Программно-аппаратные средства обеспечения информационной безопасности.

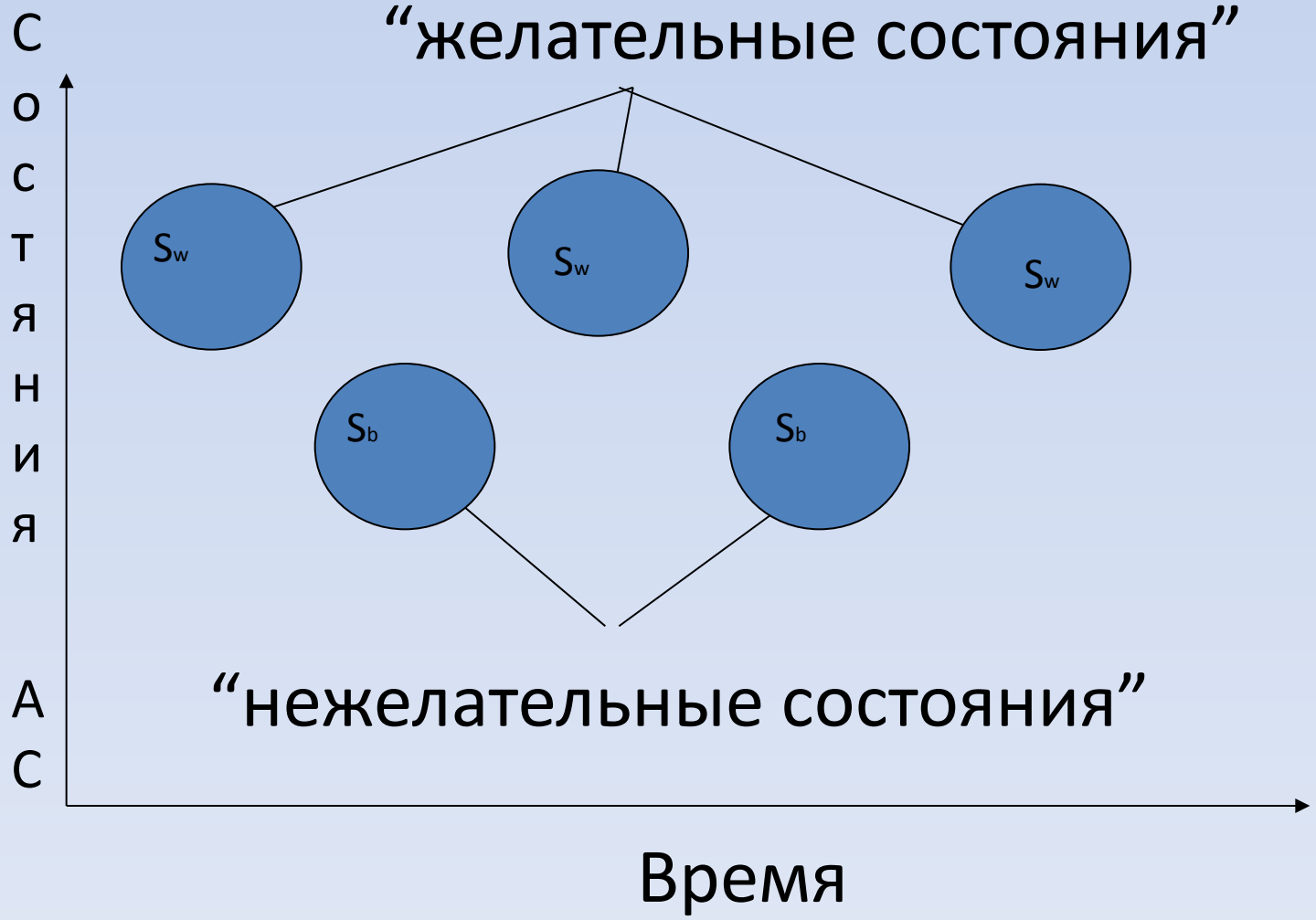
Лекция №2

Политика безопасности. Модель автоматизированной системы. Замкнутая программная среда

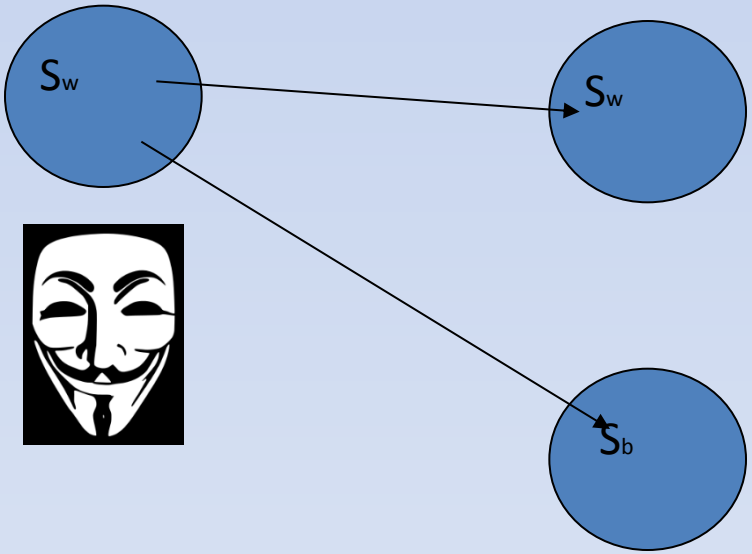
Рахманенко И.А.

