Стандарты оценки безопасности

Стандарты оценки безопасности компьютерных систем и информационных технологий

Предназначены для:

- пользователей;
- разработчиков;
- оценщиков (специалистов по сертификации).

«Оранжевая книга»

Trusted Computer System Evaluation Criteria.

Введено понятие безопасной компьютерной системы (КС называется безопасной, если она обеспечивает контроль за доступом к информации так, что только уполномоченные пользователи и процессы, действующие от их имени, имели право читать, писать, создавать или уничтожать информацию).

«Оранжевая книга»

Введены три группы требований к защищенности компьютерных систем:

- Политика (наличие и реализация набора правил разграничения доступа на основе мандатного или дискреционного управления доступом).
- Подотчетность (идентификация и аутентификация субъектов доступа, аудит событий, связанных с безопасностью).
- Доверие (гарантии обеспечения требований безопасности, постоянство защиты).

«Оранжевая книга»

Введены 4 группы и 7 классов защищенности компьютерных систем.

- Группы D (минимальная защита), C (дискреционная защита), B (мандатная защита), A (верифицированная защита).
- Класс D1 (зарезервирован для КС, не аттестованных на другие классы).
- Классы C1 и C2 (по сравнению с C1 дополнительно требуются возможность определения прав доступа для каждого отдельного пользователя и поддержка аудита).

«Оранжевая книга»

- Классы B1, B2, B3 (постоянное нарастание требований в рамках мандатного разграничения доступа).
- Класс A1 (формальная модель политики безопасности, доказательство ее соответствия своим аксиомам и достаточности аксиом, формальная высокоуровневая спецификация подсистемы защиты и демонстрация ее соответствия модели политики безопасности, неформальное подтверждение элементов подсистемы защиты ее высокоуровневой спецификации).

Руководящие документы ФСТЭК (ГТК) по защите от НСД к информации

- Отдельно рассматривается защищенность средств вычислительной техники (СВТ) и автоматизированных систем (АС).
- При оценке защищенности АС рассматриваются дополнительные характеристики: полномочия пользователей, модель нарушителя, технология обработки информации.

Классы защищенности СВТ

- 7 классов (по аналогии с «оранжевой книгой»).
- Классы 6 и 5 предполагают реализацию дискреционного разграничения доступа к объектам. Классы 4, 3, 2 и 1 – мандатного.
- Начиная с класса 2 требуется обеспечить контроль установки и модификации СВТ.
- Всего 21 показатель защищенности СВТ.

Группы защищенности АС

- Группа 3 (однопользовательские АС с информацией одного уровня конфиденциальности).
- Группа 2 (многопользовательские АС с одинаковыми полномочиями пользователей и с информацией разного уровня конфиденциальности).
- Группа 1 (многопользовательские АС с разными правами пользователей и с информацией разного уровня конфиденциальности).

Классы защищенности АС

- Классы 3Б и 3А.
- Классы 2Б и 2А.
- Классы 1Д, 1Г, 1В, 1Б, 1А. Класс 1Г примерно соответствует классу С2 по классификации «оранжевой книги».

Стандарты первого поколения

- Ориентация на системы силовых структур.
- Ориентация на противодействие в основном попыткам несанкционированного доступа (нарушения конфиденциальности).
- Использование единой жесткой шкалы оценки степени защищенности.

Структура требований безопасности

- Элемент (неделимое требование безопасности).
- Компонент (набор элементарных требований безопасности, выбираемых совместно для включения в профиль защиты или задание по безопасности),
- Семейство (группировка компонентов, обеспечивающих выполнение отдельных целей безопасности).
- Класс (объединение семейств, разделяющих общие цели безопасности).