Основы формальной теории защиты информации

Положение 1. Любая информация в автоматизированной системе (АС) представляется словом на языке ***L***

Пусть А- конечный алфавит;

А1 – множество слов конечной длины в алфавите А;

L, принадлежащее А1, - язык для описания процессов;

Определения:

Объект – элемент системы, обладающий свойством хранения информации;

Субъект – 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

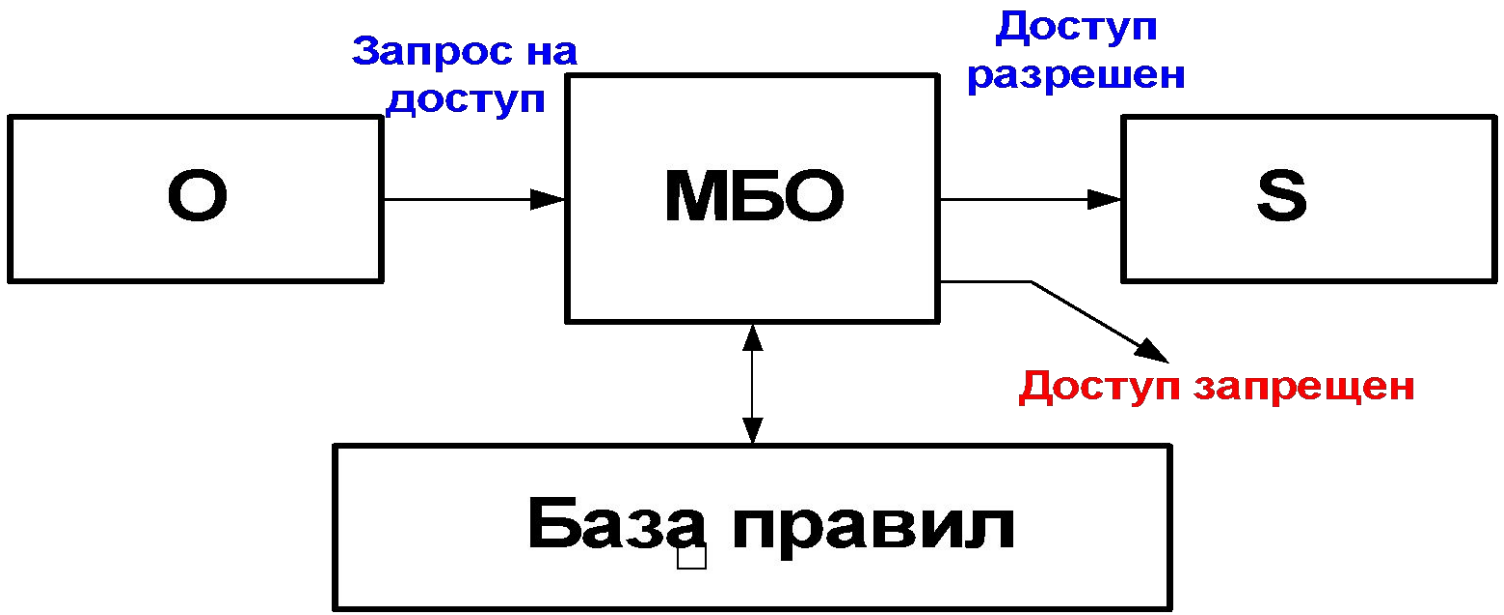
Если субъект ***S*** получает доступ к объекту ***O*** на запись, то это означает, что производится перенос информации от ***S*** к ***O;***

