Стандарты по оценке защитных систем

стандарты и спецификации двух разных видов:

- оценочные стандартов, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;
- технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Стандарт Министерства обороны США опубликован в августе 1983 года "Критерии оценки доверенных компьютерных систем".

"Оранжевая книга"

Стандарт Министерства обороны США

абсолютно безопасных систем не существует

оценивается лишь степень доверия, которую можно оказать той или иной системе

Система - система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Степень доверия оценивается по двум основным критериям:

- 1). политика безопасности
- 2). уровень гарантированности

Руководящие документы Гостехкомиссии России:

- Классификация автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и
- Классификация межсетевых экранов (МЭ).

Требования к защищенности автоматизированных систем

Подсистемы и требования	Классы								
	3 Б	3 А	2 Б	2 А	1 Д	1 Г	1 В	1 Б	1 А
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+

Классификация межсетевых экранов

Основной критерий классификации МЭ служит протокольный уровень, на котором осуществляется фильтрация информации.

Чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Дискреционная политика безопасности- политика безопасности осуществляемая на основании заданного администратором множества разрешенных отношений доступа.

Дискреционное управление доступом определяется двумя свойствами:

- все субъекты и объекты должны быть идентифицированы;
- права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила.

Достоинства

- относительно простая реализация соответствующих механизмов защиты.

Недостаток

- статическая система

Мандатная политика безопасности – политика безопасности основанная на совокупности предоставления доступа, определенного на множестве атрибутов безопасности субъекта и объекта.

Основа - мандатное управление доступом, которое подразумевает, что:

- все субъекты и объекты системы должны быть однозначно идентифицированы;
- задан линейно упорядоченный набор меток секретности;
- каждому объекту системы присвоена метка секретности, определяющая ценность содержащейся в нем информации - его уровень секретности в АС;
- каждому субъекту системы присвоена метка секретности, определяющая уровень доверия к нему в АС

Основная цель мандатной политики безопасности - предотвращение утечки информации от объектов с высоким уровнем доступа к объектам с низким уровнем доступа, т.е. противодействие возникновению в АС информационных каналов сверху вниз.

Достоинство МПБ – более высокая степень надежности, правила ясны и понятны.

Недостатки – реализация систем с политикой безопасности данного типа довольно сложна и требует значительных ресурсов вычислительной системы.