ПОЛИТИКА БЕЗОПАСНОСТИ

К понятию “защищенность системы “

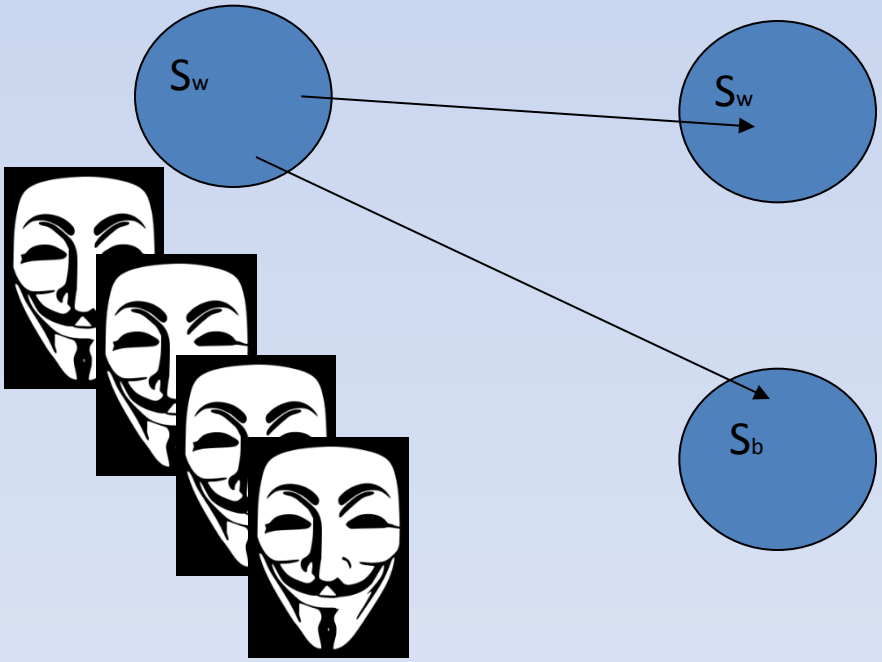


Связь понятий “защищенность”, “злоумышленник”



Злоумышленник - внешняя причина для вывода системы из состояния защищенности

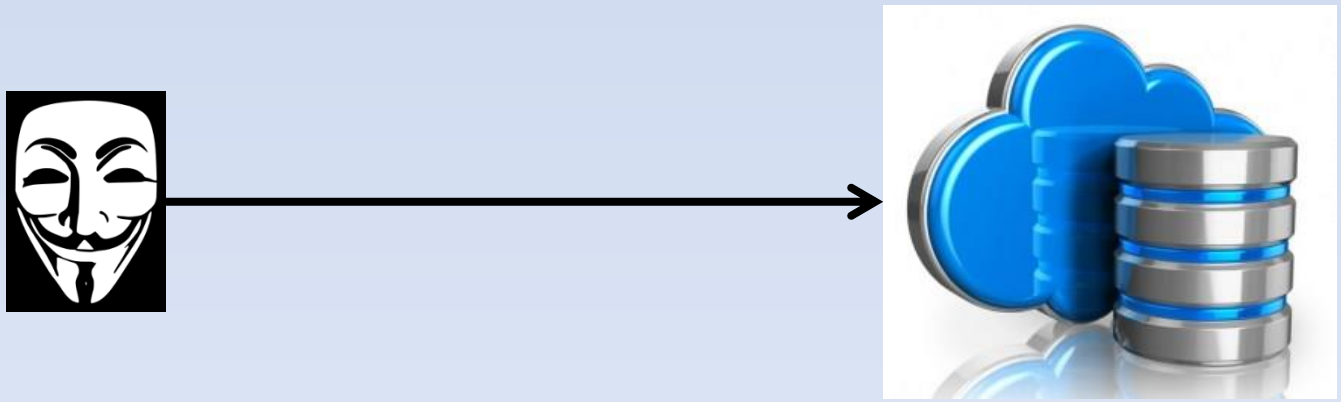
Связь понятий “защищенность”, “угроза”



угроза -понятие, обезличивающее причину вывода системы из защищенного состояния из-за действий злоумышленника

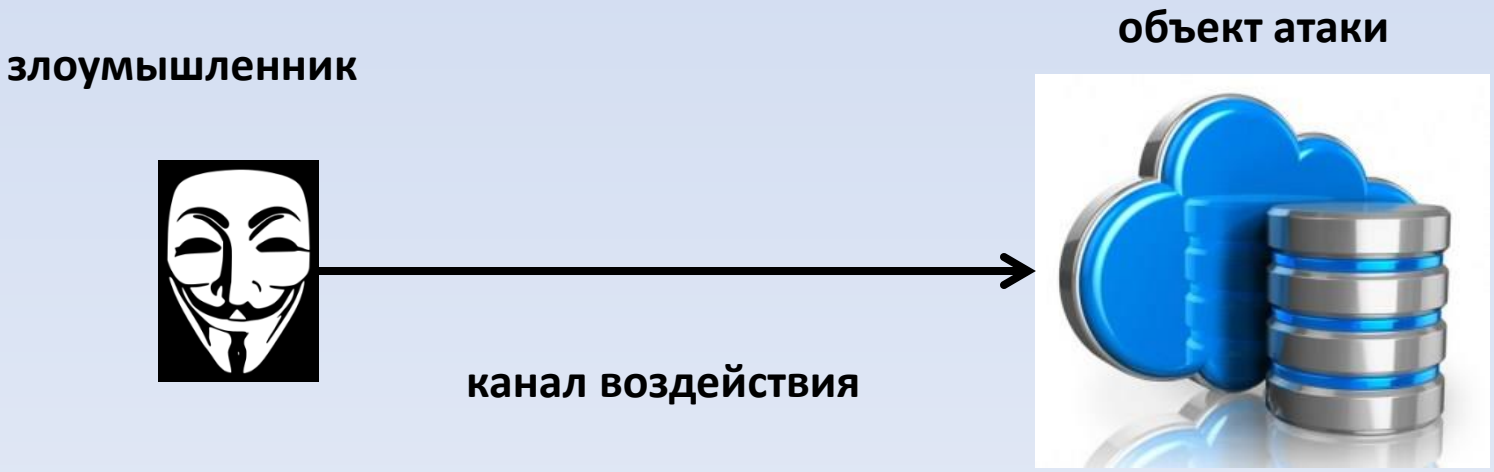
Злоумышленник

Объекты воздействия злоумышленника - часть системы, связанная с теми или иными действиями злоумышленника. "объект атаки"



Нарушение безопасности системы

Злоумышленник – внешний по отношению к системе источник нарушения свойства безопасность
Объект атаки – часть, принадлежащая системе, на которую злоумышленник производит воздействие
Канал воздействия – среда переноса злоумышленного воздействия



Политика безопасности

- ***Политика безопасности (Security Policy).*** Совокупность норм и правил, обеспечивающих эффективную защиту системы обработки информации от заданного множества угроз безопасности.

Политика безопасности

Описание политики безопасности включает:

- Множество возможных операций над объектами.
- Для каждой пары "субъект-объект" (S_iO_i) назначение множества разрешенных операций, являющегося подмножеством всего множества возможных операций.

