2.1 Имя пакета

Имя пакета - это уровень гарантии оценки 1 (EAL1), функционально протестирован.

4.4.2.2 Тип пакета

Это пакет гарантии.

4.4.2.3 Обзор пакета

EAL1 применяется, когда требуется некоторая уверенность в правильной работе, но угрозы безопасности не рассматриваются как серьезные. Он имеет ценность, когда требуется независимая гарантия для поддержки утверждения о том, что была проявлена должная осторожность в отношении защиты персональной или аналогичной информации.

EAL1 требует только ограниченного ST. Достаточно просто указать требуемые функциональные требования безопасности (SFR) для TOE, а не выводить их из угроз, политик безопасности организации (OSP) и предположений через цели безопасности.

EAL1 предоставляет оценку TOE, предоставленную заказчику, включая независимое тестирование по спецификации и проверку предоставленной руководящей документации. Предполагается, что оценка EAL1 может быть успешно проведена без помощи разработчика TOE и с минимальными издержками.

Оценка на настоящем уровне предоставляет доказательство того, что TOE функционирует в соответствии с документацией.

4.4.2.4 Цели пакета

EAL1 предоставляет базовый уровень гарантии с помощью ограниченного ST и анализа SFR в настоящем ST с использованием функциональной и интерфейсной спецификации и руководящей документации для понимания режима безопасности.

Анализ поддерживается поиском потенциальных уязвимостей в общедоступных источниках и независимым тестированием (функциональным и внедрением) функциональности безопасности (TSF) TOE.

EAL1 также предоставляет гарантию посредством уникальной идентификации TOE и соответствующих документах оценки.

Настоящий EAL предоставляет значительное увеличение гарантий по сравнению с неоцененными IТ.

4.4.2.5 Компоненты гарантий

В таблице 2 приведены компоненты гарантий, включенные в EAL 1.

**Таблица 2 - EAL1**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_FSP.1 Базовая функциональная спецификация |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.1 Маркировка TOE |
| ALC\_CMS.1 Охват TOE CM |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.1 Цели безопасности для операционной среды |
| ASE\_REQ.1 Установленные требования безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |
| ATE: Тесты | ATE\_IND.1 Независимое тестирование. Соответствие |
| AVA: Оценка уязвимости | AVA\_VAN.1 Анализ степени уязвимости |

4.4.3 Уровень гарантии оценки 2 (EAL2). Структурно протестирован

4.4.3.1 Имя пакета

Имя пакета - уровень гарантии оценки 2 (EAL2). Структурно протестирован.

4.4.3.2 Тип пакета

Это пакет гарантии.

4.4.3.3 Обзор пакета

EAL2 требует сотрудничества разработчика с точки зрения предоставления информации о проекте и результатов тестирования, но не должен требовать от разработчика больших усилий, чем это согласуется с надлежащей коммерческой практикой. Таким образом, он не должен требовать существенного увеличения затрат или времени.

Поэтому EAL2 применим в тех обстоятельствах, когда разработчикам или пользователям требуется низкий или средний уровень независимо гарантированной безопасности при отсутствии готовой доступности полной записи разработки. Такая ситуация может возникнуть при обеспечении безопасности устаревших систем или когда доступ к разработчику может быть ограничен.

4.4.3.4 Цели

EAL2 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и интерфейсную спецификацию, руководящую документацию и базовое описание архитектуры TOE, чтобы понять режим безопасности.

Анализ поддерживается независимым тестированием TSF, доказательством тестирования разработчика на основе функциональной спецификации, выборочным независимым подтверждением результатов тестирования разработчика и анализом уязвимостей (на основе функциональной спецификации, проекта TOE, описания архитектуры безопасности и предоставленных руководящих доказательств), демонстрирующим устойчивость к внедрению злоумышленников с базовым потенциалом нападения.

EAL2 также предоставляет гарантию с помощью использования системы управления конфигурацией и доказательством процедур безопасной поставки.

Настоящий EAL представляет собой значительное увеличение гарантии по сравнению с EAL1, требуя тестирования разработчика, анализа уязвимостей (в дополнение к поиску в открытом доступе) и независимого тестирования на основе более подробных спецификаций TOE.

4.4.3.5 Компоненты гарантии

В таблице 3 приведены компоненты гарантии, включенные в EAL 2.

**Таблица 3 - EAL2**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры безопасности |
| ADV\_FSP.2 Функциональные спецификации по соблюдению безопасности |
| ADVTDS.1 Базовое проектное решение |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.2 Использование системы CM |
| ALC\_CMS.2 Части охвата TOE CM |
| ALC\_DEL.1 Процедуры поставки |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Выведенные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |
| ATE: Испытания | ATE\_COV.1 Свидетельство об охвате |
| ATE\_FUN.1 Функциональное тестирование |
| ATE\_IND.2 Независимое тестирование. Образец |
| AVA: Оценка уязвимости assessment | AVA\_VAN.2 Анализ уязвимости |

4.4.4 Уровень гарантии оценки 3 (EAL3). Методически проверено и протестировано

4.4.4.1 Имя пакета

Имя пакета - уровень гарантии оценки 3 (EAL3). Методически протестировано и проверено.

4.4.4.2 Тип пакета

Это пакет гарантии.

4.4.4.3 Обзор пакета

EAL3 позволяет добросовестному разработчику получить максимальную гарантию от безотказной техники обеспечения безопасности на этапе проектирования без существенного изменения существующих надежных методов разработки.

EAL3 применим в тех обстоятельствах, когда разработчикам или пользователям требуется умеренный уровень независимо гарантированной безопасности и требуется тщательное исследование TOE и его разработки без существенной технологической перестройки (реинжиниринга).

4.4.4.4 Цели

EAL3 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и интерфейсную спецификацию, руководящую документацию и архитектурное описание проектного решения TOE, чтобы понять режим безопасности.

Анализ поддерживается независимым тестированием TSF, доказательством тестирования разработчика на основе функциональной спецификации и проектного решения TOE, выборочным независимым подтверждением результатов тестирования разработчика и анализом уязвимости (на основе функциональной спецификации, проектного решения TOE, описания архитектуры безопасности и предоставленных руководящих доказательств), демонстрирующим устойчивость к внедрению злоумышленников с базовым потенциалом нападения.

