

Лекция 6

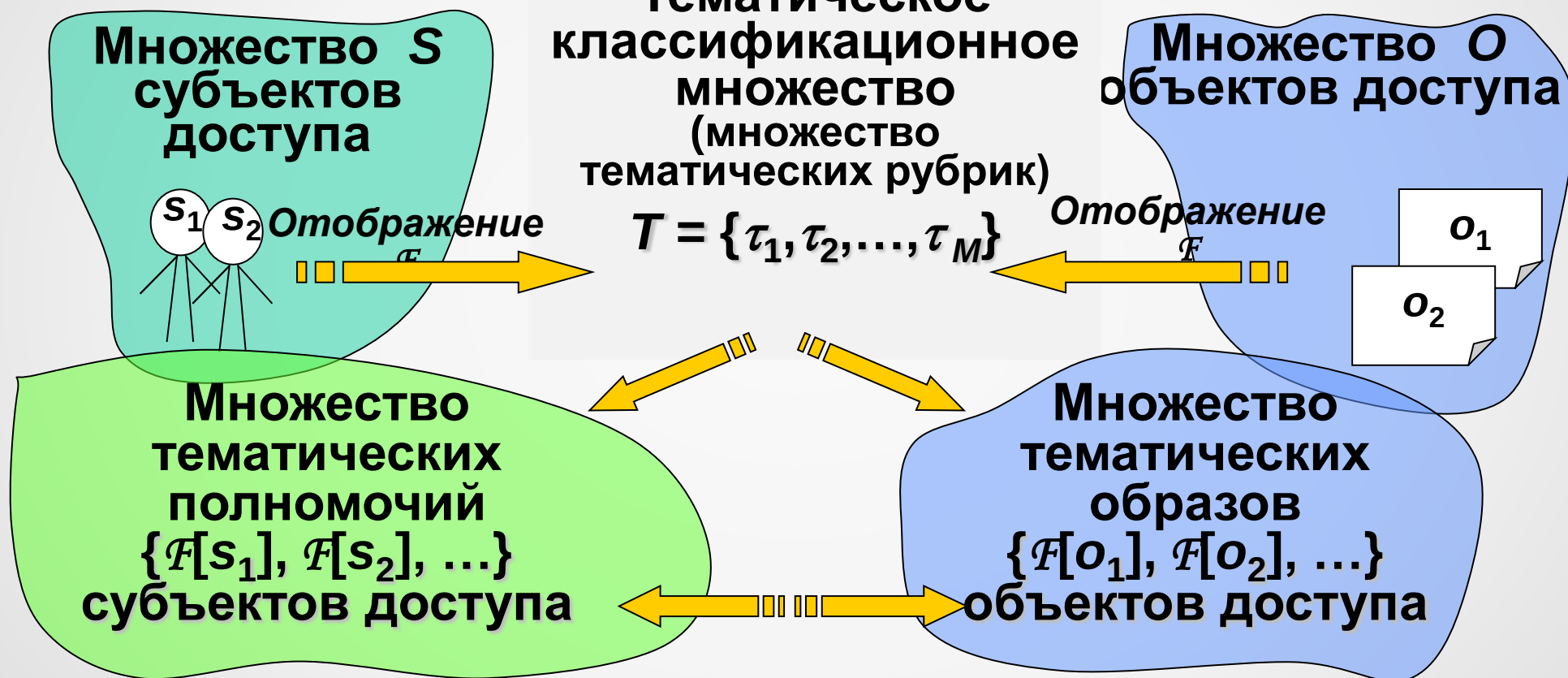
Модели безопасности на основе тематической политики доступа

Модели безопасности на основе тематической политики доступа

Множество субъектов и объектов доступа $X = S \cup O$ тематически классифицируются

Тематическое классификационное множество
(множество тематических рубрик)

$$T = \{\tau_1, \tau_2, \dots, \tau_M\}$$



На множестве тематических полномочий субъектов и тематических образов устанавливается частичный порядок (отношение доминирования $\leq$)