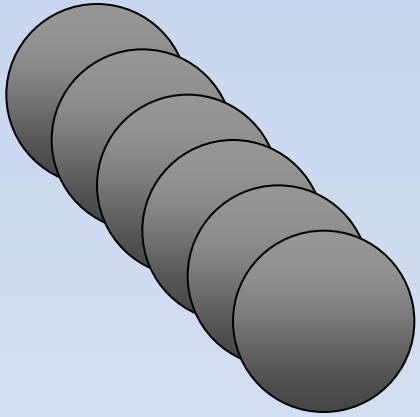
Модель АС

В теории компьютерной безопасности рассматривается модель, основанная на конечных множествах:

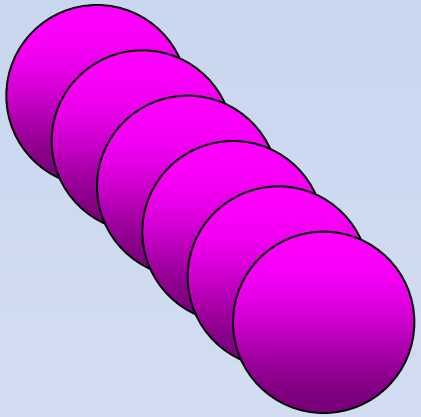
- Множество объектов (O_i).
- Множество субъектов (S_i).

Модель компьютерной системы

Конечное множество элементов



Множество объектов



Множество субъектов

Субъектно-объектная модель КС

Примеры субъектов и объектов

объект	Файл на внешнем носителе
	Область оперативной памяти
	Запись в базе данных
субъект	Исполняемый файл, загруженный в оперативную память и которому передано управление

МОДЕЛЬ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ

Порождение субъектов

- Определение 1.

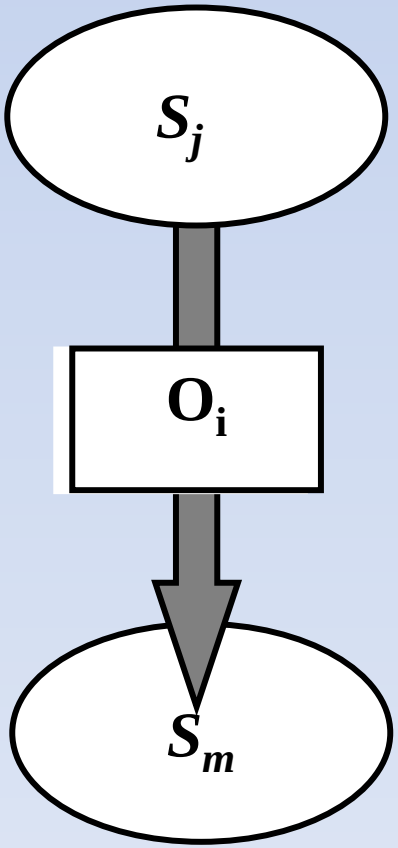
Объект $\mathbf{O_i}$ называется источником для субъекта $\mathbf{S_m}$, если существует субъект $\mathbf{S_j}$, в результате воздействия которого на объект $\mathbf{O_i}$ в КС возникает субъект $\mathbf{S_m}$.

- ***Create*** $(\mathbf{S_j}, \boldsymbol{O_i})$ **->** $\mathbf{S_m}$ - из объекта $\mathbf{O_i}$ порожден субъект $\mathbf{S_m}$ при активизирующем воздействии субъекта $\mathbf{S_j}$.

- ***Create*** $(\mathbf{S_j}, \boldsymbol{O_i})$ **-> NULL –** порождение нового субъекта невозможно

Порождение субъектов

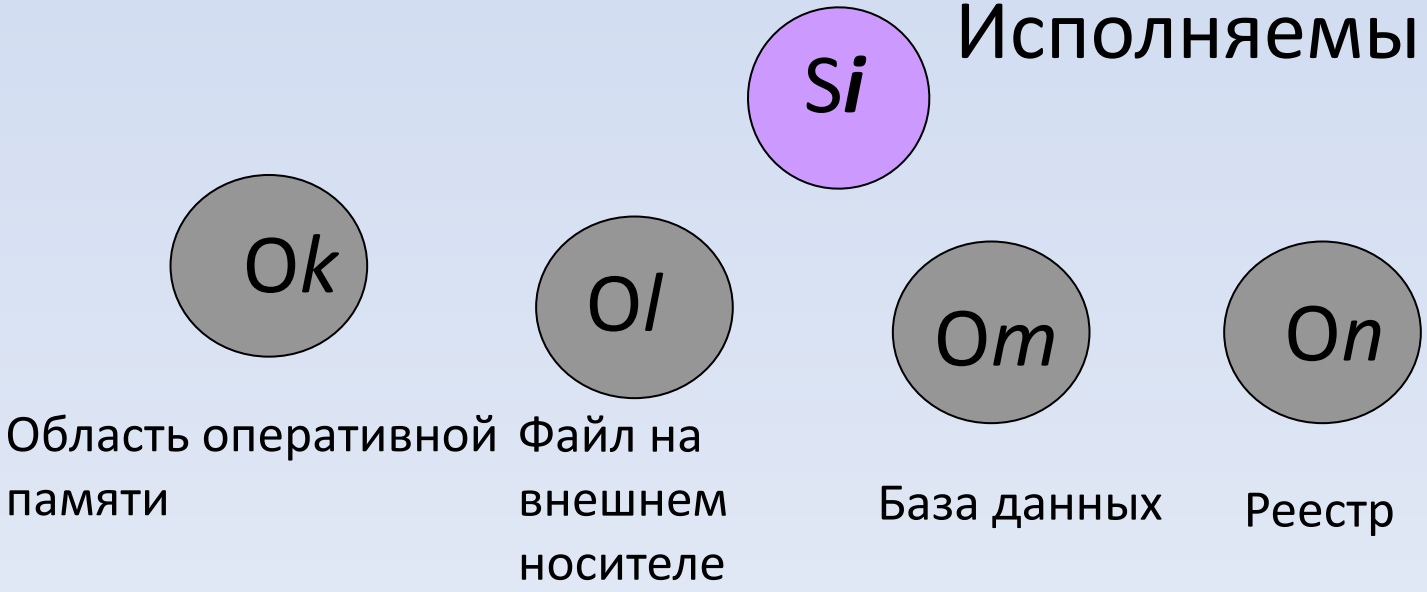
Create(**S**$_j$, ***O***$_i$) -> Sm



Ассоциированный объект

- Определение 2.