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

Положение 2. 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

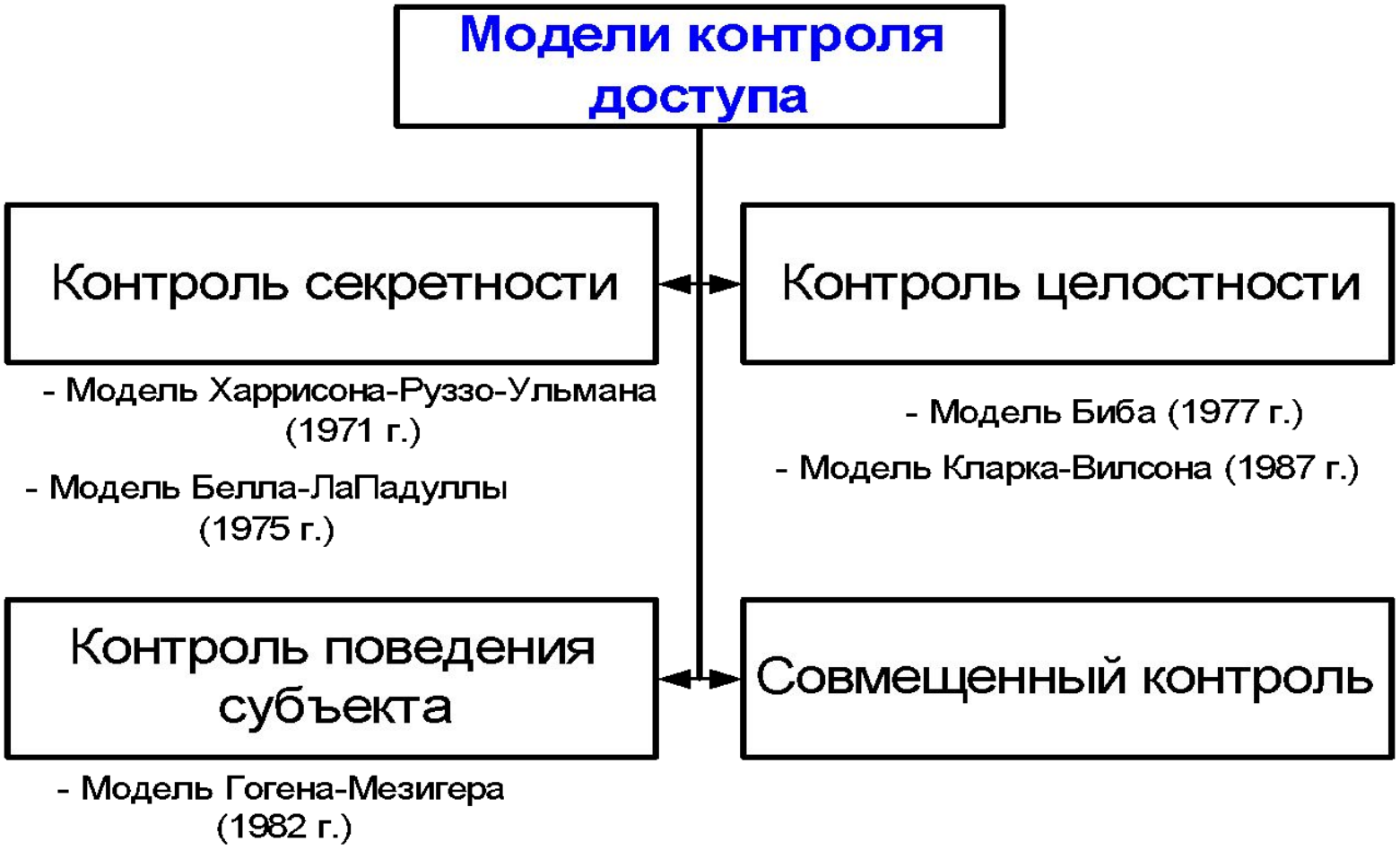


Требования к МБО:

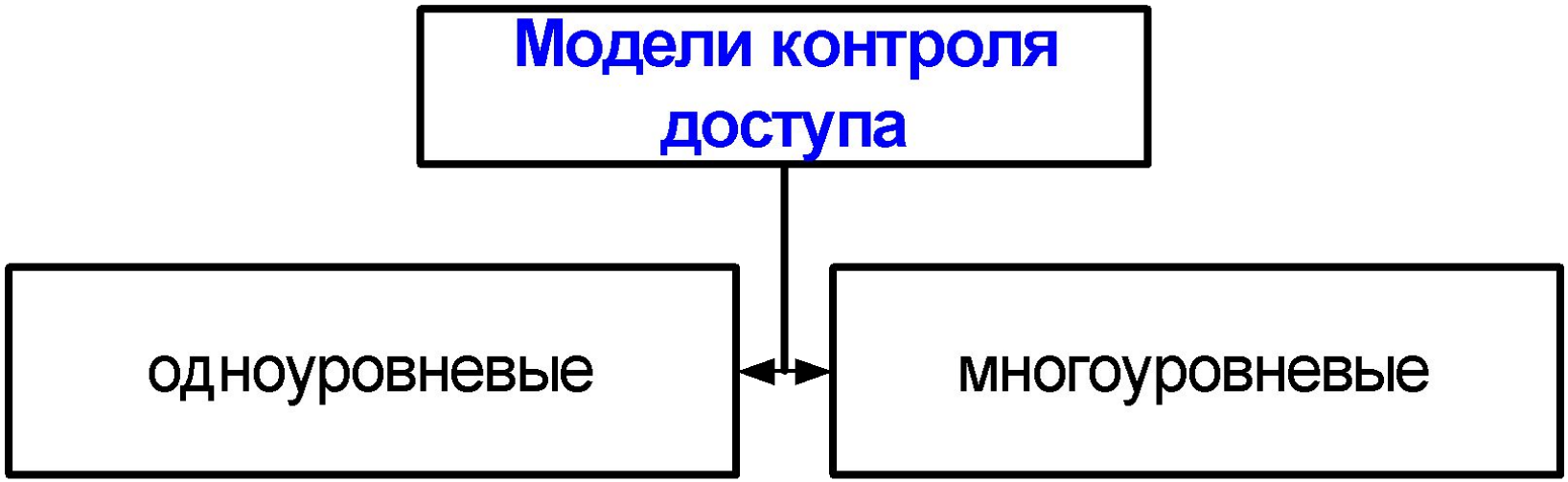
1. *Ни один запрос на доступ не должен выполняться в обход МБО*
2. *Работа МБО должна быть защищена от постороннего вмешательства;*
3. *Представление МБО должно быть простым для возможности верификации его работы*

