

# **ЗАНЯТИЕ 3/1**

**«Стандарт ИСО/МЭК  
15408-1-2008 Часть 1.».**

## *Учебные вопросы.*

1. Введение и общая модель.
2. Краткий обзор стандарта.

**1-й учебный вопрос:**

**«Введение и общая модель»**

ИСО/МЭК 15408 под общим наименованием "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" состоит из следующих частей:

- часть 1. Введение и общая модель;
- часть 2. Функциональные требования безопасности;
- часть 3. Требования доверия к безопасности.

*В настоящем стандарте применены следующие термины с соответствующими определениями.*

- **активы (assets)**: Информация или ресурсы, подлежащие защите контрмерами. ОО.

- **назначение (assignment)**: Спецификация определенного параметра в компоненте.

- **доверие (assurance)**: Основание для уверенности в том, что сущность отвечает своим целям безопасности.

- **потенциал нападения (attack potential)**: Прогнозируемый потенциал для успешного (в случае реализации) нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя.

- **усиление** (augmentation): Добавление одного или нескольких компонентов доверия из ИСО/МЭК 15408-3 в оценочный уровень доверия (ОУД) или пакет требований доверия.

- **аутентификационные данные** (authentication data): Информация, используемая для верификации предъявленного идентификатора пользователя.

- **уполномоченный пользователь** (authorised user): Пользователь, которому в соответствии с политикой безопасности объекта оценки (ПБО) разрешено выполнять некоторую операцию.

- **класс** (class): Группа семейств, объединенных общим назначением.

- **компонент** (component): Наименьшая выбираемая совокупность элементов, которая может быть включена в профиль защиты (ПЗ), задание по безопасности (ЗБ) или пакет.

- **связность** (connectivity): Свойство объекта оценки (ОО), позволяющее ему взаимодействовать с сущностями ИТ, внешними по отношению к ОО. Данное взаимодействие включает в себя обмен данными по проводным или беспроводным средствам на любом расстоянии, в любой среде или при любой конфигурации.

- **зависимость** (dependency): Соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть, как правило, удовлетворено с тем, чтобы и другие требования могли отвечать своим целям.

- **элемент** (element): Неделимое требование безопасности.

- **оценка** (evaluation): Оценка ПЗ, ЗБ или ОО по определенным критериям.

**- оценочный уровень доверия (evaluation assurance level):** Пакет компонентов доверия из ИСО/МЭК 15408-3, представляющий некоторое положение на определенной в ИСО/МЭК 15408 шкале доверия.

**- орган оценки (evaluation authority):** Организация, которая посредством системы оценки обеспечивает реализацию ИСО/МЭК 15408 для определенного сообщества и в связи с этим устанавливает стандарты и контролирует качество оценок, проводимых организациями в пределах данного сообщества.

**- система оценки (evaluation scheme):** Административно-правовая структура, в рамках которой в определенном сообществе органы оценки применяют ИСО/МЭК 15408.



**- расширение (extension):** Добавление в ЗБ или ПЗ функциональных требований, не содержащихся в ИСО/МЭК 15408-2, и/или требований доверия, не содержащихся в ИСО/МЭК 15408-3.

**- внешняя сущность ИТ (external IT entity):** Любой продукт или система ИТ, доверенные или нет, находящиеся вне ОО и взаимодействующие с ним.

**- семейство (family):** Группа компонентов, которые направлены на достижение одних и тех же целей безопасности, но могут отличаться акцентами или строгостью.

- **формальный (formal)**: Выраженный на языке с ограниченным синтаксисом и определенной семантикой, основанной на установившихся математических понятиях.

- **документация руководств (guidance documentation)**: Документация руководств, описывающая поставку, установку, конфигурирование, эксплуатацию, управление и использование ОО в той части, в которой эти виды деятельности имеют отношение к пользователям, администраторам и интеграторам ОО. Требования к области применения и содержанию документированных руководств определяются в ПЗ и ЗБ.

