Дисциплина «Стандарты информационной безопасности»

Стандарт ISO/IEC 15408

асс. Цырульник Валерия Федоровна

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

"Критерии оценки безопасности информационных технологий". Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

Данный стандарт часто называют "Общими критериями" (или даже ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

ОК содержат два основных вида **требований безопасности**:

- **функциональные**, предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия**, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Рисунок 1 - Понятия, используемые при оценке, и их взаимосвязь

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

Безопасность в «Общих критериях» рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка:

- требований безопасности;
- проектирования;
- эксплуатации.

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

В "Общих критериях" введена иерархия **класс-семейство-компонент-элемент**.

- **Классы** определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).
- **Семейства** в пределах класса различаются по строгости и другим нюансам требований.
- **Компонент** - минимальный набор требований, фигурирующий как целое.
- **Элемент** - неделимое требование.

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

- **Профиль защиты (ПЗ)** представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).
- **Задание по безопасности** содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования **доверия безопасности**.

Стандарт ISO/IEC 15408 (Общие критерии, ОК)

- **Функциональный пакет** - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.
- Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Классы функциональных требований (11 классов, 66 семейств, 135 компонентов)

- **идентификация и аутентификация**;
- **защита данных пользователя**;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки**;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);
- **связь** (аутентификация сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

Классы «Приватность» и «Использование ресурсов»

Четыре семейства функциональных требований класса «Приватность»:

1. Анонимность (полная/выборочная).
2. Псевдонимность.
3. Невозможность ассоциации.
4. Скрытность.

Три семейства класса «Использование ресурсов»:

1. Отказоустойчивость (активная/пассивная);
2. Обслуживание по приоритетам;
3. Распределение ресурсов.

Недостатки стандарта ISO/IEC 15408 (Общие критерии, ОК)

Недостатки стандарта ISO/IEC 15408:

1. Отсутствие объектного подхода;

2. Сужается круг фиксируемых знаний;

3. Отсутствие архитектурных требований.

Типы элементов требований доверия

Каждый элемент требований доверия принадлежит одному из трех типов:

- ***действия разработчиков;***
- ***представление и содержание свидетельств;***
- ***действия оценщиков.***

Классы требований доверия (10 классов, 44 семейства, 93 компонента)

- **разработка** (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- **поддержка жизненного цикла** (включая порядок устранения недостатков и защиту среды разработки);
- **тестирование**;
- **оценка уязвимостей** (включая оценку стойкости функций безопасности);
- **поставка и эксплуатация**;
- **управление конфигурацией**;
- **руководства** (требования к эксплуатационной документации);
- **поддержка доверия** (для поддержки этапов жизненного цикла после сертификации);
- **оценка профиля защиты**;
- **оценка задания по безопасности**.

Оценочные уровни доверия

Применительно к **требованиям доверия** в "Общих критериях" введены **оценочные уровни доверия**, содержащие осмысленные комбинации компонентов, что не было реализовано для функциональных требований:

- Оценочный уровень доверия 1 (начальный) предусматривает анализ функциональной спецификации, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.
- Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие проекта верхнего уровня объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.
- На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

Оценочные уровни доверия (продолжение)

- На уровне 4 добавляются полная спецификация интерфейсов, проекты нижнего уровня, анализ подмножества реализации, применение неформальной модели политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.
- Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с демонстрацией соответствия между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.
- На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.
- Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.