Стандарты информационной безопасности: "Общие критерии"

Введение

Цели изучения темы

- изучить основные положения международного стандарта ISO/IEC 15408 по оценке защищенности информационных систем.

Требования к знаниям и умениям

- основное содержание оценочного стандарта ISO/IEC 15408;
- отличия функциональных требований от требований доверия;
- классы функциональных требований и требований доверия.
- Студент должен уметь:
- использовать стандарт для оценки защищенности информационных систем.

Ключевой термин

- Ключевой термин: стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий".
- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. "Общие критерии" – метастандарт, определяющий инструменты оценки безопасности информационных систем и порядок их использования.

Второстепенные термины

- функциональные требования;
- требования доверия.

Требования безопасности к информационным системам

- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам. 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. Именно поэтому этот стандарт очень часто называют "Общими критериями".
- "Общие критерии" являются метастандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.
- Как и "Оранжевая книга", "Общие критерии" содержат два основных вида требований безопасности:
- **функциональные** – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия** – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

- В отличие от "Оранжевой книги", "Общие критерии" не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из требований безопасности, существующих для конкретной организации и/или конкретной информационной системы.
- Очень важно, что безопасность в "Общих критериях" рассматривается не статично, а в привязке к жизненному циклу объекта оценки.
- Угрозы безопасности в стандарте характеризуются следующими параметрами:
- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Принцип иерархии: класс – семейство – компонент – элемент

- Для структуризации пространства требований, 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 тонкостям требований.
- **Компонент** – минимальный набор требований, фигурирующий как целое.
- **Элемент** – неделимое требование.
- Между компонентами могут существовать зависимости, которые возникают, когда компонент сам по себе недостаточен для достижения цели безопасности.
- Подобный принцип организации защиты напоминает принцип программирования с использованием библиотек, в которых содержатся стандартные (часто используемые) функции, из комбинаций которых формируется алгоритм решения.

- "Общие критерии" позволяют с помощью подобных библиотек (компонент) формировать два вида нормативных документов: профиль защиты и задание по безопасности.
- **Профиль защиты** 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.
- Функциональный пакет – это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности.
- **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.

Функциональные требования

Все **функциональные требования** объединены в группы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов. Это гораздо больше, чем число аналогичных понятий в "Оранжевой книге".

"Общие критерии" включают следующие классы функциональных требований:

- 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).

Рассмотрим содержание одного из классов.

Класс функциональных требований "Использование ресурсов" включает три семейства.

- **Отказоустойчивость**. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В стандарте различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.
- **Обслуживание по приоритетам**. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

- **Распределение ресурсов**. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.
- Аналогично и другие классы включают наборы семейств требований, которые используются для формулировки требований к системе безопасности.
- "Общие критерии" – достаточно продуманный и полный документ с точки зрения функциональных требований и именно на этот стандарт безопасности ориентируются соответствующие организации в нашей стране и в первую очередь Гостехкомиссия РФ.

Требования доверия

Вторая форма требований безопасности в "Общих критериях" – требования доверия безопасности.

Установление доверия безопасности основывается на активном исследовании объекта оценки.

Форма представления требований доверия, та же, что и для функциональных требований (класс – семейство – компонент).

Всего в "Общих критериях" 10 классов, 44 семейства, 93 компонента требований доверия безопасности.

Классы требований доверия безопасности:

- Разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации).
- Поддержка жизненного цикла (требования к модели 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.

Применительно к требованиям доверия (для функциональных требований не предусмотрены) в "Общих критериях" введены оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Степень доверия возрастает от первого к седьмому уровню. Так, оценочный уровень доверия 1 (начальный) применяется, когда угрозы не рассматриваются как серьезные, а оценочный уровень 7 применяется к ситуациям чрезвычайно высокого риска.

Выводы по теме

- Стандарт ISO/IEC 15408 "Критерии оценки безопасности информационных технологий" (издан 1 декабря 1999 года) относится к оценочным стандартам.
- "Общие критерии" являются стандартом, определяющим инструменты оценки безопасности информационных систем и порядок их использования.
- "Общие критерии" содержат два основных вида требований безопасности:
  - функциональные – соответствуют активному аспекту защиты – предъявляемые к функциям безопасности и реализующим их механизмам;
  - требования доверия – соответствуют пассивному аспекту – предъявляемые к технологии и процессу разработки и эксплуатации.

- Угрозы безопасности в стандарте характеризуются следующими параметрами:
  - источник угрозы;
  - метод воздействия;
  - уязвимые места, которые могут быть использованы;
  - ресурсы (активы), которые могут пострадать.
- Для структуризации пространства требований 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 тонкостям требований.
- **Компонент** – минимальный набор требований, фигурирующий как целое.
- **Элемент** – неделимое требование.

Вопросы для самоконтроля

1. Какие виды требований включает стандарт ISO/IEC 15408?
2. Чем отличаются функциональные требования от требований доверия?
3. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
4. Какова цель требований по отказоустойчивости информационных систем?
5. Сколько классов функциональных требований?