- **человек-пользователь (human user)**: Любое лицо, взаимодействующее с ОО.

**- идентификатор (identity):** Представление уполномоченного пользователя (например строка символов), однозначно его идентифицирующее. Таким представлением может быть полное или сокращенное имя этого пользователя или его псевдоним.

**- неформальный (informal):** Выраженный на естественном языке.

**- внутренний канал связи (internal communication channel):** Канал связи между разделенными частями ОО.

**- передача в пределах ОО (internal TOE transfer):** Передача данных между разделенными частями ОО.

**- передача между ФБО (inter-TSF transfers):**

Передача данных между функциями безопасности объекта оценки (ФБО) и функциями безопасности других доверенных продуктов ИТ.

**- итерация (iteration):** Более чем

однократное использование компонента при различном выполнении операций.

**- объект (object):** Сущность в пределах

области действия ФБО (ОДФ), которая содержит или получает информацию и над которой субъекты выполняют операции.

**- политика безопасности организации** (organisational security policies): Одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

**- пакет (package):** Предназначенная для многократного использования совокупность функциональных компонентов или компонентов доверия (например, ОУД), объединенных для удовлетворения совокупности определенных целей безопасности.

**- продукт (product):** Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

**- профиль защиты (protection profile):**

Независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

**- монитор обращений (reference monitor):**

Концепция абстрактной машины, осуществляющей политики управления доступом ОО.

**- механизм проверки правомочности**

**обращений (reference validation mechanism):**

Реализация концепции монитора обращений, обладающая следующими свойствами:

защищенностью от проникновения; постоянной готовностью; простотой, достаточной для проведения исчерпывающего анализа и тестирования.

- **уточнение (refinement)**: Дополнение компонента деталями.

- **роль (role)**: Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и ОО.

- **секрет (secret)**: Информация, которая должна быть известна только уполномоченным пользователям и/или ФБО для осуществления определенной политики функции безопасности (ПФБ).

- **атрибут безопасности (security attribute)**: Характеристики субъектов, пользователей объектов, информации и/или ресурсов, которые используются для осуществления ПБО.

**- функция безопасности (security function):**

Функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

**- политика функции безопасности (security function policy):** Политика безопасности, осуществляемая функцией безопасности (ФБ).

**- цель безопасности (security objective):**

Изложенное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям.

**- задание по безопасности (security target):**

Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО.



- **выбор** (selection): Выделение одного или нескольких элементов из перечня в компоненте.
- **полуформальный** (semiformal): Выраженный на языке с ограниченным синтаксисом и определенной семантикой.
- **базовая СФБ** (SOF-basic): Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.
- **высокая СФБ** (SOF-high): Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.

- **средняя СФБ (SOF-medium)**: Уровень стойкости функции безопасности ОО, на котором, как показывает анализ, функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.

- **стойкость функции безопасности (strength of function)**: Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности.

- **субъект (subject)**: Сущность в пределах ОДФ, инициирующая выполнение операций.

- **система (system)**: Специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

- **объект оценки (target of evaluation)**: Продукт или система ИТ и связанная с ними документация руководств, являющиеся предметом оценки.
- **ресурс ОО (TOE resource)**: Все, что может быть использовано или потреблено ОО.
- **функции безопасности ОО (TOE security functions)**: Совокупность всех функций безопасности ОО, направленных на осуществление ПБО.
- **интерфейс функций безопасности ОО (TOE security functions interface)**: Совокупность интерфейсов как интерактивных (человеко-машинные интерфейсы), так и программных (интерфейсы прикладных программ), с использованием которых осуществляется доступ к ресурсам ОО при посредничестве ФБО или получение от ФБО какой-либо информации.

**- политика безопасности ОО (TOE security policy):** Совокупность правил, регулирующих управление активами, их защиту и распределение в пределах ОО.

