# ЗАНЯТИЕ 3/2

# «Стандарт ИСО/МЭК 15408-3. Часть 3.».

## *Учебные вопросы.*

1. Требования доверия к безопасности.
2. Краткий обзор стандарта.

# 1-й учебный вопрос:

# «  Требования доверия к безопасности»

**Основная концепция ИСО/МЭК 15408**

- обеспечение доверия, основанное на оценке (активном исследовании) продукта ИТ, который должен соответствовать определенным критериям безопасности.

**По возможности уязвимости следует**:

a) **устранить,** т.е. следует предпринять активные действия для выявления, а затем удаления или нейтрализации всех уязвимостей, которые могут проявиться;

b) **минимизировать,** т.е. следует предпринять активные действия для уменьшения до допустимого остаточного уровня возможного ущерба от любого проявления уязвимостей;

c) **отслеживать**, т.е. следует предпринять активные действия для обнаружения любой попытки использовать остаточные уязвимости с тем, чтобы ограничить ущерб.

Уязвимости **могут возникать из-за недостатков**:

a) **требований,** т.е. продукт ИТ может обладать требуемыми от него функциями и свойствами, но все же содержать уязвимости, которые делают его непригодным или неэффективным в части безопасности;

b) **проектирования**, т.е. продукт ИТ не отвечает спецификации, и/или уязвимости являются следствием некачественных стандартов проектирования или неправильных проектных решений;

c) **эксплуатации,** т.е. продукт ИТ разработан в полном соответствии с корректной спецификацией, но уязвимости возникают как результат неадекватного управления при эксплуатации.

**Методы оценки могут, в частности, включать в себя:**

- анализ и проверку процесса (процессов) и процедуры (процедур);
- проверку того, что процесс (процессы) и процедура (процедуры) действительно применяются;
- анализ соответствия между представлениями проекта ОО;
- анализ соответствия каждого представления проекта ОО требованиям;

- верификацию доказательств;
- анализ руководств;
- анализ разработанных функциональных тестов и предоставленных результатов;
- независимое функциональное тестирование;
- анализ уязвимостей, включающий предположения о недостатках;
- тестирование проникновения.

Основные принципы ИСО/МЭК 15408 содержат утверждение, что **большее доверие** является результатом приложения *больших усилий* при оценке, и что цель состоит в применении минимальных усилий, требуемых для обеспечения необходимого уровня доверия.

**Повышение уровня усилий может быть основано на:**

- ***области охвата***, т.е. увеличении рассматриваемой части продукта ИТ;
- ***глубине***, т.е. детализации рассматриваемых проектных материалов и реализации;
- ***строгости***, т.е. применении более структурированного и формального подхода.

