5. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»

В 1990 году в Международной организацией стандартов (ISO) была начата работа по созданию международных критериев оценки безопасности компьютерных систем. Результатом явился стандарт «Общие критерии безопасности информационных технологий» (ОК), который на данный момент признается одним из наиболее функциональных стандартов в сфере информационной безопасности (ИБ).

Его разработка велась совместными усилиями США, Канады, Франции, Германии, Нидерландов и Великобритании. В последствии к проекту присоединился ряд других стран. Версия 2.1 ОК в 1999 году была утверждена в качестве международного стандарта ISO/IEC 15408. В России в настоящее время внедряется адаптированная 3 версия стандарта ISO/IEC 15408.

ОК разработаны таким образом, чтобы удовлетворить потребности трех групп специалистов: разработчиков, экспертов по сертификации и пользователей продуктов информационных технологий (ИТ-продуктов). Под ИТ-продуктом понимается программный (или аппаратно-программный) продукт или информационная система. В процессе оценки ИТ-продукт именуется объектом оценки (ОО). К таким объектам относятся, например, операционные системы, вычислительные сети, распределенные системы, прикладные программы.

Стандарт ISO 15408 состоит из трех частей:

- Часть 1. Введение и общая модель.
- Часть 2. Функциональные требования безопасности.
- Часть 3. Гарантийные требования безопасности (вариант перевода - "требования гарантированности").

Как видно из приведенного перечня, "Общие критерии" предусматривают наличие двух типов требований безопасности - функциональных и гарантированности. Функциональные требования относятся к сервисам безопасности, таким как идентификация, аутентификация, управление доступом, аудит и т.д. Требования гарантированности относятся к технологии разработки, тестированию, анализу уязвимостей, поставке, сопровождению, эксплуатационной документации и т.д.

Описание обоих типов требований выполнено в едином стиле: они организованы в иерархию "класс - семейство - компонент - элемент". Термин "класс" используется для наиболее общей группировки требований безопасности, а элемент - самый нижний, неделимый уровень требований безопасности.

Между компонентами могут существовать зависимости. Они возникают, когда компонент недостаточен для выполнения цели безопасности и необходимо наличие другого компонента.

Промежуточная комбинация компонентов названа пакетом. Пакет включает набор требований, которые обеспечивают выполнение многократно используемого поднабора целей безопасности.

Основные структуры "Общих критериев" - это Профиль защиты и Проект защиты.

По определению стандарта ISO/IEC 15408 Профиль Защиты есть независимое от реализации множество требований безопасности для некоторой категории объектов оценки, которые отвечают определенным нуждам потребителей. Профиль состоит из компонентов или пакетов функциональных требований и одного из уровней гарантированности. Структура профиля защиты представлена на рис.2.4.