EAL3 также предоставляет гарантию с помощью использования элементов управления средой разработки, управления конфигурацией TOE и доказательств процедур безопасной поставки.

Настоящий EAL представляет собой значительное увеличение гарантии по сравнению с EAL2, требуя более полного охвата тестированием функциональности безопасности и механизмов и/или процедур, которые обеспечивают некоторую уверенность в том, что TOE не будет подделан во время разработки.

4.4.4.5 Компоненты гарантии

В таблице 4 приведены компоненты гарантии, включенные в EAL 3.

**Таблица 4 - EAL3**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры безопасности |
| ADV\_FSP.3 Функциональная спецификация с полным кратким содержанием |
| ADVTDS.2 Архитектурное проектирование |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.3 Контроль авторизации |
| ALC\_CMS.3 Охват представления реализации CM |
| ALC\_DEL.1 Процедуры поставки |
| ALC\_DVS.1 Идентификация мер безопасности |
| ALC\_LCD.1 Модель жизненного цикла, определенная разработчиком |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Выведенные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |
| ATE: Испытания | ATE\_COV.2 Анализ охвата |
| ATE\_DPT.1 Испытание: базовое проектное решение |
| ATE\_FUN.1 Функциональное тестирование |
| ATE\_IND.2 Независимое тестирование. Образец |
| AVA: Уязвимость | AVA\_VAN.2 Анализ уязвимости |

4.4.5 Уровень гарантии оценки 4 (EAL4). Методически разработано, протестировано и проверено

4.4.5.1 Имя пакета

Имя пакета - уровень гарантии оценки 4 (EAL4). Методически разработано, протестировано и проверено.

4.4.5.2 Тип пакета

Это пакет гарантии.

4.4.5.3 Обзор пакета

EAL4 позволяет разработчику получить максимальную гарантию от безотказной техники безопасности на основе надлежащих коммерческих практик разработки, которые, несмотря на то что и являются строгими, не требуют существенных специальных знаний, навыков и других ресурсов. EAL4 - это наивысший уровень, на котором, вероятно, будет экономически целесообразно модернизировать существующую линейку продуктов.

Таким образом, EAL4 применим в тех обстоятельствах, когда разработчикам или пользователям требуется средний или высокий уровень независимо гарантированной безопасности в обычных товарных TOE и они готовы понести дополнительные расходы на технику безопасности.

4.4.5.4 Цели

EAL4 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и полную спецификацию интерфейса, руководящую документацию, описание базового модульного проектного решения TOE и подмножество реализации, чтобы понять режим безопасности.

Анализ поддерживается независимым тестированием TSF, доказательством тестирования разработчика на основе функциональной спецификации и конструкции TOE, выборочным независимым подтверждением результатов тестирования разработчика и анализом уязвимости (на основе функциональной спецификации, проекта TOE, представления реализации, описания архитектуры безопасности и предоставленных руководящих доказательств), демонстрирующим устойчивость к внедрению злоумышленников с потенциалом нападения Enhanced-Basic.

EAL4 также предоставляет гарантию с помощью использования элементов управления средой разработки и дополнительного управления конфигурацией TOE, включая автоматизацию и доказательство процедур безопасной поставки.

Настоящий уровень EAL представляет собой значительное увеличение гарантии по сравнению с EAL3, требуя большего описания проектного решения, представления реализации для всей TSF и улучшенных механизмов и/или процедур, которые обеспечивают уверенность в том, что TOE не будет подделан во время разработки.

4.4.5.5 Компоненты гарантии

В таблице 5 приведены компоненты гарантии, включенные в EAL 4.

**Таблица 5 - EAL4**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектурной безопасности |
| ADV\_FSP.4 Полная функциональная спецификация |
| ADV\_IMP.1 Представление реализации TSF |
| ADVTDS.3 Модульная архитектура |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |

*Продолжение таблицы 5*

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ALC: Поддержка жизненного цикла | ALC\_CMC.4 Поддержка производства, правила приемки и автоматизация | |
| ALC\_CMS.4 Отслеживание проблем охвата CM | |
| ALC\_DEL.1 Процедуры поставки | |
| ALC\_DVS.1 Идентификация мер безопасности | |
| ALC\_LCD.1 Определенная разработчиком модель жизненного цикла | |
| ALC\_TAT.1 Четко определенные средства разработчика | |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии | |
| ASE\_ECD.1 Определение расширенных компонентов | |
| ASE\_INT.1 Введение ST | |
| ASE\_OBJ.2 Цели безопасности | |
| ASE\_REQ.2 Выведенные требования безопасности | |
| ASE\_SPD.1 Определение проблемы безопасности | |
| ASE\_TSS.1 Спецификация краткого содержания TOE | |
| ATE: Тесты | ATE\_COV.2 Анализ охвата | |
| ATE\_DPT.1 Тестирование: базовое проектное решение | |
| ATE\_FUN.1 Функциональное тестирование | |
| ATE\_IND.2 Независимое тестирование. Образец | |
| AVA: Оценка уязвимости | AVA\_VAN.3 Ориентированный анализ уязвимости | |

4.4.6 Уровень гарантии оценки 5 (EAL5). Проверено, разработано и протестировано наполовину формально

4.4.6.1 Имя пакета

Имя пакета - уровень гарантии оценки 5 (EAL5). Разработано и протестировано наполовину формально

4.4.6.2 Тип пакета

Это пакет гарантии.

4.4.6.3 Обзор пакета

EAL5 позволяет разработчику получить максимальную гарантию от проектирования безопасности на основе строгих коммерческих практик разработки, поддерживаемых умеренным применением специализированных техник обеспечения безопасности. Такое задание по оценке (TOE), вероятно, спроектировано и разработано с целью достижения гарантии EAL5. Вероятно, что дополнительные затраты, связанные с требованиями EAL5, по сравнению со строгой разработкой без применения специализированных методов, невелики.

Поэтому уровень EAL5 применим в тех обстоятельствах, когда разработчикам или пользователям требуется высокий уровень независимо гарантированной безопасности в запланированной разработке и требуется строгий подход к разработке без необоснованных затрат, связанных со специализированными техниками обеспечения безопасности.