# 2-й учебный вопрос:

# «Краткий обзор стандарта»

**Функциональный класс**

**Имя класса**

**Представление класса**

**Функциональные семейства**

**Функциональное семейство**

**Имя семейства**

**Характеристика семейства**

**Ранжирование компонентов**

**Управление**

**Аудит**

**Компоненты**

**уровни детализации**:

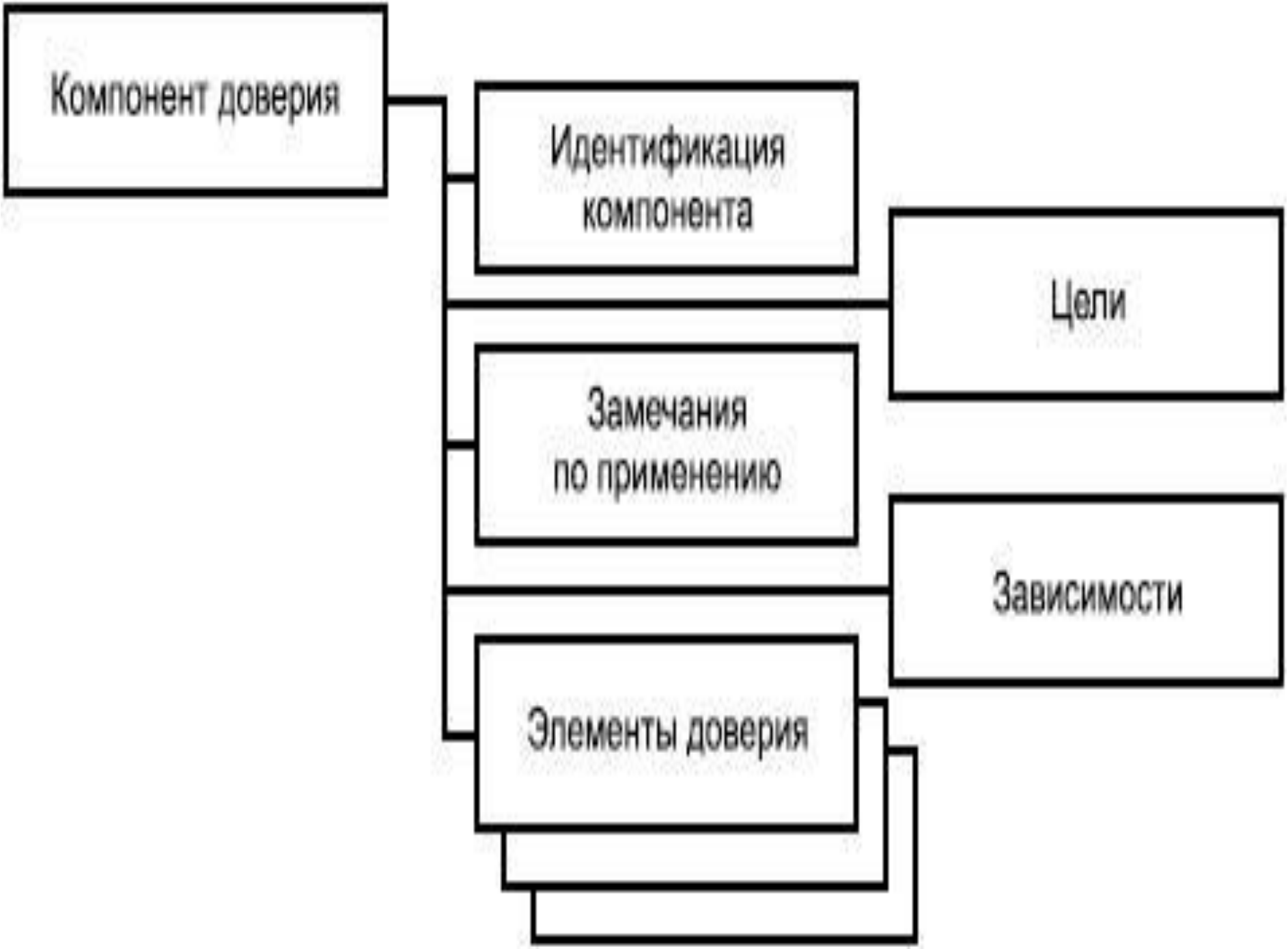
- ***минимальный*** – успешное использование механизма безопасности;
- ***базовый*** – любое использование механизма безопасности, а также информация о текущих значениях атрибутов безопасности.
- ***детализированный*** – любые изменения конфигурации механизма безопасности, включая параметры конфигурации до и после изменения.

