

## **3. Общие**

### **критерии**

#### **3.1. Введение**

В России «Общие критерии» приняты в качестве ГОСТ в 2002 году и введёны в действие с 1 января 2004 г. Точное название документа: **ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»**.

Документ состоит из трёх частей:

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

#### **3.2. Основные идеи «Общих критериев»**

**Категории пользователей, которые используют «Общие критерии»:**

##### **1. Потребители.**

ОК позволяют определить, вполне ли оцениваемый продукт или система удовлетворяют их потребностям в безопасности.

##### **2. Разработчики**

Конструкции ОК могут быть использованы для формирования утверждения о соответствии объекта оценки установленным требованиям.

##### **3. Оценщики**

Стандарт может быть использован при формировании заключения о соответствии ПО предъявляемым к ним требованиям безопасности.

# аспекты среды объекта оценки (ОО)

## **Предположения безопасности**

выделяют ОО из общего контекста и задают границы его рассмотрения. Предполагается, что среда ОО удовлетворяет данным предположениям. При проведении оценки предположения безопасности принимаются без доказательств.

## **Угрозы безопасности**

Выделяются угрозы, безопасность которых в рассматриваемой среде установлено или предполагается. Угроза характеризуется следующими параметрами:

- источник угрозы;
- предполагаемый способ реализации угрозы;
- уязвимости, которые являются предпосылкой для реализации угрозы;
- активы, которые являются целью нападения;
- нарушаемые свойства безопасности активов;
- возможные последствия реализации

## **Политики безопасности**

Излагаются положения политики безопасности, применяемые в организации, которые имеют непосредственное отношение к ОО.

## **Цели безопасности для ОО**

## **Требования безопасности**

## **Функциональные требования**

## **Требования доверия**

При формулировании требований к ОО разрабатываются два документа

**Профиль  
защиты**

не зависящая от конкретной реализации совокупность требований информационных технологий для некоторой категории ОО. Профиль защиты (ПЗ) непривязан к конкретному ОО и представляет собой обобщённый стандартный набор функциональных требований и требований доверия для определённого класса продуктов или систем.

