**Лекция 9**

# **Классификация автоматизированных систем (АС) по требованиям ИБ**

# Классификация осуществляется на основании Руководящего документа (РД): «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утверждено решением председателя государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года.

Основные этапы классификации автоматизированных систем (АС):  
  
- разработка и анализ исходных данных;  
  
- выявление основных признаков АС, необходимых для классификации;  
  
- сравнение выявленных признаков АС с классифицируемыми;  
  
- присвоение АС соответствующего класса защиты информации oт несанкционированного доступа (НСД).

Исходные данные для проведения классификации АС:  
  
- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;  
  
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;  
  
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;  
  
- режим обработки данных в АС.

Выбор класса АС производится заказчиком и разработчиком с привлечением специалистов по защите информации. К числу определяющих признаков, по которым производится группировка АC в различные классы, относятся:  
  
- наличие в АС информации различного уровня конфиденциальности;  
  
- уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;  
  
- режим обработки данных в АС - коллективный или индивидуальный.

**Документы ФСТЭК РФ** устанавливают **9 классов** защищенности АС от НСД. Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются **на три группы**, отличающиеся особенностями

обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Группы отличаются особенностями обработки информации в АС (см. рис. 1).

**Первая группа** включает многопользовательские АС, в которых 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.

**Вторая группа** включает АС, в которых пользователи имеют одинаковые

права доступа (полномочия) ко всей информации АС, обрабатываемой и

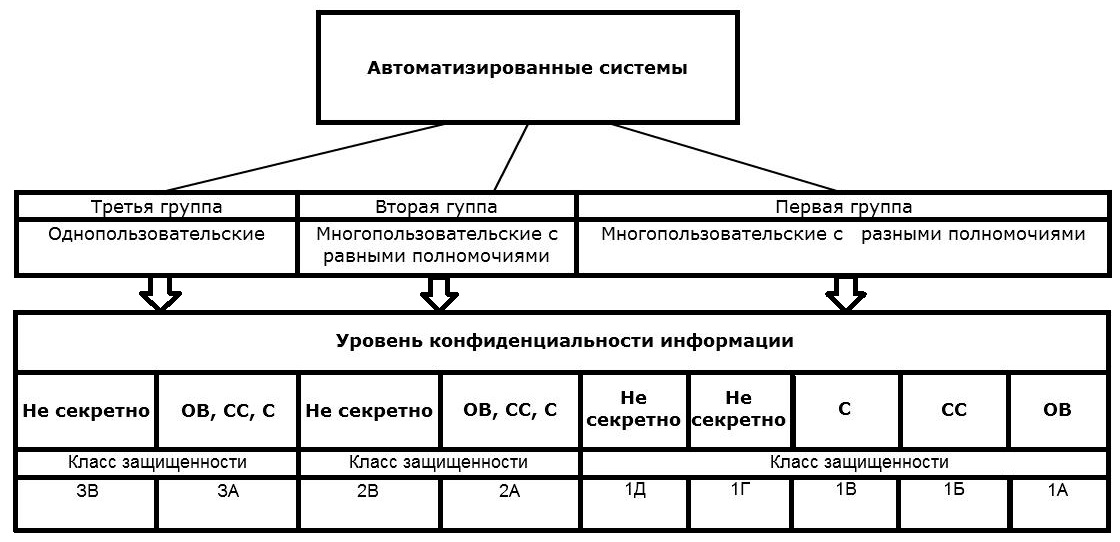
(или) хранимой на носителях различного уровня конфиденциальности.

Группа содержит два класса - 2Б и 2А

**Третья группа** включает АС, в которых работает один пользователь,

допущенный ко всей информации АС, размещенной на носителях одного

уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.



С – секретно, СС – сов. секретно, ОВ – особой важности

Рис. 1 – Классы защищенности АС от НСД

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД

реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;

- регистрации и учета;

- криптографической;

- обеспечения целостности.