Компонент

Имя семейства

Функциональные элементы

Зависимости

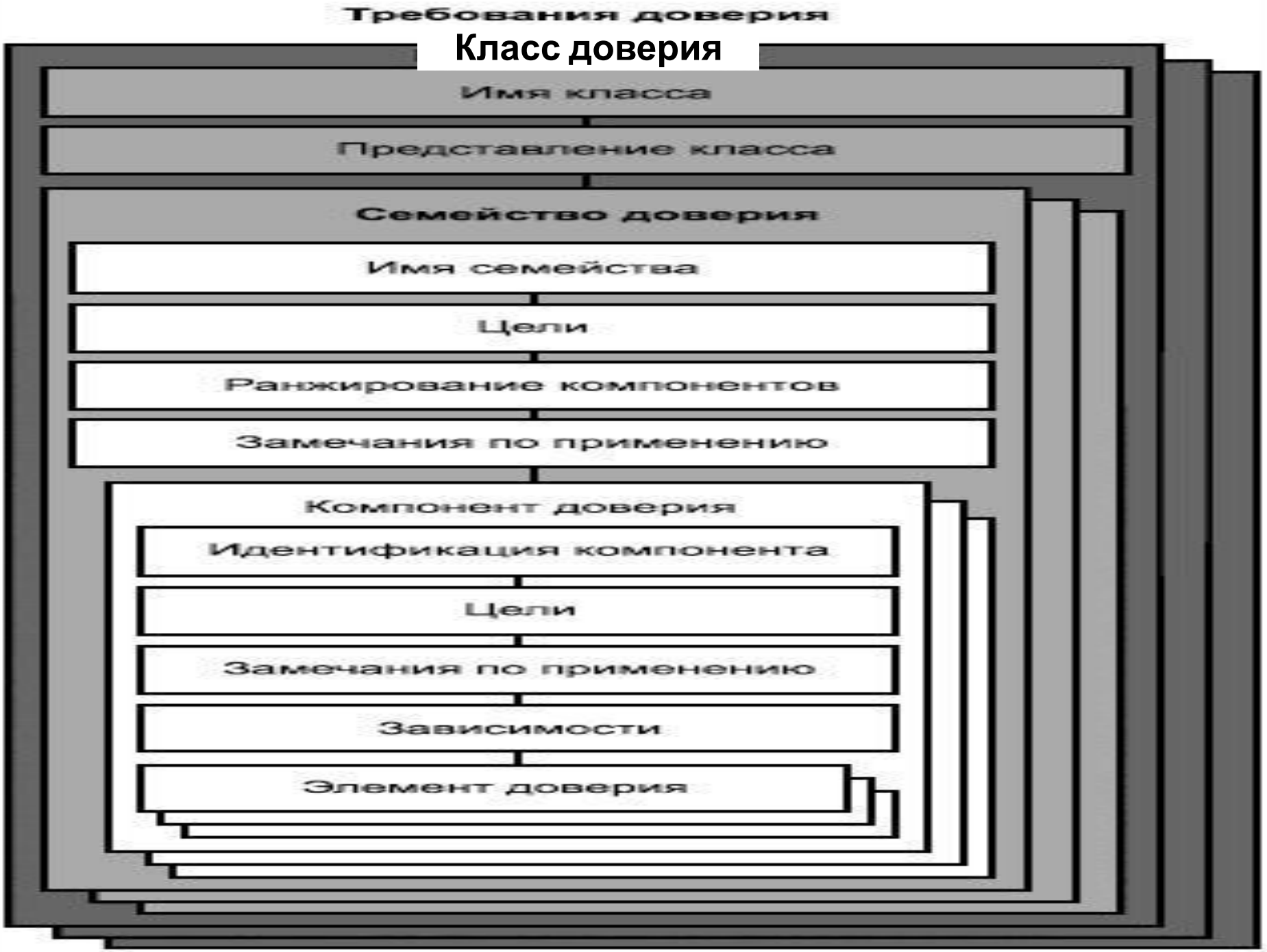

Компонент доверия
Идентификация компонента
Цели
Замечания по применению
Зависимости
Элементы доверия

# Имя класса

## Семейство 1

## Семейство 2

## Семейство 3


Требования доверия
Класс доверия
Имя класса
Представление класса
Семейство доверия
Имя семейства
Цели
Ранжирование компонентов
Замечания по применению
Компонент доверия
Идентификация компонента
Цели
Замечания по применению
Зависимости
Элемент доверия

**Каждый элемент доверия принадлежит к одному из трех типов:**

a) ***Элементы действий разработчика***, определяющие действия, которые должны выполняться разработчиком. Требования к действиям разработчика обозначены ***буквой "D"*** после номера элемента.

b) ***Элементы содержания и представления свидетельств***, определяющие требуемые свидетельства и отражаемую в них информацию. Требования к содержанию и представлению свидетельств обозначены ***буквой "C"*** после номера элемента.

c) ***Элементы действий оценщика***, определяющие действия, которые должны выполняться оценщиком. Требования к действиям оценщика обозначаются ***буквой "E"*** после номера элемента.