4.4.6.4 Цели

EAL5 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и полную спецификацию интерфейса, руководящую документацию, описание проектного решения TOE и реализацию, чтобы понять режим безопасности. Также требуется модульное проектное решение TSF.

Анализ поддерживается независимым тестированием TSF, доказательством тестирования разработчика на основе функциональной спецификации, проектного решения TOE, выборочным независимым подтверждением результатов тестирования разработчика и независимым анализом уязвимостей, демонстрирующим устойчивость к внедрению злоумышленников с умеренным потенциалом нападения.

EAL5 также предоставляет гарантию посредством использования элементов контроля средой разработки и комплексного управления конфигурацией TOE, включая автоматизацию и подтверждение процедур безопасной поставки.

Настоящий EAL представляет собой значительное увеличение гарантии по сравнению с EAL4, требуя наполовину формальных описаний проектного решения, более структурированной (и, следовательно, анализируемой) архитектуры и улучшенных механизмов и/или процедур, которые обеспечивают уверенность в том, что TOE не будет подделан во время разработки.

4.4.6.5 Компоненты гарантии

В таблице 6 приведены компоненты гарантии, включенные в EAL 5.

**Таблица 6 - EAL5**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры гарантии |
| ADV\_FSP.5 Полная наполовину формальная спецификация с дополнительной информацией об ошибке |
| ADV\_IMP.1 Представление реализации TSF |
| ADV\_INT.2 Хорошо структурированные внутренние элементы |
| ADVTDS.4 Наполовину формальное модульное проектное решение |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.4 Поддержка производства, правила приемки и автоматизация |
| ALC\_CMS.5 Инструменты разработки охвата CM |
| ALC\_DEL.1 Процедура поставки |
| ALC\_DVS.1 Идентификация мер безопасности |
| ALC\_LCD.1 Определенная разработчиком модель жизненного цикла |
| ALC\_TAT.2 Соответствие стандартам реализации |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Выведенные требования безопасности |
| ASE\_SPD.1 Определение проблем безопасности |
| ASE\_TSS.1 Спецификация краткого содержанияTOE |
| ATE: Тесты | ATE\_COV.2 Анализ охвата |
| ATE\_DPT.3 Тестирование: модульное проектное решение |
| ATE\_FUN.1 Функциональное тестирование |
| ATE\_IND.2 Независимое тестирование. Образец |
| AVA: Оценка уязвимости assessment | AVA\_VAN.4 Методичный анализ уязвимости |

4.4.7 Уровень гарантии оценки 6 (EAL6). Проверенное наполовину формально и протестированное проектное решение

4.4.7.1 Имя пакета

Имя пакета - уровень гарантии оценки 6 (EAL6). Проверенное наполовину формально и протестированное проектное решение.

4.4.7.2 Тип пакета

Это пакет гарантий.

4.4.7.3 Обзор пакета

Уровень EAL6 позволяет разработчикам получить высокую гарантию от применения методов проектирования безопасности в строгой среде разработки для создания первоклассного ТОЕ для защиты ценных активов от существенных рисков.

Поэтому уровень EAL6 применим к разработке ТОЕ безопасности для применения в ситуациях высокого риска, когда ценность защищенных активов оправдывает дополнительные затраты.

4.4.7.4 Цели

EAL6 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и полную спецификацию интерфейса, руководящую документацию, проектное решение ТОЕ и реализацию для понимания режима безопасности. Гарантия дополнительно достигается с помощью формальной модели выбранных политик безопасности ТОЕ и полуформального представления функциональной спецификации и проектного решения ТОЕ. Также требуется модульное, многоуровневое и простое проектное решение TSF.

Анализ поддерживается независимым тестированием TSF, доказательством тестирования разработчика на основе функциональной спецификации, проектированием TOE, выборочным независимым подтверждением результатов тестирования разработчика и независимым анализом уязвимостей, демонстрирующим устойчивость к внедрению злоумышленников с высоким потенциалом нападения (атаки).

EAL6 также предоставляет гарантию за счет использования структурированного процесса разработки, средств управления средой разработки и комплексного управления конфигурацией TOE, включая полную автоматизацию, и доказательством процедур безопасной поставки.

Настоящий EAL представляет собой значительное увеличение гарантии по сравнению с EAL5, требуя более комплексного анализа, структурированного представления реализации, большей архитектурной структуры (например, многоуровневости), более комплексного независимого анализа уязвимостей и улучшенного управления конфигурацией и средств управления средой разработки.

4.4.7.5 Компоненты гарантии

В таблице 7 приведены компоненты гарантии, включенные в EAL 6.

**Таблица 7 - EAL6**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры безопасности |
| ADV\_FSP.5 Полная полуформальная функциональная спецификация с дополнительной информацией об ошибке |
| ADV\_IMP.2 Полное сопоставление представления реализации TSF |
| ADV\_INT.3 Минимально усложненные внутренние элементы |
| ADV\_SPM.1 Политика модели безопасности формального TOE policy |

*Продолжение таблицы 7*

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
|  | ADVTDS.5 Полное полуформальное модульное проектное решение |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.5 Усовершенствованная поддержка |
| ALC\_CMS.5 Охват CM средств разработки |
| ALC\_DEL.1 Процедуры поставки |
| ALC\_DVS.2 Достаточность мер защиты |
| ALC\_LCD.1 Модель жизненного цикла, определенная разработчиком |
| ALC\_TAT.3 Соответствие стандартам реализации. Все части |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Выведенные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |
| ATE: Тесты | ATE\_COV.3 Строгий анализ охвата |
| ATE\_DPT.3 Тестирование: модульное проектное решение |
| ATE\_FUN.2 Упорядоченное функциональное тестирование |
| ATE\_IND.2 Независимое тестирование. Образец |
| AVA: Оценка уязвимости | AVA\_VAN.5 Усовершенствованный методичный анализ уязвимости |

4.4.8 Уровень гарантии оценки 7 (EAL7). Формально проверенное и протестированное проектное решение

4.4.8.1 Имя пакета

Имя пакета - уровень гарантии оценки 7 (EAL7). Формально проверенное и протестированное проектное решение.

