Тема 5: Стандарты информационной безопасности: "Общие критерии"

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.

- "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.

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.

- "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

- "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).

- 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.

Требования доверия

- **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.

Домашнее задание

Подготовить рефераты.