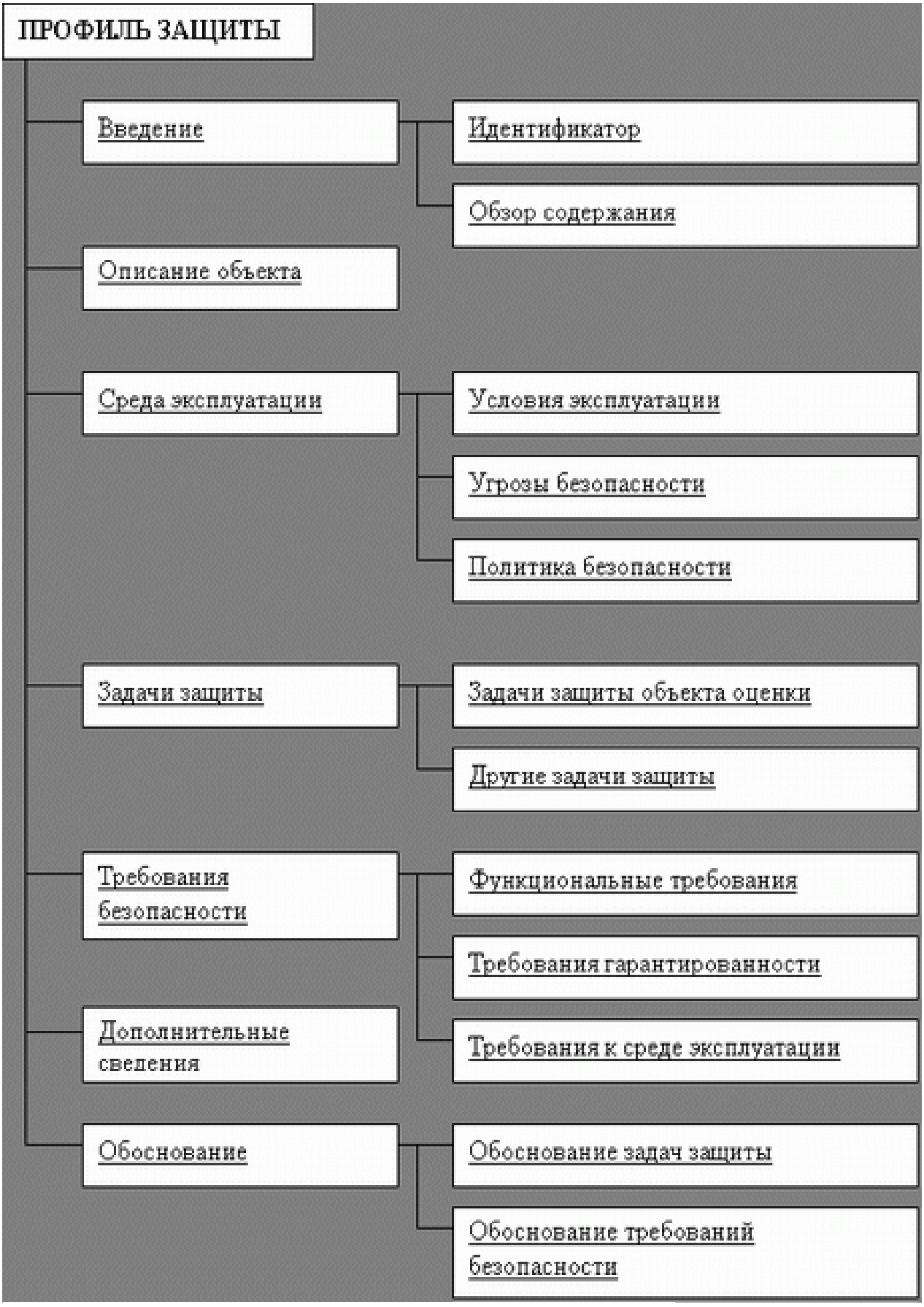

Рис.2.4. Структура профиля защиты.

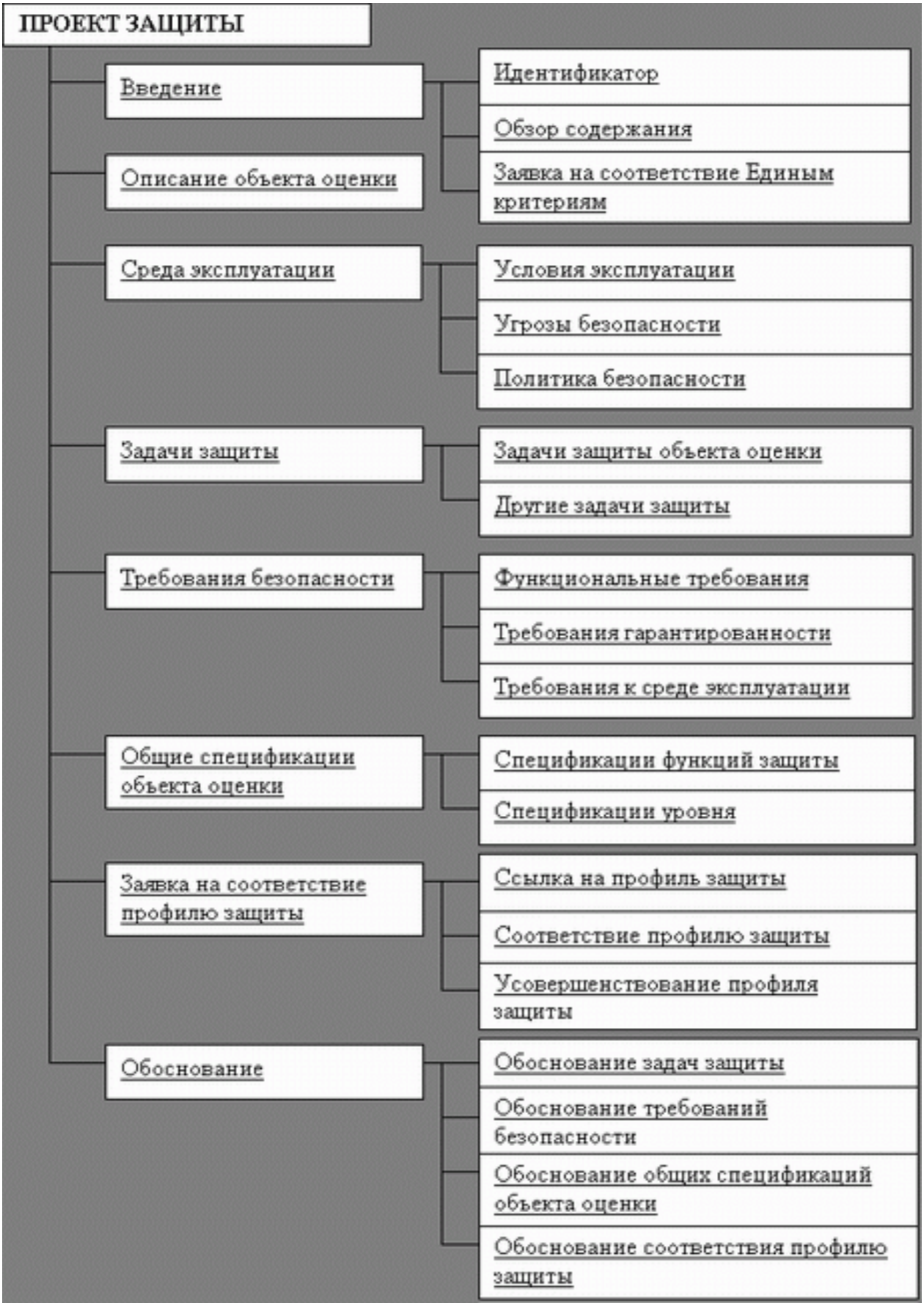

Рис.2.5. Структура Проекта защиты.