4.4.8.2 Тип пакета

Это пакет гарантии.

4.4.8.3 Обзор пакета

EAL7 применим к разработке TOE безопасности для применения в ситуациях с чрезвычайно высоким риском и/или когда высокая стоимость активов оправдывает более высокие затраты. Практическое применение EAL7 в настоящее время ограничено TOE с узкоспециализированной функциональностью безопасности, которая поддается обширному формальному анализу.

4.4.8.4 Цели

EAL7 предоставляет гарантию с помощью полного ST и анализа SFR в настоящем ST, используя функциональную и полную спецификацию интерфейса, руководящую документацию, проект TOE и структурированное представление реализации для понимания режима безопасности. Гарантия дополнительно достигается посредством формальной модели выбранных политик безопасности TOE и полуформального представления функциональной спецификации и проектного решения TOE. Также требуется модульное, многоуровневое и простое проектное решение TSF.

Анализ поддерживается независимым тестированием TSF, доказательствами тестирования разработчика на основе функциональной спецификации, проектным решением TOE и представлением реализации, полным независимым подтверждением результатов тестирования разработчика и независимым анализом уязвимостей, демонстрирующим устойчивость к внедрению злоумышленников с высоким потенциалом нападения.

EAL7 также предоставляет гарантию посредством использования структурированного процесса разработки, контроля среды разработки и комплексного управления конфигурацией TOE, включая полную автоматизацию и доказательства процедур безопасной поставки.

Настоящий EAL представляет собой значительное увеличение гарантии по сравнению с EAL6, требуя более комплексного анализа с использованием формальных представлений и формальной переписки, а также комплексного тестирования.

4.4.8.5 Компоненты гарантии

В таблице 8 приведены компоненты гарантии, включенные в EAL 7.

**Таблица 8 - EAL7**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ADV: Разработка | ADV\_ARC.1 Описание архитектуры безопасности |
| ADV\_FSP.6 Полная полуформальная функциональная спецификация с дополнительной формальной спецификацией |
| ADV\_IMP.2 Полное сопоставление представления реализации TSF |
| ADV\_INT.3 Минимально усложненные внутренние элементы |
| ADV\_SPM.1 Политика модели безопасности формального TOE |
| ADVTDS.6 Полное полуформальное модульное проектное решение с формальным представлением высокоуровневого проектного решения |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.5 Усовершенствованная поддержка |
| ALC\_CMS.5 Охват CM инструментов разработки |
| ALC\_DEL.1 Процедуры поставки |
| ALC\_DVS.2 Достаточность мер безопасности |
| ALC\_LCD.2 Модель измеримого жизненного цикла |
| ALC\_TAT.3 Соответствие стандартам реализации, все части |
| ASE: Оценка ST | ASE\_CCL.1 Утверждения о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_REQ.2 Выведенные требования безопасности |
| ASE\_SPD.1 Определение проблем безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |
| ATE: Тесты | ATE\_COV.3 Строгий анализ охвата |
| ATE\_DPT.4 Тестирование: представление реализации |
| ATE\_FUN.2 Упорядоченное функциональное тестирование |
| ATE\_IND.3 Независимое тестирование. Полное |

*Продолжение таблицы 8*

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| AVA: Оценка уязвимости | AVA\_VAN.5 Упорядоченный методичный анализ уязвимости |

**5 Составные пакеты гарантии (CAP)**

**5.1 Имя семейства**

Имя настоящего семейства пакетов — составные пакеты гарантии (CAP).

**5.2 Обзор составного пакета гарантий (CAP)**

5.2.1 Общие положения

Структура CAP аналогична структуре EAL. Основное различие между настоящими двумя типами пакетов заключается в типе TOE, к которому они применяются. EAL, применяемые к компонентным TOE, и CAP, применяемые к составным TOE.

Рисунок 2 иллюстрирует CAP и связанную с ними структуру, определенную в настоящем документе.

Примечание - Несмотря на то, что на рисунке показан контент компонентов гарантий, предполагается, что эта информация включена в CAP путем ссылки на фактические компоненты, определенные в ISO/IEC 15408-3.

Некоторые зависимости идентифицируют действия, выполняемые во время оценки зависимого компонента, на который опирается составная деятельность TOE. Если явно не указано, что зависимость связана с деятельностью зависимого компонента, зависимость связана с другой деятельностью по оценке составного TOE.

Более высокий уровень гарантий, чем тот, который предоставляется данным CAP, может быть достигнут путем:

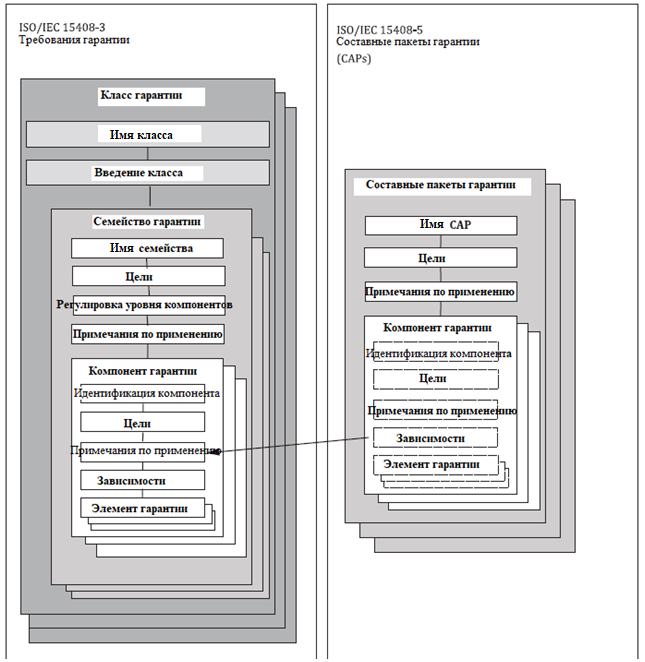
a) включения дополнительных компонентов гарантий из других семейств гарантий;

b) замена компонента гарантии на компонент гарантии более высокого уровня из того же семейства гарантии.

ACO: Компоненты состава, включенные в пакеты гарантии CAP, не должны использоваться в качестве расширений для оценок TOE компонента, поскольку это не обеспечит значимой гарантии для компонента.