Формальные модели управления доступом
Классификация моделей

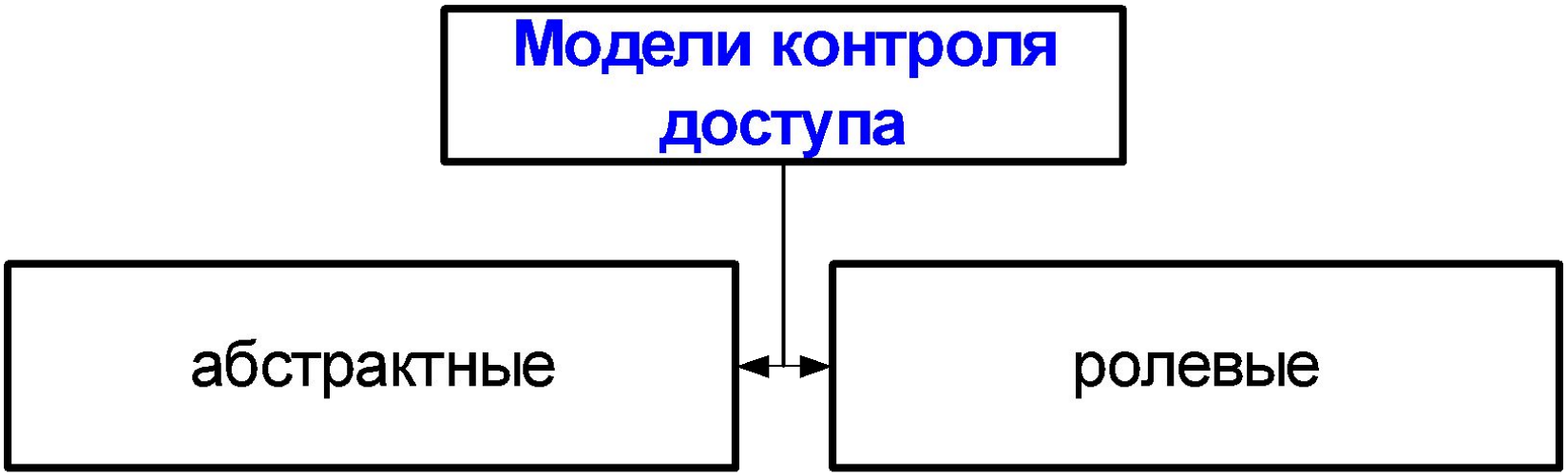
1. По назначению



2. По числу уровней секретности



3. По степени абстракции



- Модель Харрисона-Руззо-Ульмана

Модель Харрисона-Руззо-Ульмана (1971 г.)

Разработана в виде матрицы доступа и правил ее преобразования, описывающей права доступа субъектов к объектам.

Введем обозначения:

S – множество субъектов АС;

O – множество объектов АС;

R={r1,r2, …, rk} – множество прав доступа;

O x S x R – пространство состояний системы;

M – матрица прав доступа;

Q(S,O,M) – текущее состояние системы;

M(s,o) – ячейка матрицы, содержащая набор прав доступа субъекта ***s*** из ***S*** объекту ***o*** из ***O.***

Матрица доступа

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

Переходы состояний матрицы выполняются по следующим 6 командам:

1. *Добавление права субъекту*
2. *Лишение права субъекта*
3. *Создание нового субъекта*
4. *Удаление существующего субъекта*
5. *Создание нового субъекта*
6. *Удаление существующего субъекта*

ФОРМАЛЬНОЕ ОПИСАНИЕ СИСТЕМЫ В МОДЕЛИ ХАРРИСОНА-РУЗЗО-УЛЬМАНА

Система состоит из следующих ***элементов***:

- Конечный набор прав доступа $R=\{r1, r2, \dots, rn\}$;
- Конечный набор исходных субъектов $S0=\{s1, s2, \dots, sm\}$;
- Конечный набор исходных объектов $O=\{o1, o2, \dots, ok\}$;
- Конечный набор команд C;
- Исходная матрица доступа $M0$.

Поведение системы в дискретном времени рассматривается как последовательность состояний $\{Q_i\}, i=1,2 \dots$.

Каждое последующее состояние является результатом применения некоторой команды по отношению к ***элементам*** предыдущего состояния:

$Q_{n+1} = c_n(Q_n)$.

Для заданной системы начальное состояние $Q_0=\{S_0, Q_0, M_0\}$ называется безопасным относительно права r, если не существует применимой к Q_0 последовательности команд, в результате выполнения которой право r будет занесено в ячейку матрицы M, в которой оно отсутствовало в состоянии Q_0.

Иначе: субъект никогда не получит право доступа r к объекту, если он не имел его изначально.

Если же право r оказалось в ячейке матрицы M, в которой оно изначально отсутствовало, то говорят, что произошла утечка права r.

МОДЕЛЬ БЕЛЛА-ЛА ПАДУЛЛЫ

Предложена в 1975 году для формализации механизмов мандатного управления доступом.