  Объект $\mathbf{O_i}$ в момент времени **t** ассоциирован с субъектом $\mathbf{S_m}$, если состояние объекта $\mathbf{O_i}$ повлияло на состояние субъекта в следующий момент времени.



- множество объектов

  $\{O_m\}t$

  ассоциировано с субъектом

  S_j

  в момент времени t:

$$S_j(\{O_m\}t).$$

Один субъект может иметь несколько ассоциированных объектов

Поток

- Определение 3.

  Потоком информации между объектом $\mathbf{O_m}$ и объектом $\mathbf{O_j}$ называется произвольная операция над объектом $\mathbf{O_j}$, реализуемая в субъекте $\mathbf{S_i}$ и зависящая от $\mathbf{O_m}$.

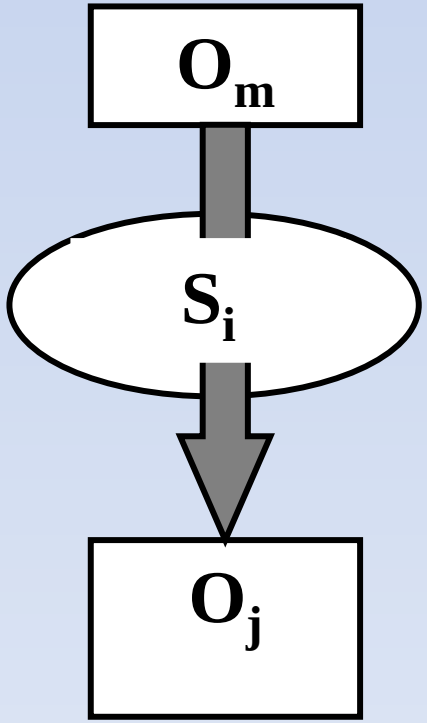
Поток информации от объекта $\mathbf{O_m}$ к объекту $\mathbf{O_j}$

$\boldsymbol{Stream(S_i,O_m)->O_j}$

$\boldsymbol{O_m}$ **-** источник потока информации
$\boldsymbol{O_j}$ – получатель информации

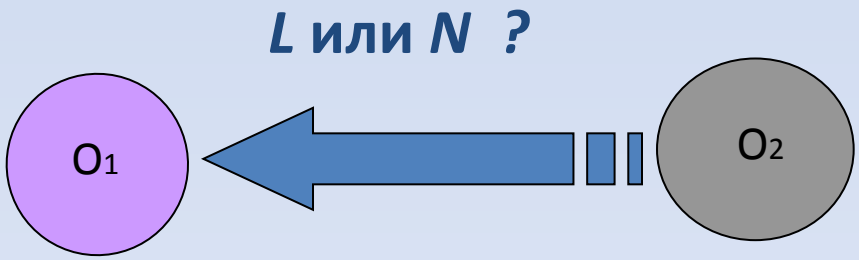
Поток

$Stream(S_i, O_m) \rightarrow O_j$



Множество всевозможных потоков делится на два подмножества:

1. Подмножество потоков характеризующие **легальный** доступ ***L***
2. Подмножество потоков характеризующие **несанкционированный** доступ ***N***