5.2.2 Связь между гарантиями и пакетами гарантии

Рисунок 2 иллюстрирует связь между SAR и CAP, определенными в настоящем документе. Несмотря на то, что компоненты гарантии далее разлагаются на элементы гарантии, на элементы гарантии нельзя ссылаться по отдельности пакетами гарантии.



Примечание - Стрелка на рисунке представляет собой ссылку от CAP к компоненту гарантии в пределах класса, где он определен.

**Рисунок 2 -Связь гарантии и составного пакета гарантии (CAP)**

**5.3 Цели составного пакета гарантии (CAP)**

CAP предоставляют увеличивающуюся шкалу, которая уравновешивает уровень гарантии, полученной с ценностью и осуществимостью получения настоящей степени гарантии для составных TOE.

Примечание - В CAP включено лишь небольшое количество семейств и компонентов из ISO/IEC 15408-3. Это связано с их природой построения на результатах оценки ранее оцененных субъектов (базовых компонентов и зависимых компонентов), и это не означает, что они не предоставляют значимых и заданных гарантий.

CAP должны применяться к составным TOE, состоящим из компонентов, которые прошли или проходят оценку компонентного TOE (см. ISO/IEC 15408-3:2022   
(приложение B)). Отдельные компоненты сертифицированы по EAL или другому пакету гарантий, указанному в ST. Ожидается, что базовый уровень гарантий в составном TOE достигается путем применения EAL1, что может быть достигнуто с помощью информации о компонентах, которая обычно доступна в открытом доступе. (EAL1 может применяться, как указано, как к компонентным, так и к составным TOE.) CAP предоставляют альтернативный подход к получению более высоких уровней гарантий для составного TOE, чем применение EAL выше EAL1.

Несмотря на то, что зависимый компонент может быть оценен с использованием ранее оцененного и сертифицированного базового компонента для удовлетворения требований ИТ-платформы в среде, это не предоставляет какой-либо формальной гарантии взаимодействия между компонентами или возможного внедрения уязвимостей полученной из состава. CAP рассматривают настоящие взаимодействия и на более высоких уровнях гарантии, при условии, что интерфейс между компонентами сам по себе был предметом тестирования. Анализ уязвимости составного TOE также выполняется для рассмотрения возможного появления уязвимостей в результате составления компонентов.

Таблица 9 представляет собой краткое содержание CAP. Столбцы представляют собой иерархически упорядоченный набор CAP, в то время как строки представляют собой семейства гарантий. Каждое число в полученной матрице идентифицирует конкретный компонент гарантии, где это применимо.

В соответствии с 5.4, в настоящем стандарте определены три иерархически упорядоченных CAP для оценки гарантии составного TOE. Они иерархически упорядочены, поскольку каждый CAP представляет большую гарантию, чем все более низкие CAP. Увеличение гарантии от одного CAP к другому CAP достигается путем замены иерархически более высокого компонента гарантии из того же семейства гарантий (т. е. увеличения строгости, области применения и/или глубины) и путем добавления компонентов гарантии из других семейств гарантий (т. е. добавления новых требований). Настоящие увеличения приводят к более глубокому анализу состава для определения влияния на результаты оценки, полученные для отдельных компонентов TOE.

Настоящие CAP состоят из соответствующей комбинации компонентов гарантии, в соответствии с описанием в ISO/IEC 15408-3:2022 (раздел 6). Точнее, каждый CAP включает не более одного компонента каждого семейства гарантии, и рассматриваются все зависимости гарантии каждого компонента.

CAP рассматривают только устойчивость к злоумышленнику с потенциалом нападения вплоть до Enhanced-Basic (усовершенствованный - базовый). Это связано с уровнем информации о проектном решении, который может быть предоставлен через ACO\_DEV, ограничивая некоторые факторы, связанные с потенциалом нападения (знание составного TOE), и впоследствии влияя на строгость анализа уязвимости, который может быть выполнен оценщиком. Таким образом, уровень гарантии в составном TOE ограничен несмотря на то, что гарантия в отдельных компонентах в составе TOE может быть намного выше.

Таблица 9 показывает краткое содержание CAP.

**Таблица 9 - Краткое содержание состава пакета гарантии**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Класс гарантии | Семейство гарантии | Компоненты гарантии по пакету гарантии состава | | |
| CAP-A | CAP-B | CAP-C |
| Состав | ACO\_COR | **1** | 1 | 1 |

*Продолжение таблицы 9*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Класс гарантии | Семейство гарантии | | Компоненты гарантии по пакету гарантии состава | | |
| CAP-A | CAP-B | CAP-C |
|  | ACO\_CTT | | **1** | **2** | 2 |
| ACO\_DEV | | **1** | **2** | **3** |
| ACO\_REL | | **1** | 1 | **2** |
| ACO\_VUL | | **1** | **2** | **3** |
| Руководящие документы | AGD\_OPE | | **1** | 1 | 1 |
| AGD\_PRE | | **1** | 1 | 1 |
| Поддержка жизненного цикла | ALC\_CMC | | **1** | 1 | 1 |
| ALC\_CMS | | **2** | 2 | 2 |
| Оценка ST | | ASE\_CCL | **1** | 1 | 1 |
| ASE\_ECD | **1** | 1 | 1 |
| ASE\_INT | **1** | 1 | 1 |
| ASE\_OBJ | **1** | **2** | 2 |
| ASE\_REQ | **1** | **2** | 2 |
| ASE\_SPD |  | **1** | 1 |
| ASE\_TSS | **1** | 1 | 1 |

**5.4 Пакеты в семействе CAP**

5.4.1 Пакет гарантий состава A - структурно составленный

5.4.1.1 Имя пакета

Имя пакета - пакет гарантии состава A (CAP-A) - структурно составленный.

5.4.1.2 Тип пакета

Это пакет гарантии.

5.4.1.3 Обзор пакета

CAP-A применяется, когда интегрирован составной TOE и требуется уверенность в правильной работе безопасности полученного составного объекта. Это требует сотрудничества разработчика зависимого компонента с точки зрения предоставления информации о проектном решении и результатов испытаний из сертификации зависимого компонента, без необходимости привлечения разработчика базового компонента.

