

Распознавание и контроль поведения пользователя

Определения:

***Объект** – элемент системы, обладающий свойством хранения информации;*

***Субъект** (пользователь) – элемент системы, обладающий свойством управления процессами хранения и обработки информации*

Два основных доступа к объекту

1. Доступ на чтение



Если субъект **S** получает доступ к объекту **O** на чтение, то это означает, что производится перенос информации от **O** к **S**;

2. Доступ на запись



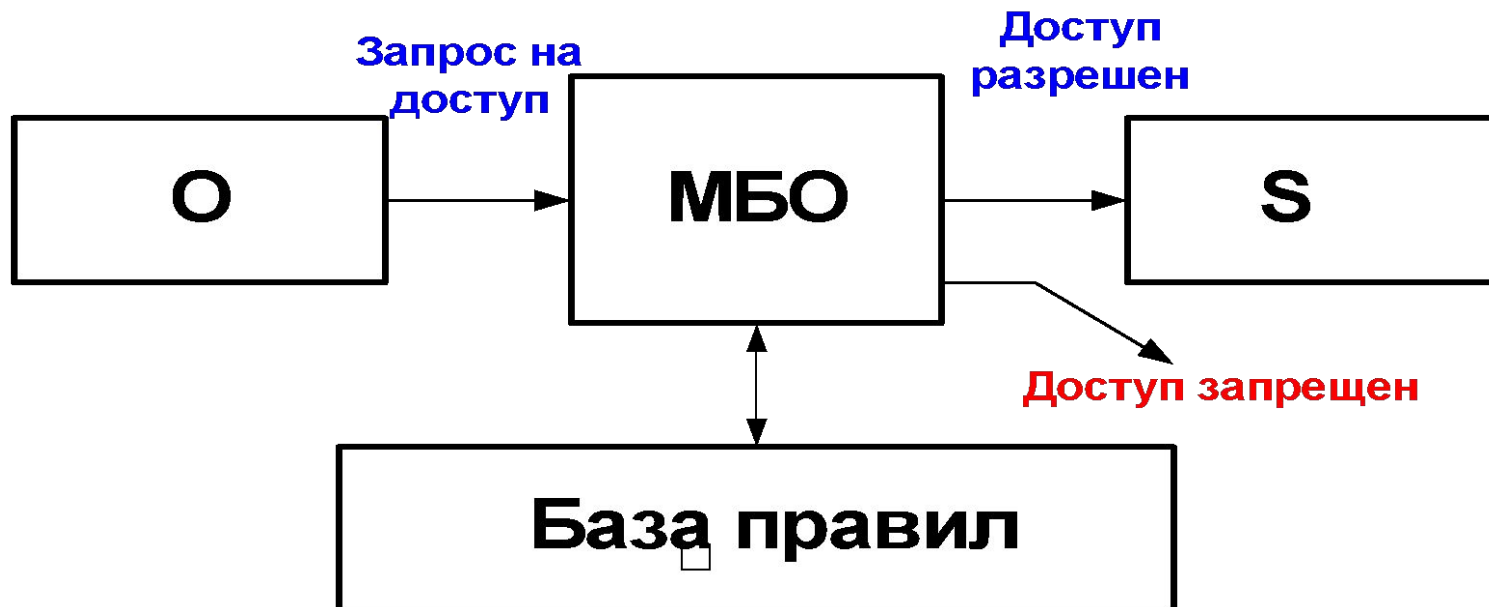
Если субъект **S** получает доступ к объекту **O** на запись, то это означает, что производится перенос информации от **S** к **O**;

3. Также существует и модификация доступа в виде **доступа на активизацию процесса в О**

Положение: Все вопросы безопасности информации описываются доступами субъектов к объектам (правами на управление чтением или записью)

Монитор безопасности обращений (МБО)

- это фильтр, который разрешает или запрещает доступ, основываясь на установленных в системе правилах разграничения доступа