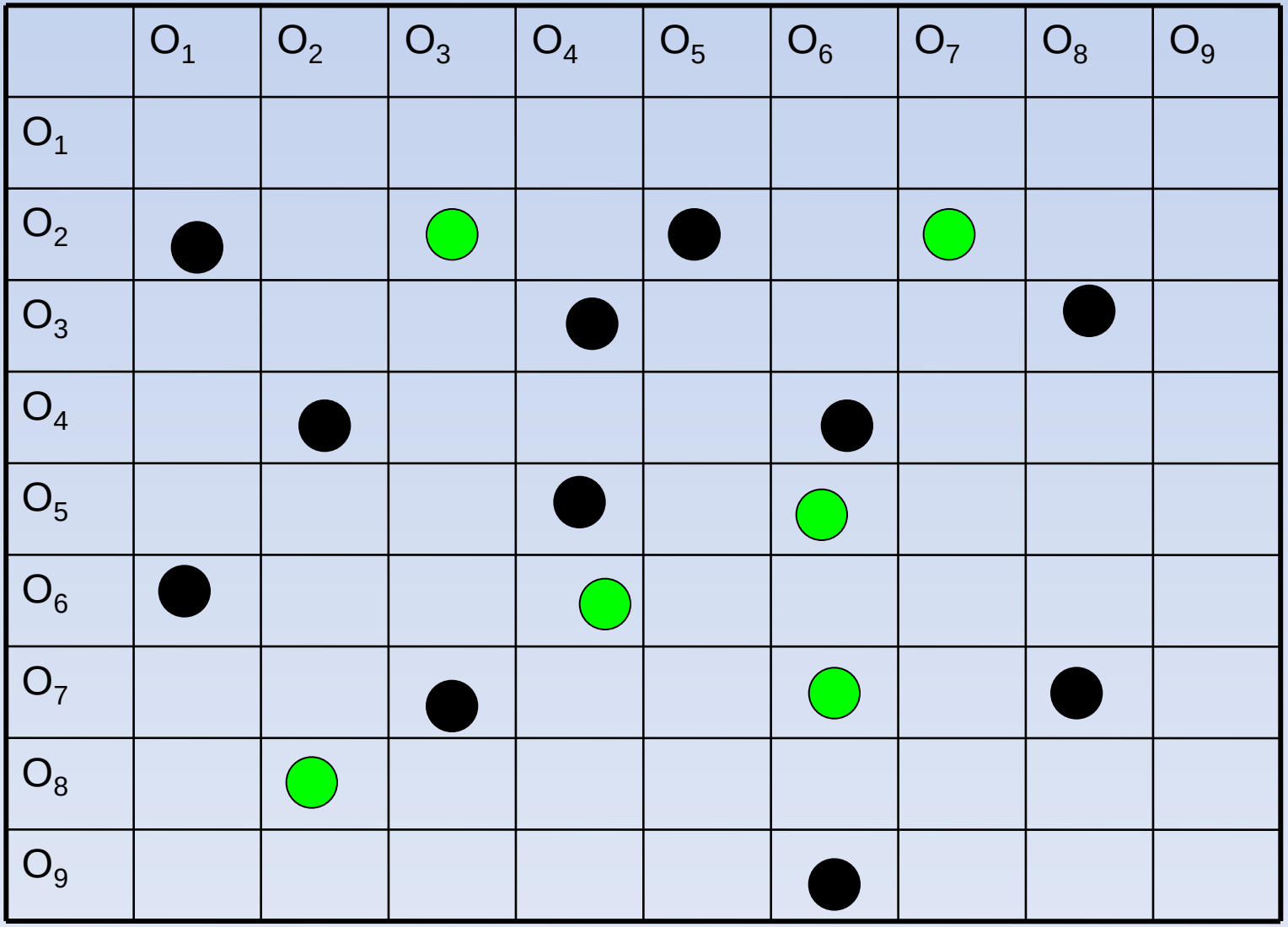


Доступ субъекта к объекту

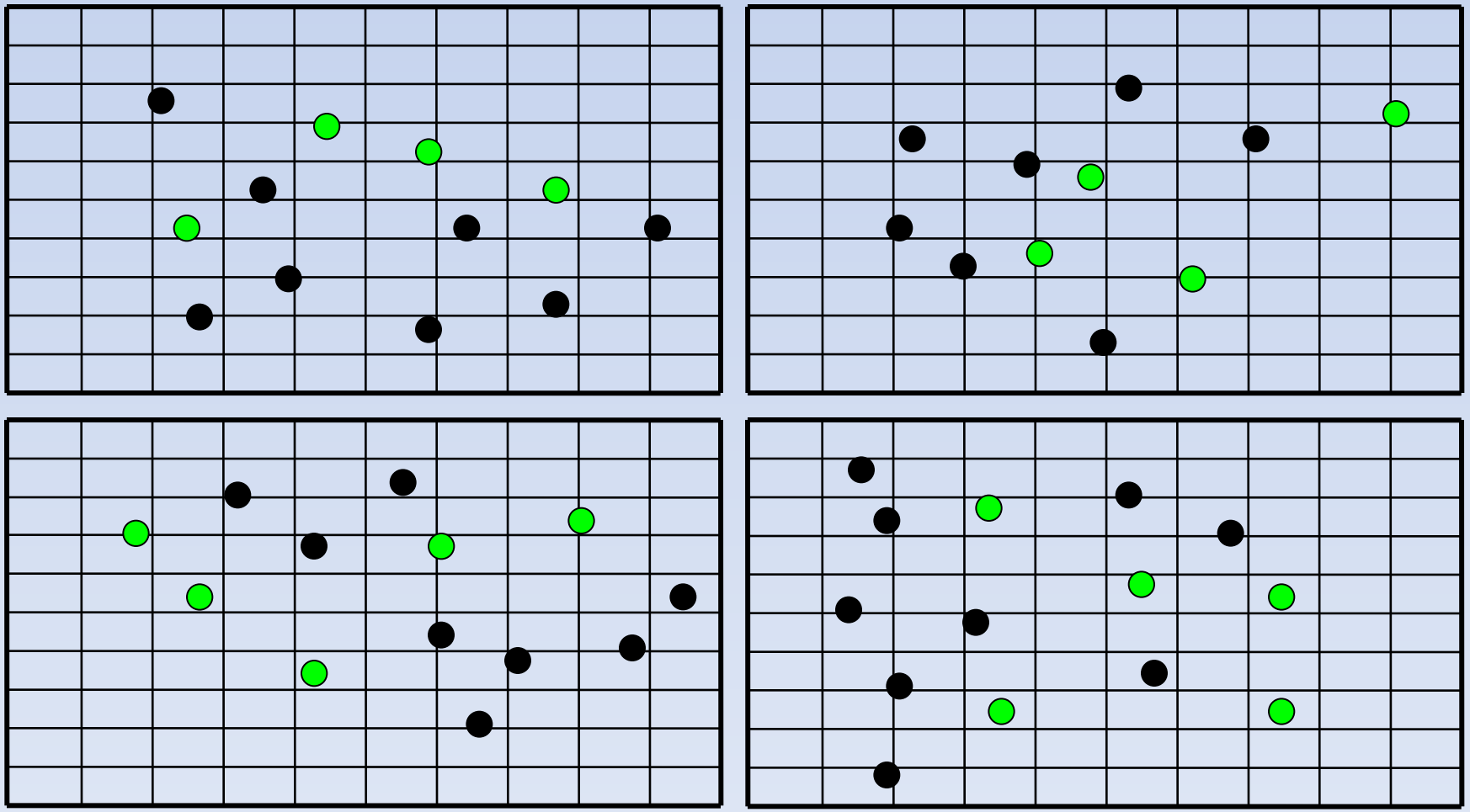
- Определение 4.

  Доступом субъекта $\mathbf{S}_j$ к объекту $\mathbf{O}_j$ будем называть порождение потока информации между некоторым объектом (например, ассоциированными с субъектом объектами) и объектом $\mathbf{O}_j$.