Таким образом, CAP-A применяется в тех обстоятельствах, когда разработчикам или пользователям требуется низкий или средний уровень независимо гарантированной безопасности при отсутствии готовой доступности полной записи разработки.

5.4.1.4 Цели

CAP-A предоставляет гарантии путем анализа ST для составного TOE. SFR в ST составного TOE анализируются с использованием результатов оценок компонентов TOE (например, ST, руководящей документации) и спецификации интерфейсов между компонентными TOE в составном TOE для понимания режима безопасности.

Анализ поддерживается независимым тестированием интерфейсов базового компонента, на которые полагается зависимый компонент, в соответствии с описанием в информации о зависимости, доказательством тестирования разработчика на основе информации о зависимости, информации о разработке и обосновании состава и выборочного независимого подтверждения результатов тестирования разработчика. Анализ также поддерживается обзором уязвимостей составного TOE оценщиком.

CAP-A также предоставляет гарантию посредством уникальной идентификации составного TOE (т.е. IT TOE и руководящей документации).

5.4.1.5 Компоненты гарантии

В таблице 10 приведены компоненты гарантии, включенные в CAP-A.

**Таблица 10 - CAP-A**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ACO: Состав | ACO\_COR.1 Обоснование состава |
| ACO\_CTT.1 Тестирование интерфейса |
| ACO\_DEV.1 Функциональное описание |
| ACO\_REL.1 Информация о базовой зависимости |
| ACO\_VUL.1 Обзор уязвимости состава |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC Поддержка жизненного цикла | ALC\_CMC.1 Маркировка TOE |
| ALC\_CMS.1 Охват TOE CM |
| ASE: Оценка ST | ASE\_CCL.1 Заявления о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASEJNT.1 Введение ST |
| ASE\_OBJ.1 Цели безопасности для операционной среды |
| ASE\_REQ.1 Утвержденные требования к безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |

5.4.2 Пакет гарантии состава B. Составлен методически

5.4.2.1 Имя пакета

Имя пакета - пакет гарантии состава B (CAP-B). Методически составлен.

5.4.2.2 Тип пакета

Это пакет гарантии

5.4.2.3 Обзор пакета

CAP-B позволяет добросовестному разработчику получить максимальную уверенность от понимания на уровне подсистем эффектов взаимодействия между компонентами TOE, интегрированными в составной TOE, при этом минимизируя необходимость участия разработчика базового компонента.

CAP-B применим в тех обстоятельствах, когда разработчикам или пользователям требуется умеренный уровень независимо гарантированной безопасности и тщательное исследование составного TOE и его разработки без существенной модернизации (реинжиниринга).

5.4.2.4 Цели

CAP-B предоставляет гарантии путем анализа полного ST для составного TOE. SFR в ST составного TOE анализируются с использованием результатов оценок компонентов TOE (например, ST, руководящей документации), спецификации интерфейсов между компонентными TOE и проектным решением TOE (описывающей подсистемы TSF), содержащейся в составной информации о разработке, для понимания режима безопасности.

Анализ поддерживается независимым тестированием интерфейсов базового компонента, на которые полагается зависимый компонент, в соответствии с описанием в информации о зависимости (теперь также включающей проектное решение TOE), доказательствами тестирования разработчика на основе информации о зависимости, информации о разработке и обоснования состава и выборочного независимого подтверждения результатов тестирования разработчика. Анализ также поддерживается анализом уязвимости составного TOE оценщиком, демонстрирующим устойчивость к злоумышленникам с базовым потенциалом нападения.

Настоящий CAP представляет собой значительное увеличение гарантий по сравнению с CAP-A, требуя более полного охвата тестирования функциональности безопасности.

5.4.2.5 Компоненты гарантий

В таблице 11 приведены компоненты гарантий, включенные в CAP-B.

**Таблица 11 - CAP-B**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ACO: Состав | ACO\_COR.1 Обоснование состава |
| ACO\_CTT.2 Строгое тестирование интерфейса |
| ACO\_DEV.2 Базовое свидетельство проектного решения |
| ACO\_REL.1 Информация о базовой зависимости |
| ACO\_VUL.2 Анализ состава уязвимости |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.1 Маркировка TOE |
| ALC\_CMS.2 Части охватаTOE CM |
| ASE: Оценка ST | ASE\_CCL.1 Заявления о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности для операционной среды |
| ASE\_REQ.2 Утвержденные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |

5.4.3 Пакет гарантии состава C. Методически составленный, протестированный и проверенный

5.4.3.1 Имя пакета

Имя пакета - пакет гарантии состава C (CAP-C). Методически составленный, протестированный и проверенный.

5.4.3.2 Тип пакета

Это пакет гарантии.

5.4.3.3 Обзор пакета

CAP-C позволяет разработчику получить максимальную гарантию от положительного анализа взаимодействий между компонентами составного TOE, которые, несмотря на то, что и являются строгими, не требуют полного доступа ко всем свидетельствам оценки базового компонента.

Поэтому CAP-C применим в тех обстоятельствах, когда разработчикам или пользователям требуется средний или высокий уровень независимо гарантированной безопасности в обычных товарных составных TOE и они готовы понести дополнительные расходы на проектирование, связанные с безопасностью.

5.4.3.4 Цели

CAP-C предоставляет гарантию путем анализа полного ST для составного TOE. SFR в ST составного TOE анализируются с использованием результатов оценок компонентов TOE (например, ST, руководящей документации), спецификации интерфейсов между компонентами TOE и проектного решения TOE (описывающего модули TSF), содержащегося в составной информации о разработке, для понимания режима безопасности.

Анализ поддерживается независимым тестированием интерфейсов базового компонента, на которые полагается зависимый компонент, в соответствии с описанием в информации о зависимости (теперь включая проектное решение TOE), доказательством тестирования разработчика на основе информации о зависимости, информации о разработке и обосновании состава, а также выборочным независимым подтверждением результатов тестирования разработчика. Анализ также поддерживается анализом уязвимости составного TOE оценщиком, демонстрирующим устойчивость к злоумышленникам с потенциалом нападения Enhanced-Basic.

Настоящий CAP представляет собой значительное увеличение гарантии от CAP-B, требуя большего описания проектного решения и демонстрации устойчивости к более высокому потенциалу нападения.