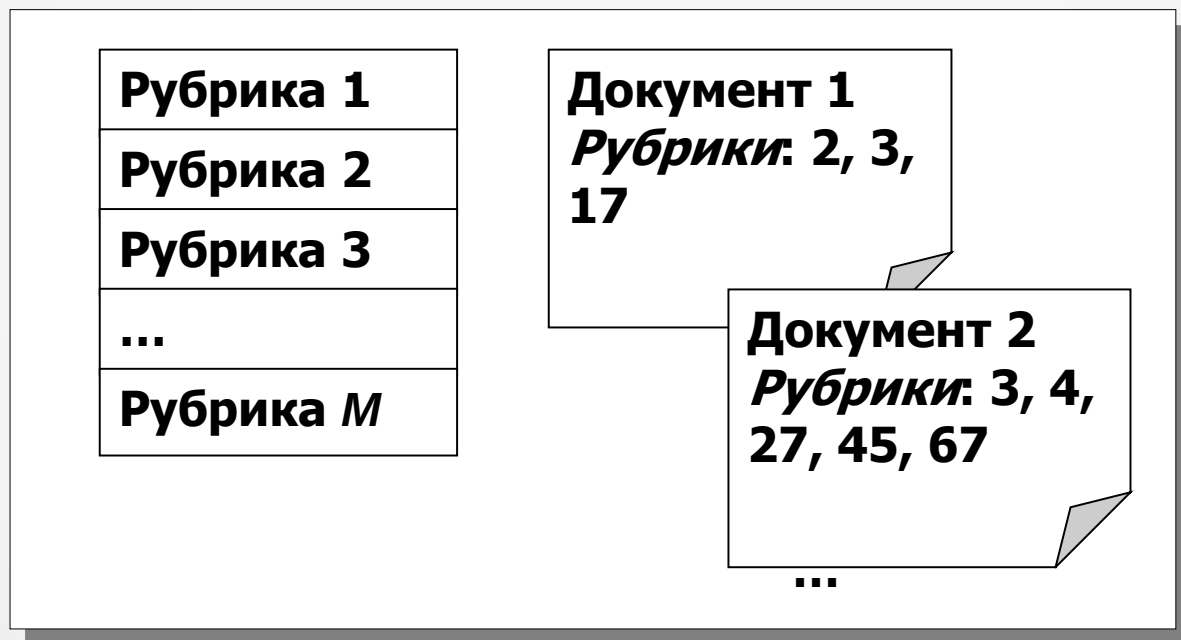
Модели безопасности на основе тематической политики доступа

Три способа тематической классификации

- дескрипторная
- иерархическая
 - монорубрицированная
 - мультирубрицированная
- фасетная
- никакая

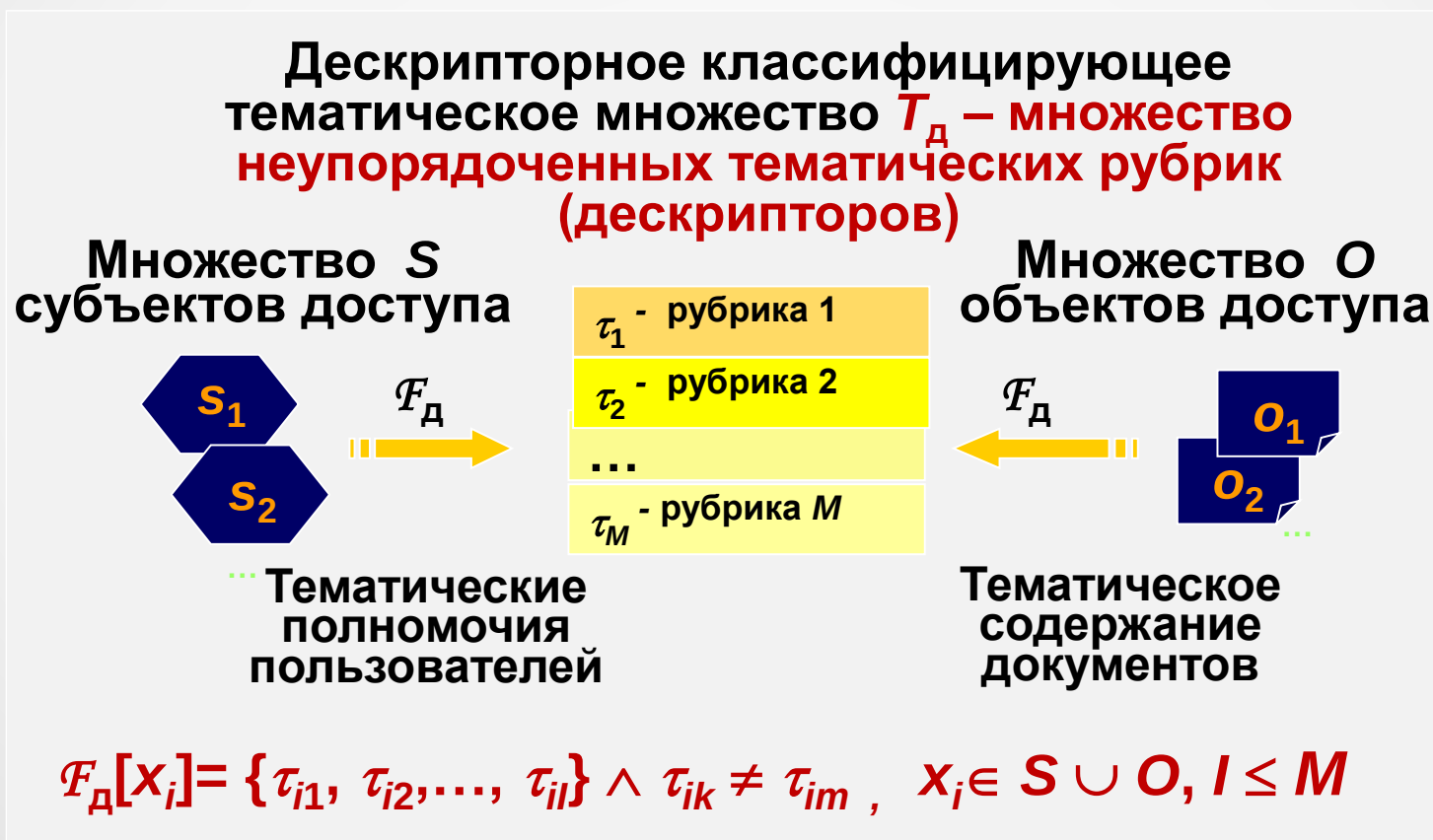
Модели безопасности на основе тематической политики доступа