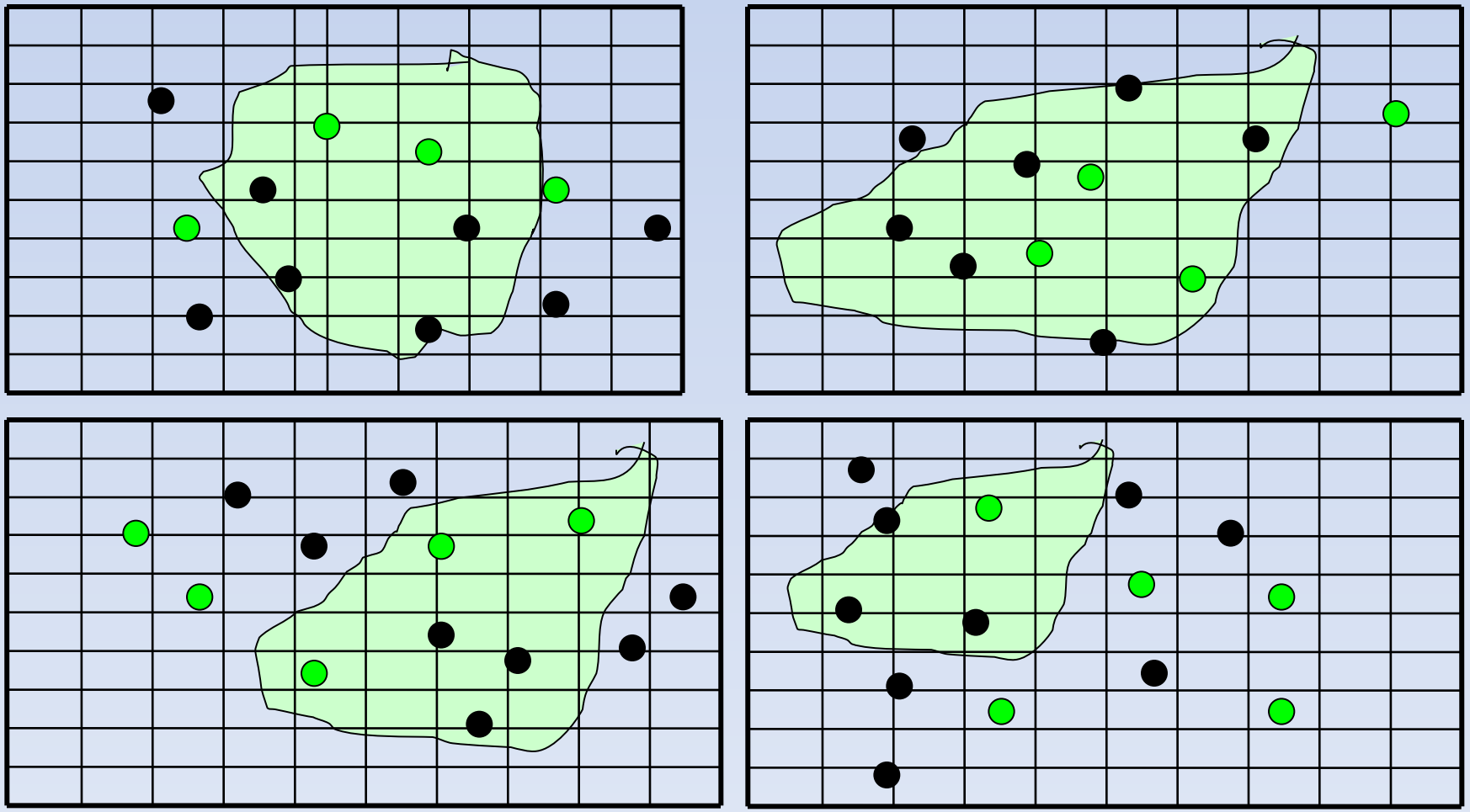
Множество потоков в момент времени t_1



Множество потоков в моменты времени: t_1, t_2,... t_k,... t_{end},



Множество легальных потоков в моменты времени: t_1, t_2,… t_k,… t_{end},



Правила разграничения доступа

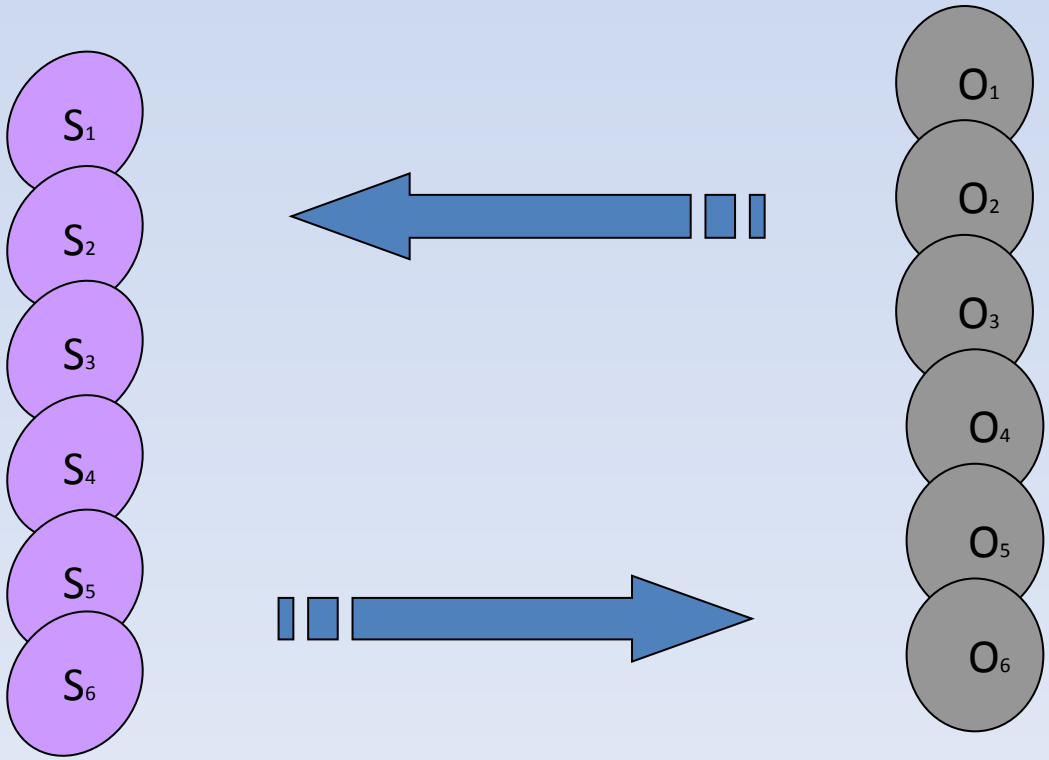
Определение 5.

Правила разграничения доступа субъектов к объектам есть формально описанные потоки, принадлежащие подмножеству легальных потоков **L**.

Монитор обращений

Определение 6.

Монитор обращений (МО) – субъект, активизирующийся при возникновении потока от любого сбъекта к любому объектаму.



Монитор обращений

Выделяют два вида **МО**:

- **Индикаторный МО** – устанавливает только факт обращения субъекта к объекту.

- **Содержательный МО** – субъект, функционирующий таким образом, что при возникновении потока от ассоциированного объекта $\mathbf{O_m}$ любого субъекта $\mathbf{S_i}$ к объекту $\mathbf{O_j}$ и обратно существует ассоциированный с МО объект $\mathbf{O_{mo}}$ тождественный объекту $\mathbf{O_m}$.

