Лекция 9. Методы оценки защищенности компьютерных систем

1. Требования к обеспечению безопасности информационных систем в США.
2. Требования к обеспечению безопасности информационных систем в России.
3. Критерии оценки безопасности информаци-онных технологий.

- Для оценки ЗИ в АС вводится некоторая система показателей защищенности ИС и задается иерархия классов безопасности.
- Каждому классу соответствует определенная совокупность обязательных функций ЗИ.
- Степень реализации выбранных критериев показывает текущее состояние безопасности.
- Последующие действия сводятся к сравнению реальных угроз с реальным состоянием безопасности.
- Если реальное состояние ЗИ перекрывает угрозы в полной мере, система БИ считается надежной и не требует дополнительных мер. Такую систему можно отнести к классу систем с полным перекрытием угроз и КУИ. В противном случае система безопасности нуждается в дополнительных мерах защиты.

Показатель защищенности ИС - характеристика средств системы, влияющая на защищенность и описываемая определенной груп-пой требований, варьируемых по уровню и глубине в зависимости от класса защищенности.

1.Требования к обеспечению безопасности информационных систем в США.

Национальный центр компьютерной безопасности МО США (NCSC - National Computer Security Center): вопросы стандартизации и разработки нормативных требований на защиту информации.

1983 г.: «Критерии оценки безопасности компьютер-ных систем» (Trasted Computer Systems Evaluation Criteria - TCSEC)- «Оранжевая книга».

NCSC считает безопасной систему, которая «посредст-вом специальных механизмов защиты контролирует дос-туп к информации таким образом, что только имеющие соответствующие полномочия лица или процессы, выпол-няющиеся от их имени, могут получить доступ на чтение, запись, создание или удаление информации».

Стандартом предусмотрено 6 фундаментальных требований. Они разделены на группы.

1.Стратегия

1 – наличие четко определенной стратегии обеспечения безопасности.

2 - маркировка: управляющие доступом метки должны быть связаны с объектами.

2.Подотчетность

3 - идентификация: индивидуальные субъекты должны идентифицироваться.4 - подотчетность: контрольная информация должна храниться отдельно и защищаться.

3.Гарантии

5 - гарантии: ВС в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку уровня гарантий того, что система обеспечивает выполнение изложенных выше требований с 1-го по 4-е.

6 - постоянная защита: механизмы защиты сами должны быть постоянно защищены от «взламывания» и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают АС, они разделены на 4 группы - D, C, B, A, которые названы так:

- D - минимальная защита;
- C - индивидуальная защита;
- B - мандатная защита;
- A - верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс D, к группе C - два класса C1 и C2, к группе B - три класса B1, B2 и B3, к группе A - один класс A1 с выделением части систем вне класса.

2. Требования к безопасности информационных систем в России

- РД ФСТЭК: «Классификация АС и требований по ЗИ» от 1992 г.
- РД ФСТЭК: «АС. Защита от НСД к информации. Классификация АС и требо-вания по ЗИ », разделяет АС на классы по условиям их функционирования.

Дифференциация подхода к выбору мер и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качествен-ному составу пользователей и обслуживающего персонала.

Этапы классификации АС :

- обследование АС;
- выявление основных признаков АС для классификации;
- сравнение выявленных признаков АС с классифицирующими;
- присвоение АС соответствующего класса защиты от НСД.

К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- наличие в АС информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа АС на доступ к КИ;
- режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается **девять классов ЗИ** АС от НСД, каждый определя-ется минимальной совокупностью требований по ЗИ. Классы под-разделяются на три группы по особенностям и ОИ в АС.

В пределах каждой группы соблюдается иерархия требований по ЗИ в зависимости от ценности (конфиденциальности) информа-ции и, сл-но, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользо-ватель, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в кото-рых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

3 Критерии оценки безопасности информационных технологий

РД: «Критерии оценки безопасности информационных технологий. » от 2002г., содержит систематизированный каталог требований к БИТ, порядок и методические рекомендации по его использованию при задании требова-ний, разработке, оценке и сертификации продуктов и систем ИТ по требова-ниям БИ. РД не отменяет ранее принятые РД в развитие РД ФСТЭК России по защите информации от НСД и соответствует ГОСТ Р ИСО/МЭК 15408 -2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности ИТ ».

Под БИТ РД рассматривает состояние ИТ, определяющее защищен-ность информации и ресурсов ИТ от действия объективных и субъектив-ных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения непри-млемого ущерба субъектам информационных отношений.

Доверие к БИТ обеспечивается как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, прове-дением

конец