5.4.3.5 Компоненты гарантии

Таблица 12 содержит компоненты гарантии, включенные в CAP-C.

**Таблица 12 - CAP-C**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ACO: Состав | ACO\_COR.1 Обоснование состава |
| ACO\_CTT.2 Строгое тестирование интерфейса |
| ACO\_DEV.3 Детальное свидетельство проектного решения |
| ACO\_REL.2 Информация о зависимости |
| ACO\_VUL.3 Анализ уязвимости состава Enhanced-Basic |
| AGD: Руководящие документы | AGD\_OPE.1 Руководство для операционного пользователя |
| AGD\_PRE.1 Подготовительные процедуры |
| ALC: Поддержка жизненного цикла | ALC\_CMC.1 Маркировка TOE |
| ALC\_CMS.2 Части охватаTOE CM |
| ASE: Оценка ST | ASE\_CCL.1 Заявления о соответствии |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_INT.1 Введение ST |
| ASE\_OBJ.2 Цели безопасности для операционной среды |
| ASE\_REQ.2 Утвержденные требования безопасности |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_TSS.1 Спецификация краткого содержания TOE |

**6 Пакет композитного (смешанного) продукта**

**6.1 Имя пакета**

Имя пакета - пакет композитного продукта (COMP).

**6.2 Тип пакета**

Настоящий пакет является пакетом гарантии.

**6.3 Обзор пакета**

COMP предоставляет гарантию того, что композитный продукт был собран и оценен в соответствии с надлежащими критериями.

**6.4 Цели**

Компоненты гарантии \*.COMP применяются, когда для составного продукта используются методы оценки состава в соответствии с ISO/IEC 15408-1:2022 (раздел 14) и 14.3.3. Цели заключаются в следующем:

- гарантировать, что TOE состоит из уже оцененного базового компонента и зависимого компонента с учетом требований, указанных в ISO/IEC 15408-1 и   
ISO/IEC 15408-3;

- что оценка ST, требований жизненного цикла, проектного решения, тестирования и анализа уязвимостей для композитного продукта были выполнены в соответствии с критериями, указанными в ISO/IEC 15408-3.

Настоящие цели предоставляют гарантию того, что потенциальные противоречия, несоответствия или пробелы в безопасности, возникающие из-за состава базового компонента и зависимого компонента композитного продукта, были рассмотрены и отсутствуют.

**6.5 Компоненты гарантии безопасности**

Компоненты гарантии безопасности, указанные в таблице 13, включены в пакет.

**Таблица 13 - COMP**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ASE: Оценка задания по безопасности | ASE\_COMP.1 Согласованность задания по безопасности |
| ADV: Разработка | ADV\_COMP.1 Соответствие проектного решения руководству пользователя, связанному с базовыми компонентами, ETR для комплексной оценки и отчету органа оценки базовых компонентов |
| ALC: Поддержка жизненного цикла | ALC\_COMP.1 Интеграция зависимого компонента в связанный базовый компонент и проверка согласованности процедур поставки и приемки |
| ATE: Тесты | ATE\_COMP.1 Функциональное тестирование композитных продуктов |
| AVA: Оценка уязвимости | AVA\_COMP.1 Оценка уязвимости композитных продуктов |

**7 Гарантии профилей защиты**

**7.1 Имя семейства**

Имя настоящего семейства пакетов - пакеты гарантий профилей защиты (PPA).

**7.2 Обзор семейства PPA**

Семейство PPA предоставляет два пакета гарантий для оценки PP:

a) пакет гарантий для оценки прямых обоснований PP;

b) пакет гарантий для оценки стандартных PP.

Настоящие пакеты гарантий предоставляют компоненты, которые используются при оценке каждого типа PP, описанного в ISO/IEC 15408-1.

Таблица 14 представляет собой сводку PPA. Столбцы представляют набор PPA, а строки представляют семейства гарантий. Каждое число в результирующей матрице идентифицирует конкретный компонент гарантий, где это применимо.

Настоящие PPA состоят из соответствующей комбинации компонентов гарантий, в соответствии с описанием в ISO/IEC 15408-3:2022 (раздел 7). Точнее, каждый PPA включает не более одного компонента из каждого семейства гарантий, и рассматриваются все зависимости гарантий каждого компонента.

**Таблица 14 - Краткое содержание PPA**

|  |  |  |  |
| --- | --- | --- | --- |
| Класс гарантии | Семейство гарантии | Компоненты гарантии по пакету гарантии профиля защиты | |
| Пакет гарантии профиля защиты - прямое обоснование (PPA-DR) | Пакет гарантии профиля защиты - стандартный  (PPA-STD) |
| Оценка PP | APE\_CCL | **1** | 1 |
| APE\_ECD | **1** | 1 |
| APE\_INT | **1** | 1 |
| APE\_OBJ | **1** | **2** |
| APE\_REQ | **1** | **2** |
| APE\_SPD | **1** | 1 |

**7.3 Цели семейства PPA**

Цели PPA - поддержка предоставления гарантий посредством оценки того, что профиль защиты соответствует требованиям, указанным в ISO/IEC 15408-1.

**7.4 Пакеты PPA**

7.4.1 Пакет гарантий профиля защиты. Прямое обоснование PP

7.4.1.1 Имя пакета

Имя пакета - пакет гарантий профиля защиты. Прямое обоснование (PPA-DR).

7.4.1.2 Тип пакета

Настоящий пакет является пакетом гарантий.

7.4.1.3 Обзор пакета

PPA\_DR предоставляет гарантии посредством оценки профиля защиты прямого обоснования с помощью критериев, указанных в ISO/IEC 15408-3.

7.4.1.4 Цели

PPA-DR применяется при оценке PP прямого обоснования. Его можно использовать для проверки того, что PP прямого обоснования соответствует требованиям   
ISO/IEC 15408-1.

7.4.1.5 Компоненты гарантии безопасности

Компоненты гарантии безопасности, указанные в таблице 15, включены в пакет.

