

Аксиомы и определения доступа субъектов к объектам

Пусть A – конечный алфавит, A^* – множество слов конечной длины в алфавите A , $L \subset A^*$ – язык, т.е. множество слов, выделенных по определённым правилам из A^* .

Аксиома 1. Любая информация в автоматизированной системе представляется словом в некотором языке L .

Виды доступа

- **чтение** – если субъект S получает доступ к объекту O на чтение, то это означает, что производится перенос информации от объекта O к субъекту S – или, возникает информационный поток от O к S ;
- **запись** – если субъект S получает доступ к объекту O на запись, то производится перенос информации от субъекта S к объекту O , т.е. возникает информационный поток от S к O .

Аксиома 2. Все вопросы безопасности информации описываются доступами субъектов к объектам.

Разграничение доступа

Под *разграничением доступа* принято понимать установление полномочий субъектов для последующего контроля санкционированного использования ресурсов, доступных в системе.

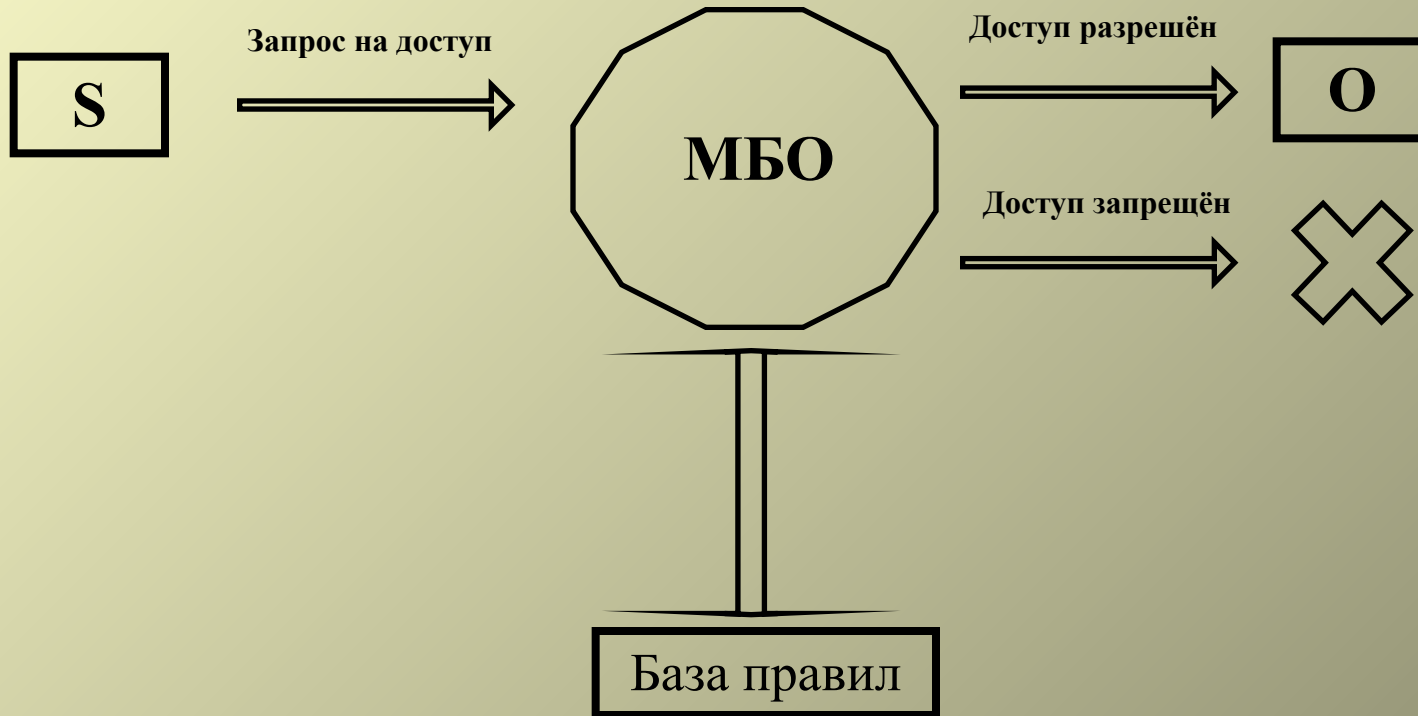
Методы разграничения доступа

- дискреционное;
- мандатное.

Схема матрицы доступа



Монитор безопасности обращений



Свойства МБО

- **ни один запрос на доступ субъекта к объекту не должен выполняться в обход МБО**
- **работа МБО должна быть защищена от постороннего вмешательства**
- **представление МБО должно быть достаточно простым для возможности верификации корректности его работы**