**- модель политики безопасности ОО (TOE security policy model):** Структурированное представление политики безопасности, которая должна быть осуществлена ОО.

**- передача за пределы области действия ФБО (transfers outside TSF control):** Передача данных сущностям, не контролируемым ФБО.

**- доверенный канал (trusted channel):** Средство взаимодействия между ФБО и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании ПБО.

- **доверенный маршрут (trusted path)**: Средство взаимодействия между пользователем и ФБО, обеспечивающее необходимую степень уверенности в поддержании ПБО.

- **данные ФБО (TSF data)**: Данные, созданные ФБО или для ФБО, которые могут повлиять на выполнение ФБО.

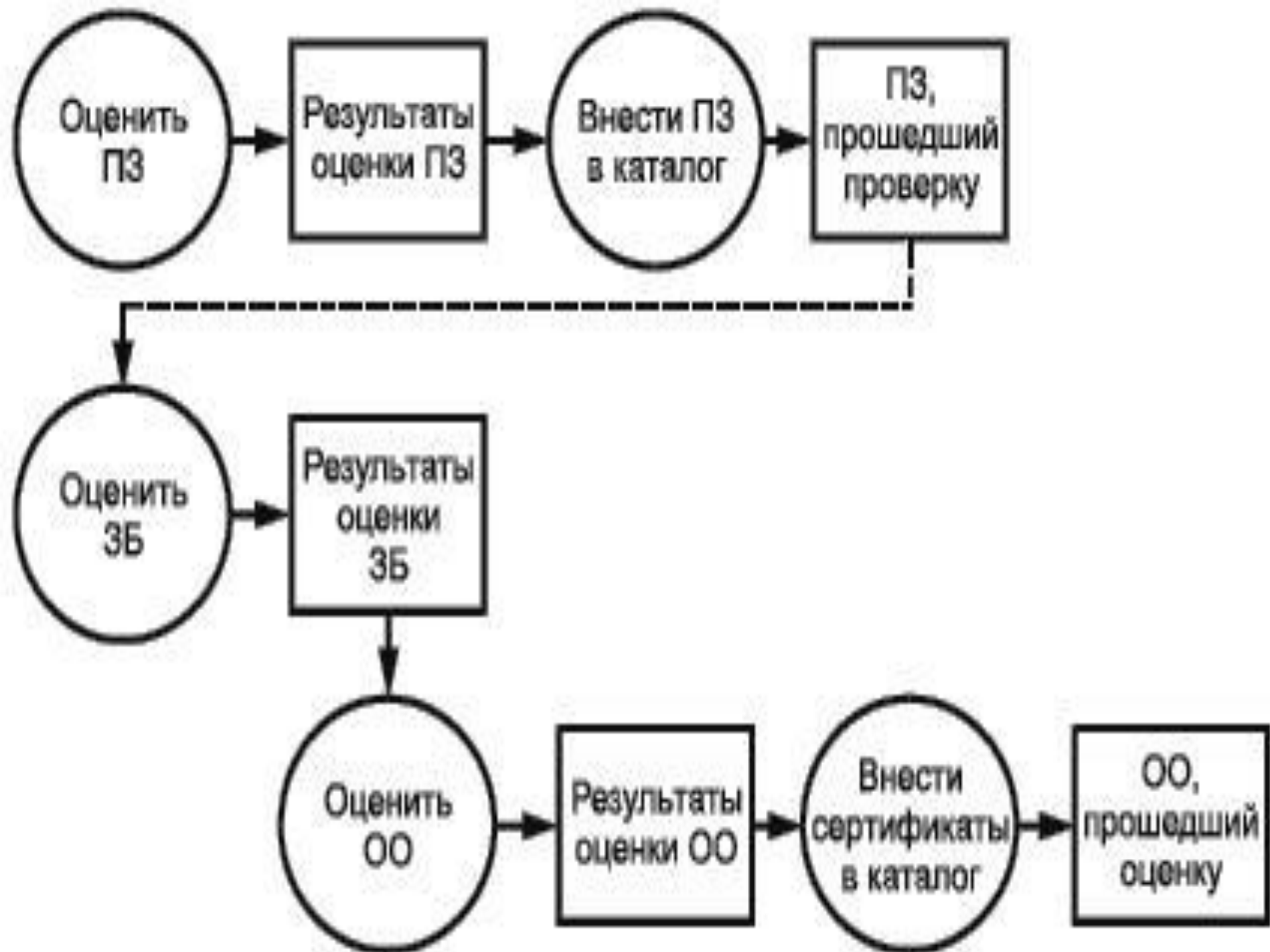
- **область действия ФБО (TSF score of control)**: Совокупность возможных взаимодействий с ОО или в его пределах, которые подчинены правилам ПБО.