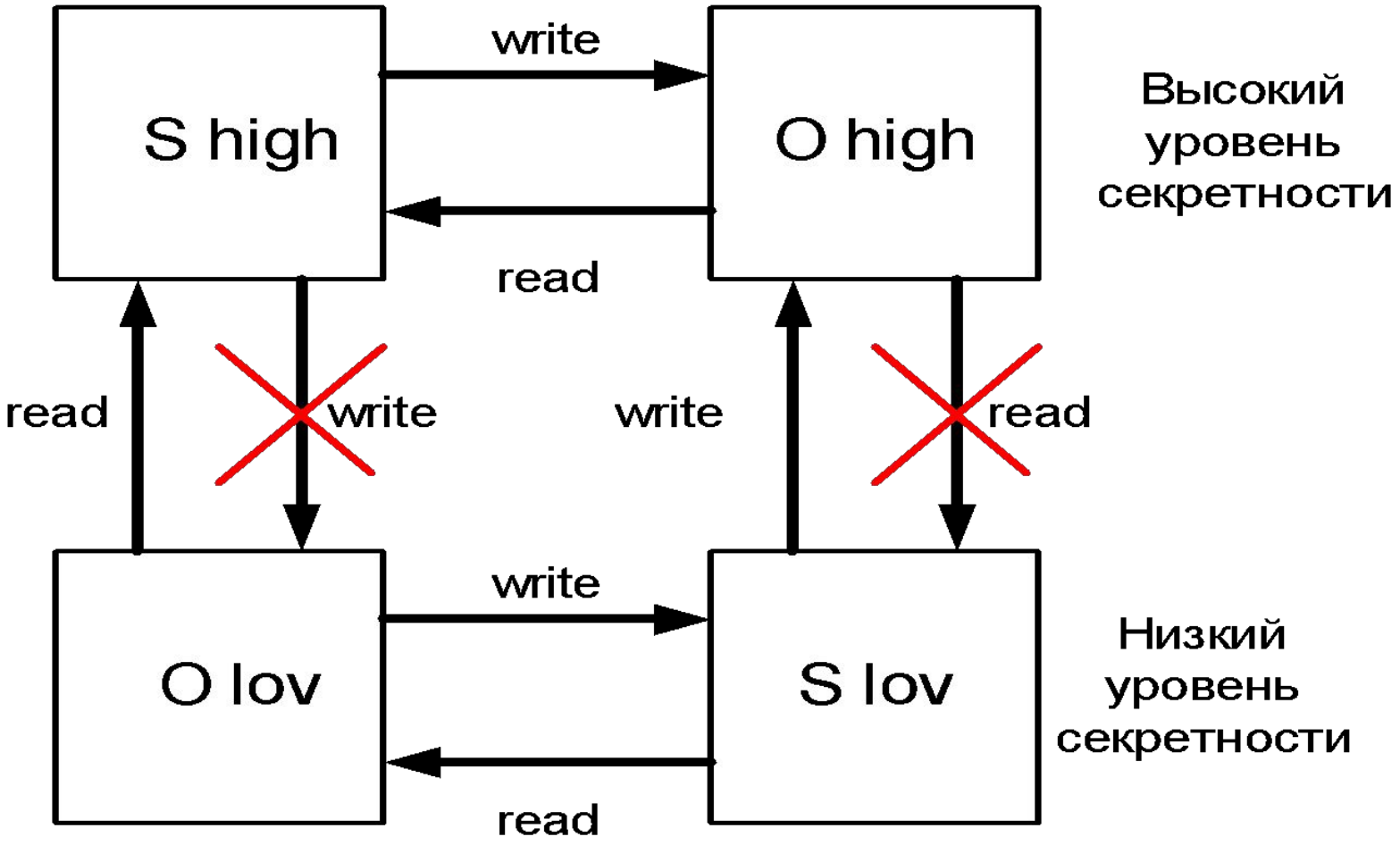
В модели Белла-ЛаПадуллы субъекты и объекты распределяются по грифам секретности.

При этом выполняются следующие правила:

1. Субъект с уровнем секретности ***xs*** может читать информацию из объекта с уровнем секретности ***xo*** тогда и только тогда, когда ***xs*** преобладает над ***xo***;

2. Субъект с уровнем секретности ***xs*** может писать информацию в объект с уровнем секретности ***xo*** тогда и только тогда, когда ***xo*** преобладает над ***xs.***

Схема информационных потоков в модели Белла-ЛаПадулы



МОДЕЛЬ БИБА

Разработана в 1977 году как модификация модели Белла-ЛаПадулы, ориентированная на обеспечение целостности данных.

Базовые правила модели Биба:

1. Простое правило целостности:

   Субъект с уровнем целостности ***xs*** может читать информацию из объекта с уровнем целостности ***xo*** тогда и только тогда, когда ***xo*** преобладает над ***xs***;

2. Правило 2.

   Субъект с уровнем целостности ***xs*** может писать информацию в объект с уровнем целостности ***xo*** тогда и только тогда, когда ***xs*** преобладает над ***xo***;

Схема информационных потоков в модели Биба