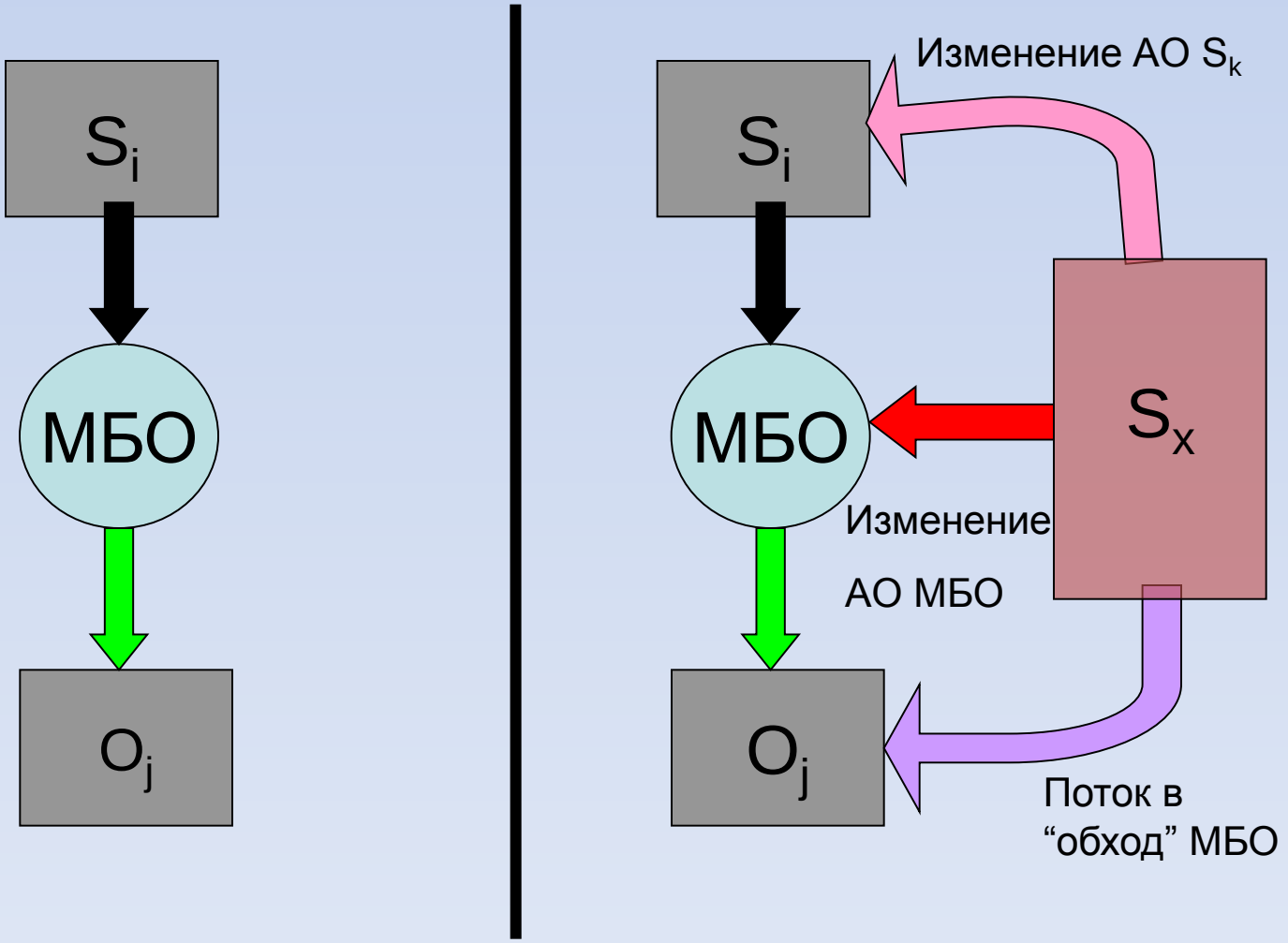
Монитор безопасности объектов

- Определение 7.

  Монитор безопасности объектов (МБО) – монитор обращений, который разрешает поток, принадлежащий только множеству легального доступа L.

ОБЕСПЕЧЕНИЕ ГАРАНТИЙ ВЫПОЛНЕНИЯ ПОЛИТИКИ БЕЗОПАСНОСТИ

Возможные пути нарушения ПБ



Корректные субъекты

- **<u>Определение 8.</u>**
  Пара субъектов S_k и S_i называется не влияющими друг на друга (или **корректными** относительно друг друга), если в любой момент времени отсутствует поток между ассоциированным объектом субъектов $S_k(O_{Sk})$ и $S_i(O_{Si})$, причем O_{Si} не является ассоциированным объектом S_k, а O_{sk} не является ассоциированным объектом S_i.

Абсолютно корректные субъекты

- **Определение 9.**

Пара субъектов называется абсолютно не влияющими друг на друга (или абсолютно корректными относительно друг друга), если множества ассоциированных объектов указанных субъектов не имеют пересечения.

Утверждение 1. Достаточное условие гарантированного выполнения политики безопасности в КС.

Монитор безопасности объектов разрешает порождение потоков только из множества **L**, если все существующие в системе субъекты абсолютно корректны относительно него и друг друга.

- **Определение 10.**

Монитор порождения субъектов (МПС) – субъект, активизирующийся при любом порождении субъектов.

- **Определение 11**.

Монитор безопасности субъектов (МБС) – субъект, который разрешает порождение субъектов только для фиксированного подмножества пар активизирующих субъектов и порождающих объектов.

Воздействие МБС выделяет во всем множестве субъектов **S** подмножество разрешенных **E**.

ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА

ЗАМКНУТАЯ ПРОГРАММНАЯ СРЕДА

- **Определение 12**.
  АС называется **замкнутой** по порождению субъектов, если в ней действует **МБС**, **разрешающий** порождение только **фиксированного** конечного подмножества субъектов для любых объектов-источников, рассматриваемых для фиксированной декомпозиции компьютерной системы на субъекты и объекты

Определение 13.

Множество субъектов АС называется **изолированным**, если в ней действует МБС и субъекты из порождаемого множества корректны относительно друг друга и МБС.