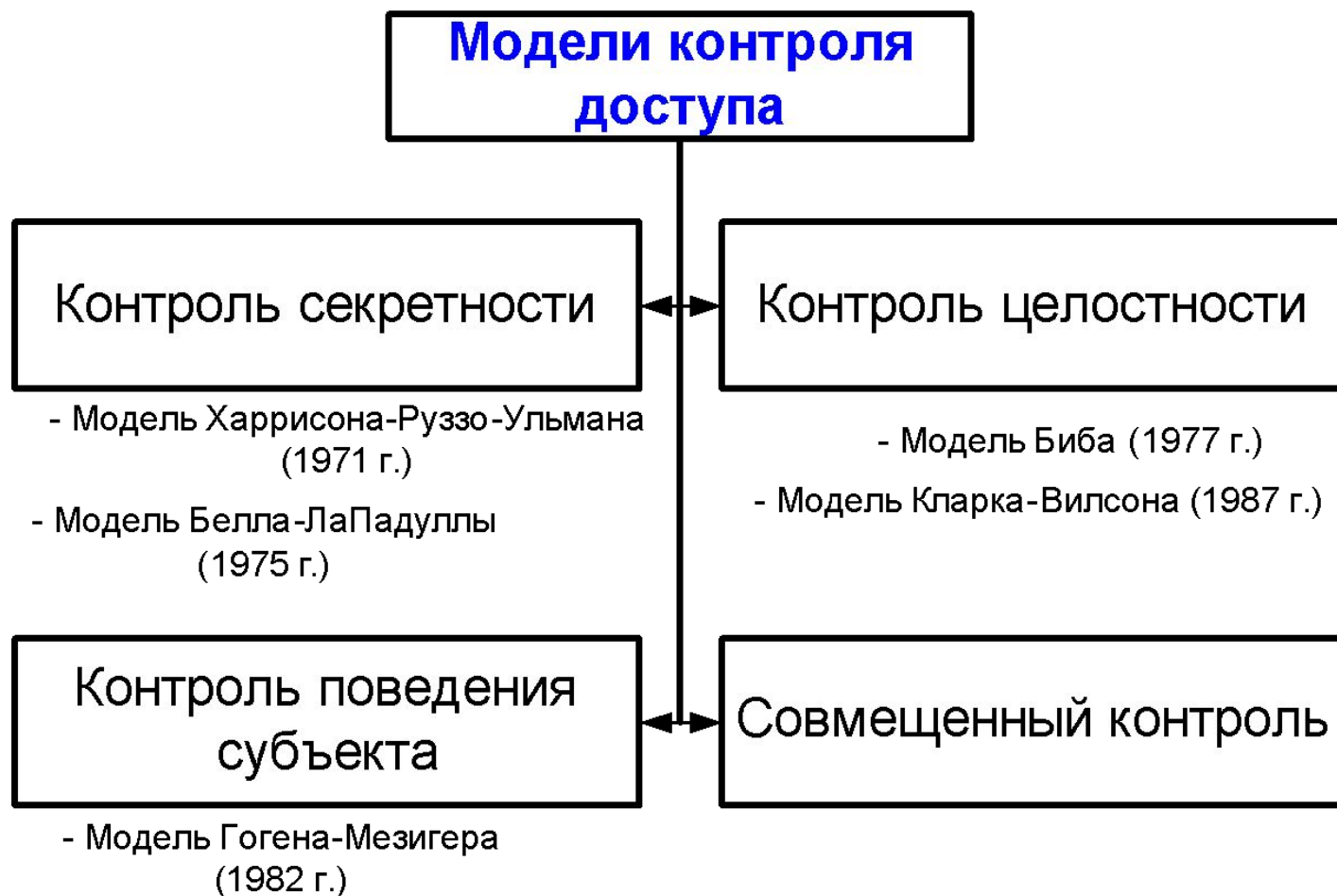
Требования к МБО:

- 1. Ни один запрос на доступ не должен выполняться в обход МБО***
- 2. Работа МБО должна быть защищена от постороннего вмешательства;***
- 3. Представление МБО должно быть простым для возможности верификации его работы***

Формальные модели управления доступом

Классификация моделей

1. По назначению



Матрица доступа

объекты субъекты	o1	o2	on
s1		r				
s2	r,w			r		w
...		r,w				
sm			w			