Как отмечается в литературе, Профиль защиты "Общих критериев", по сути, является аналогом классов "Оранжевой книги" и классов защищенности РД ГТК РФ, но базируется на значительно более полной и систематизированной совокупности компонентов требований безопасности. Количество стандартизованных профилей общих критериев потенциально не ограничено.

Профиль защиты служит основой для создания Проекта защиты, который является техническим проектом для разработки объекта оценки. Структура Проекта защиты представлена на рис.2.5. В отличие от Профиля, Проект защиты описывает также уровень функциональных возможностей средств и механизмов защиты, реализованных в объекте оценки, и приводит обоснование степени их адекватности.

Для того, чтобы профиль безопасности мог быть эффективно разработан и применен, в процессе его разработки производится выявление всех угроз безопасности осуществимых в отношении ИТ-продуктов, для которых разрабатывается профиль. В процессе исследования строятся модели угроз.

Модель угрозы - это формальное, полуформальное или неформальное описание:

- жизненного цикла угрозы;
- направленности угрозы;
- источника угрозы;
- системы ИТ, подверженной угрозе;
- ИТ и не-ИТ среды изделия ИТ;
- активов, требующих защиты;
- методов, способов и алгоритмов реализации угрозы;
- нежелательных событий;
- анализа рисков и ряда других аспектов.

У процесса описании модели угроз много общего с проведением анализа рисков. Так при описании модели угроз, источником которых является преднамеренная деятельность человека, оценивается тип источника по уровню практических навыков реализации угрозы (шкала - "низкий", "средний", "высокий", "неопределенный"), и шансы реализации угрозы (шкала - "маловероятно", "вероятно", "большая вероятность", "не определено"). Также оценивается вероятность компрометации активов в виде pc(y,z), где y - идентифицированный метод нападения, z - идентифицированный актив.

В рассмотрение вводится понятие "потенциал нападения". Под этим термином понимается прогнозируемый потенциал для успешного, в случае реализации, нападения, выраженный в показателях компетентности, ресурсов и мотивации нарушителя. Существует три уровня потенциала нападения: низкий, умеренный и высокий.

Стандарт определяет функцию безопасности, как часть или части ОО, на которые возлагается реализация тесно связанного подмножества правил из политики безопасности. Функции безопасности характеризуются стойкостью.

Стойкость функции безопасности ОО - это ее характеристика, выражающая минимально необходимое воздействие на ее механизмы безопасности, в результате которого нарушается политика безопасности в части этой функции выделяется базовая, средняя и высокая стойкость.

Базовая стойкость означает, что функция обеспечивает адекватную защиту от случайного нарушения безопасности ОО нарушителем с низким потенциалом нападения.

Средняя стойкость - функция обеспечивает защиту от целенаправленного нарушения безопасности ОО нарушителем с умеренным потенциалом нападения.

Высокая стойкость - такой уровень стойкости функции безопасности ОО, на котором она обеспечивает защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителем с высоким потенциалом нападения.

В литературе описана следующая схема вычисления потенциала нападения, в которой учитываются следующие факторы.

1. **При идентификации уязвимости:**

- время, затрачиваемое на идентификацию уязвимости (x1) ("за минуты", "за часы", "за дни", "за месяцы");
- уровень специальной подготовки (x2) ("эксперт", "специалист", "неспециалист");
- знание проекта и функционирования ОО (x3) ("отсутствие информации об ОО", "общедоступная информация об ОО", "закрытая информация об ОО");

- доступ к ОО (x4) (требуемое время на доступ к ОО, как в случае x1);
- аппаратные средства, программное обеспечение или другое оборудование (x5) ("стандартное оборудование", "специализированное оборудование", "уникальное оборудование").

2. При использовании:

- время, затраченное на использование уязвимости (y1);
- уровень специальной подготовки (y2);
- знание проекта функционирования ОО (y3);
- доступ к ОО (y4);
- аппаратные средства, программное обеспечение или другое оборудование, необходимое для использования уязвимости (y5).

Далее десяти факторам x1-x5 и y1-y5 назначаются веса, и они суммируются. Сумма используется для оценки уязвимости.

Описанный подход раскрывает еще одну "грань" задачи анализа рисков, на которой ранее мы не акцентировали внимание - в ходе анализа необходимо не только оценить возможные потери от реализации угрозы, но и описать модель нарушителя, дать оценку его возможностей по реализации угрозы, что в конечном итоге позволит оценить вероятность атаки на систему.