- **пользователь (user)**: Любая сущность (человек-пользователь или внешняя сущность ИТ) вне ОО, которая взаимодействует с ОО.

- **данные пользователя (user data)**: Данные, созданные пользователем и для пользователя, которые не влияют на выполнение ФБО.

**2-й учебный вопрос:**

**«Краткий обзор стандарта»**



В ИСО/МЭК 15408 допускается возможность того, что при формировании полного набора требований к безопасности ИТ могут понадобиться функциональные требования и требования доверия, не включенные в соответствующие каталоги. Для включения таких расширенных требований в ПЗ или ЗБ должны быть **выполнены следующие условия:**

а) любые расширенные функциональные требования или требования доверия, включенные в ПЗ или ЗБ, должны быть четко и недвусмысленно сформулированы и выражены так, чтобы была возможна оценка и демонстрация соответствия ОО этим требованиям. В качестве образца должны использоваться уровень детализации и способ выражения существующих функциональных компонентов и компонентов доверия из ИСО/МЭК 15408;



б) результаты оценки, полученные с использованием расширенных функциональных требований и требований доверия, должны содержать соответствующие пояснения;

с) включение, при необходимости, в состав ПЗ или ЗБ расширенных функциональных требований или требований доверия должно соответствовать требованиям классов APE или ASE из ИСО/МЭК 15408-3.

Результаты оценки соответствия должны включать в себя **один из следующих вариантов:**

а) "соответствие ИСО/МЭК 15408-2" - ПЗ или ОО соответствует ИСО/МЭК 15408-2, если функциональные требования основаны только на функциональных компонентах из ИСО/МЭК 15408-2;

б) "расширение ИСО/МЭК 15408-2" - ПЗ или ОО является расширенным по отношению к ИСО/МЭК 15408-2, если функциональные требования включают в себя функциональные компоненты, не содержащиеся в ИСО/МЭК 15408-2;

**а также одно из следующего:**

- а) "соответствие ИСО/МЭК 15408-3" - ПЗ или ОО соответствует ИСО/МЭК 15408-3, если требования доверия основаны только на компонентах доверия из ИСО/МЭК 15408-3;
- б) "расширение ИСО/МЭК 15408-3" - ПЗ или ОО является расширенным по отношению к ИСО/МЭК 15408-3, если требования доверия включают требования доверия не из ИСО/МЭК 15408-3.

Результат оценки соответствия может включать в себя утверждение, сделанное относительно набора определенных требований; в данном случае результат оценки соответствия включает в себя **одно из следующего:**

а) "соответствие именованному пакету" - ПЗ или ОО соответствует predetermined именованному функциональному пакету и/или пакету доверия (например ОУД), если требования (функциональные или доверия) включают в себя все компоненты, перечисленные в пакете, как часть результата оценки соответствия;

б) "усиление именованного пакета" - ПЗ или ОО является усилением predetermined именованного функционального пакета и/или пакета доверия (например ОУД), если требования (функциональные или доверия) являются надлежащим надмножеством всех компонентов, перечисленных в пакете, как часть результата оценки соответствия.