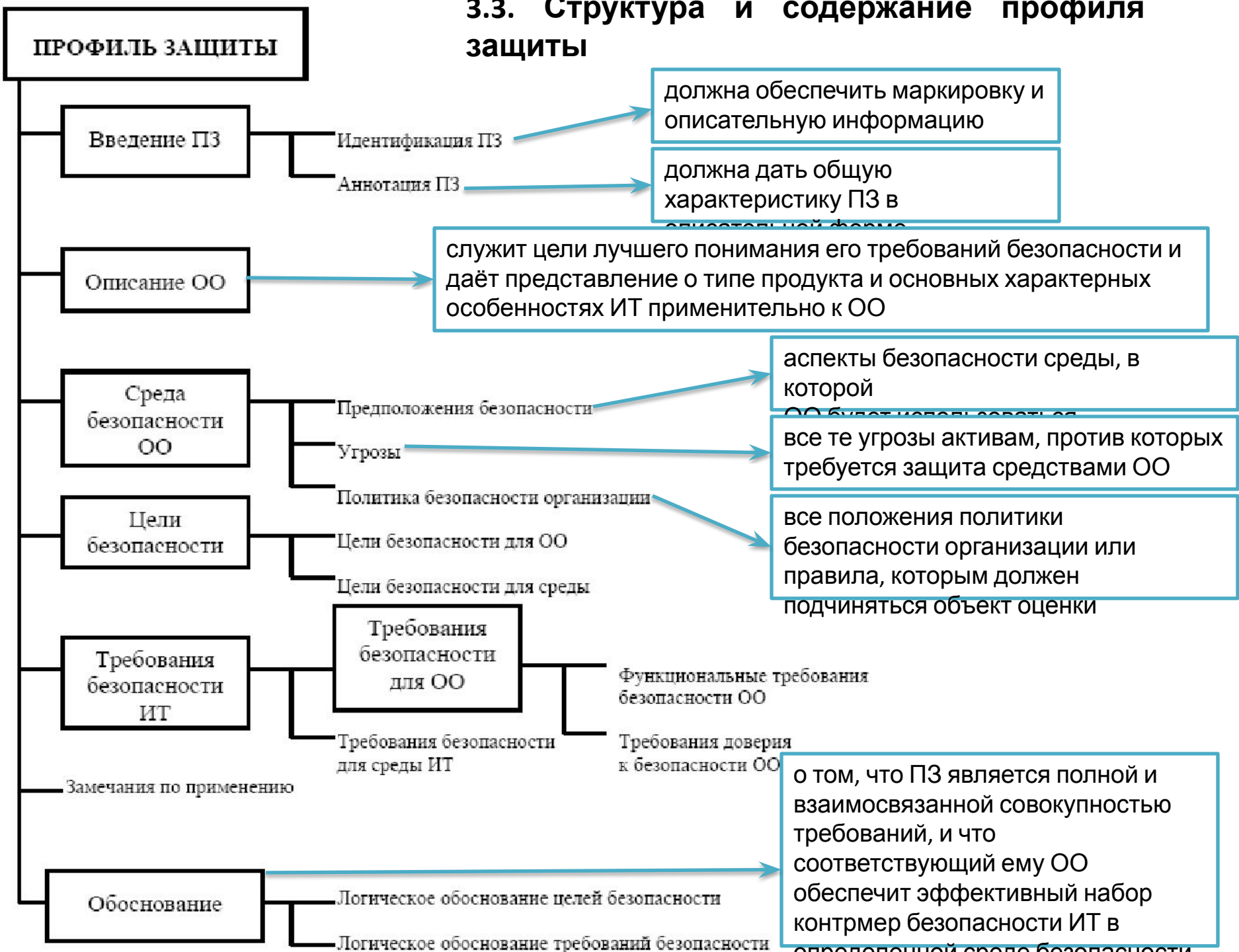
**Задание по  
безопасности**

документ, содержащий требования безопасности для конкретного ОО и специфицирующий функции безопасности и меры доверия, предлагаемые объектом оценки для выполнения установленных требований. В задании по безопасности (ЗБ) может быть заявлено соответствие одному или нескольким профилям защиты. ЗБ можно рассматривать как техническое задание на подсистему обеспечения информационной безопасности для ОО.

### **ограничени**

1. ОК не содержат критериев оценки, касающихся администрирования механизмов безопасности, непосредственно не относящихся к мерам безопасности информационных технологий.
2. Вопросы защиты информации от утечки по техническим каналам, такие как контроль ПЭМИН, непосредственно не затрагиваются, хотя многие концепции ОК потенциально применимы и в данной области.
3. В ОК не рассматриваются ни методология оценки, ни административно- правовая структура, в рамках которой критерии могут применяться органами оценки.
4. Процедуры использования результатов оценки при аттестации продуктов и систем находятся вне области действия ОК.
5. В ОК не входят критерии оценки специфических свойств криптографических алгоритмов.

### 3.3. Структура и содержание профиля защиты



### 3.4. Структура и содержание задания по безопасности





### 3.5. Общие критерии. Сопутствующие

#### документы

Наибольший интерес среди сопутствующих «Общим критериям» материалов представляет документ **«Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий»**, более известный как **«Общая методология оценки» (ОМО)**.

- Объективность
- Беспристрастность
- Воспроизводимость
- Корректность
- Достаточность
- Приемлемость

#### Взаимосвязь между ОК и ОМО



**Процесс оценки** состоит из выполнения оценщиком задачи получения исходных данных для оценки, задачи оформления результатов оценки и подвидов





Результаты оценки оформляются в виде **технического отчёта об оценке** (ТОО), имеющего следующую структуру:

### **1. Введение**

- идентификаторы системы сертификации, разработчика, заявителя, оценщика
- идентификаторы контроля конфигурации ТОО (название, дата, номер версии и т.д.);
- ссылка на ПЗ;

### **2. Описание архитектуры ОО**

- высокоуровневое описание ОО и его главных компонентов.

### **3. Оценка**

- методы, технологии, инструментальные средства и стандарты, применяемые при оценке;
- сведения об ограничениях, принятых при проведении оценки;
- правовые аспекты оценки, заявления о конфиденциальности и т.д.

### **4. Результаты оценки**

Для каждого вида деятельности приводятся

### **5. Выводы и рекомендации**

- общий вердикт;
- рекомендации, которые могут быть полезны для органа по сертификации.

### **6. Перечень свидетельств оценки**

- составитель;
- название;
- уникальная ссылка.

### **7. Перечень сокращений и глоссарий терминов**

### **8. Сообщения о проблемах**

- полный перечень сообщений о проблемах;
- их текущее состояние.

Документ **«Безопасность информационных технологий. Типовая методика оценки профилей защиты и заданий по безопасности»** предназначен для заявителей, испытательных центров (лабораторий) и органов по сертификации проводящих проверку соответствия требованиям «Общих критериев».

Документ **«Руководящий документ Руководство по разработке профилей защиты и заданий по безопасности»** содержит практические рекомендации для разработчиков ПЗ и ЗБ.

**«Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности».** Документ определяет общий порядок разработки, оценки, регистрации и публикации ПЗ и ЗБ.

**«Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты»** Документ определяет порядок ведения реестра профилей защиты.

– **«Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты»** определяет общие принципы безопасности информационных технологий.