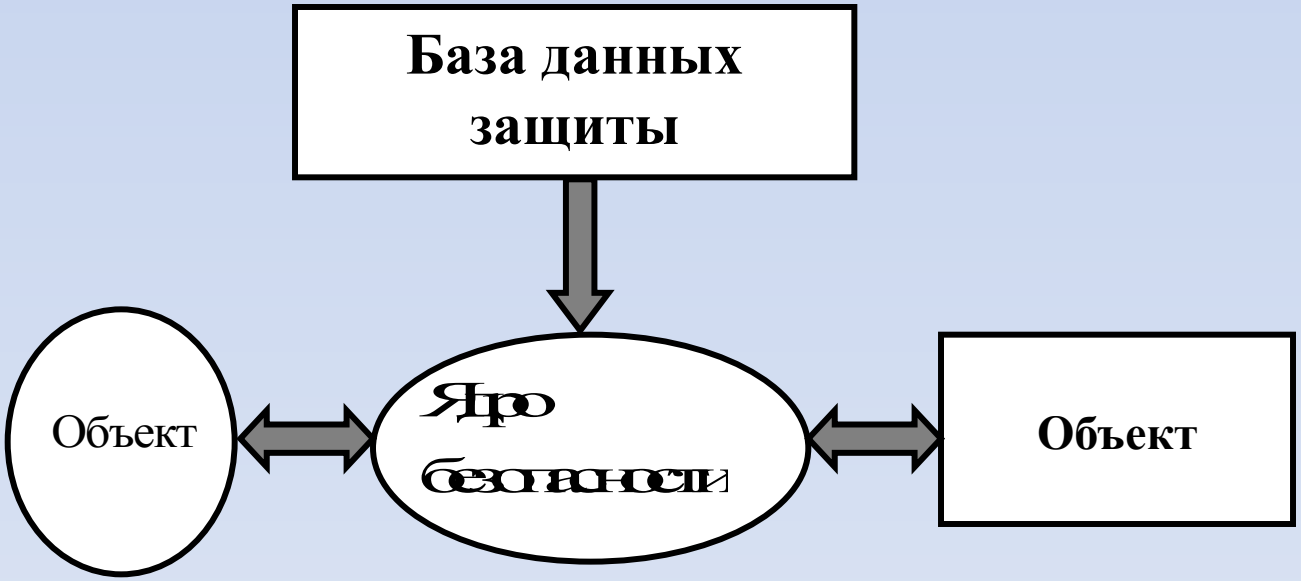
Определение 14.

Операция порождения субъекта ***Create*** $(S_k, O_m) \rightarrow S_i$ называется **порождением с контролем неизменности объекта**, если для любого момента времени $t > t_0$, в который активизирована операция порождения ***Create***, порождение субъекта S_i возможно только при тождественности объектов $O_m[t0]$ и $O_m[t]$.

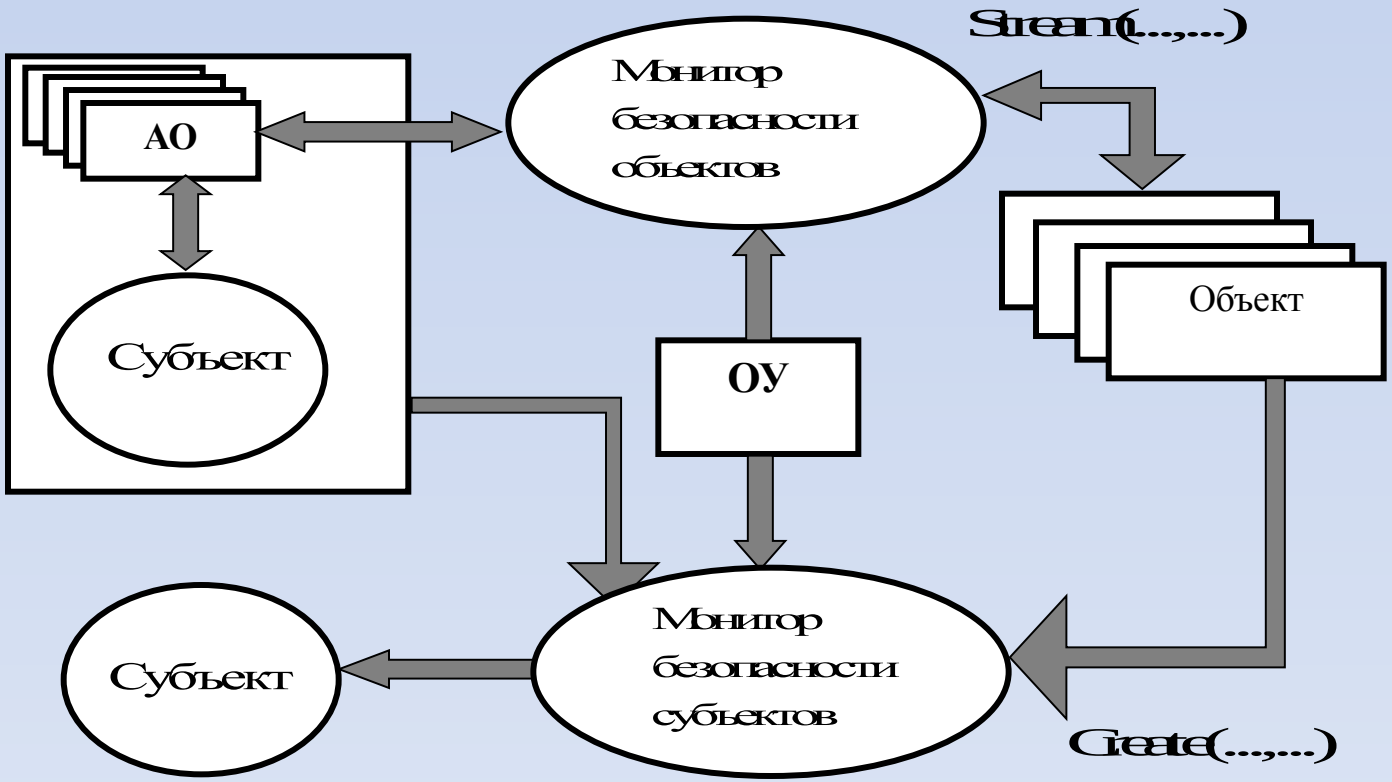
- Утверждение 2 (***базовая теорема ИПС***)

  Если в момент времени $\mathbf{t_0}$ в изолированной КС действует только порождение субъектов с контролем неизменности объекта и существуют потоки от любого субъекта к любому объекту, не противоречащие условию корректности субъектов, то в любой момент времени $\mathbf{t > t_0}$ КС также остается изолированной

Классическая модель ядра безопасности



Ядро безопасности с учетом контроля порождения субъектов



Рассмотренные вопросы

- Политика безопасности
- Модель автоматизированной системы
- Обеспечение гарантий выполнения политики безопасности
- Замкнутая программная среда