**Таблица 15 - PPA-DR**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| APE: Оценка профиля защиты | APEJNT.1 Введение PP |
| APE\_CCL.1 Заявления о соответствии |
| APE\_SPD.1 Определение проблемы безопасности |
| APE\_OBJ.1 Цели безопасности для операционной среды |
| APE\_ECD.1 Определение расширенных компонентов |
| APE\_REQ.1 Утвержденные требования безопасности |

7.4.2 Пакет гарантии профиля защиты. Стандартный

7.4.2.1 Имя пакета

Имя пакета - пакет гарантии профиля защиты. Стандартный (PPA-STD).

7.4.2.2 Тип пакета

Настоящий пакет является пакетом гарантии.

7.4.2.3 Обзор пакета

PPA\_STD предоставляет обеспечение путем оценки стандартного PP с использованием критериев, указанных в ISO/IEC 15408-3.

7.4.2.4 Цели

PPA-STD применяется при оценке стандартного PP. Его можно использовать для проверки того, что стандартный PP соответствует требованиям ISO/IEC 15408-1.

7.4.2.5 Компоненты гарантии безопасности

PPA\_STD предоставляет обеспечение путем оценки стандартного PP, в соответствии с ISO/IEC 15408-1. Компоненты гарантии, включенные в PPA\_STD, приведены в   
таблице 16.

**Таблица 16 - PPA-STD**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| APE: Оценка профиля защиты | APE\_INT.1 Введение PP |
| APE\_CCL.1 Заявления о соответствии |
| APE\_SPD.1 Определение проблемы безопасности |
| APE\_OBJ.2 Цели безопасности |
| APE\_ECD.1 Определение расширенного компонента |
| APE\_REQ.2 Требования безопасности |

**8 Гарантии задания по безопасности**

**8.1 Имя семейства**

Имя настоящего семейства пакетов - гарантии задания по безопасности (STA).

**8.2 Обзор семейства STA**

Семейство STA предоставляет два пакета гарантий для оценки ST:

a) пакет гарантий для оценки прямых обоснований ST;

b) пакет гарантий для оценки стандартных ST.

Настоящие пакеты гарантий предоставляют компоненты, которые используются при оценке каждого типа задания по безопасности, описанной в ISO/IEC 15408-1.

Таблица 17 представляет собой краткое содержание пакетов STA. Столбцы представляют набор STA, а строки представляют семейства гарантий. Каждое число в полученной матрице идентифицирует конкретный компонент гарантий, где это применимо.

Настоящие STA состоят из соответствующей комбинации компонентов гарантий, в соответствии с описанием в ISO/IEC 15408-3:2022 (раздел 9). Точнее, каждый STA включает не более одного компонента из каждого семейства гарантий, и рассматриваются все зависимости гарантий каждого компонента.

**Таблица 17 - Сводка STA**

|  |  |  |  |
| --- | --- | --- | --- |
| Класс гарантии | Семейство гарантии | Компоненты гарантии по пакету гарантии ST | |
| Пакет гарантии задания по безопасности. Прямое обоснование (STA- DR) | Пакет гарантии задания по безопасности. Стандартный (STA- STD) |
| Оценка ST | ASE\_INT | **1** | 1 |
| ASE\_CCL | **1** | 1 |
| ASE\_SPD | **1** | 1 |
| ASE\_OBJ | **1** | **2** |
| ASE\_ECD | **1** | 1 |
| ASE\_REQ | **1** | **2** |
| ASE\_TSS | **1** | 1 |

**8.3 Цели семейства STA**

Цели STA заключаются в поддержке предоставления гарантий посредством оценки того, что профиль защиты соответствует требованиям, указанным в ISO/IEC 15408-1.

**8.4 Пакеты STA**

8.4.1 Пакет гарантии задания по безопасности. Прямое обоснование

8.4.1.1 Имя пакета

Имя пакета - пакет гарантии задания по безопасности. Прямое обоснование   
(STA-DR).

8.4.1.2 Тип пакета

Настоящий пакет является пакетом гарантии.

8.4.1.3 Обзор пакета

STA\_DR предоставляет гарантии посредством оценки прямого обоснования ST, используя критерии, указанные в ISO/IEC 15408-3.

8.4.1.4 Цели

STA-DR применяется при оценке ST прямого обоснования. Его можно использовать для проверки того, что ST прямого обоснования соответствует требованиям   
ISO/IEC 15408-1.

8.4.1.5 Компоненты гарантии безопасности

Компоненты гарантии безопасности, приведенные в таблице 18, включены в пакет.

**Таблица 18 - STA-DR**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ASE: Оценка ST | ASE\_INT.1 Введение ST |
| ASE\_CCL.1 Заявления о соответствии |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_OBJ.1 Цели безопасности для операционной среды |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_REQ.1 Утвержденные требования безопасности |
| ASE-TSS.1 Спецификация краткого содержания TOE |

8.4.2 Пакет гарантии задания по безопасности. Стандартный

8.4.2.1 Имя пакета

Имя пакета - пакет гарантии задания по безопасности - стандартный (STA-STD).

8.4.2.2 Тип пакета

Настоящий пакет является пакетом гарантии.

8.4.2.3 Обзор пакета

STA\_STD предоставляет обеспечение путем оценки стандартного ST с использованием критериев, указанных в ISO/IEC 15408-3.

8.4.2.4 Цели

STA-STD применяется при оценке стандартного ST. Его можно использовать для проверки того, что стандартный ST соответствует требованиям ISO/IEC 15408-1.

8.4.2.5 Компоненты гарантии безопасности

STA\_STD предоставляет обеспечение путем оценки стандартного ST, в соответствии с ISO/IEC 15408-1. Компоненты гарантии безопасности, приведенные в таблице 19, включены в пакет.

**Таблица 19 - STA-STD**

|  |  |
| --- | --- |
| Класс гарантии | Компоненты гарантии |
| ASE: Оценка ST | ASEJNT.1 Введение ST |
| ASE\_CCL.1 Заявления о соответствии |
| ASE\_SPD.1 Определение проблемы безопасности |
| ASE\_OBJ.2 Цели безопасности |
| ASE\_ECD.1 Определение расширенных компонентов |
| ASE\_REQ.2 Утвержденные требования безопасности |
| ASE-TSS.1 Спецификация краткого содержания TOE |

**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 15408-3:2022 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 |

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

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

**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**