Дескрипторная тематическая классификация



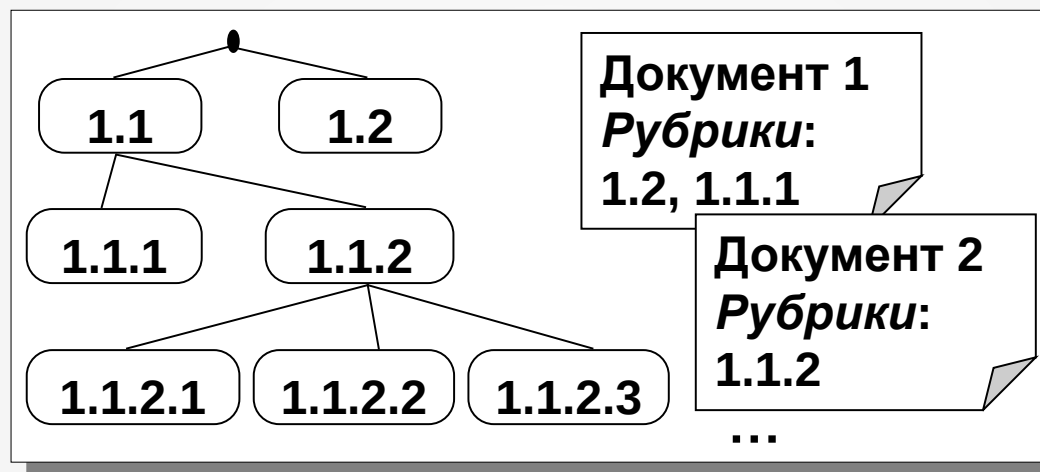
Модели безопасности на основе тематической политики доступа

Дескрипторная тематическая классификация



Модели безопасности на основе тематической политики доступа

Иерархическая тематическая классификация



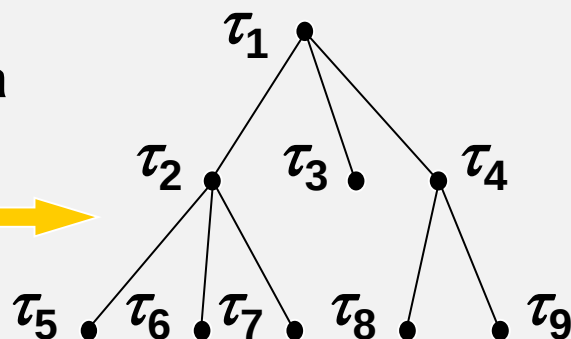
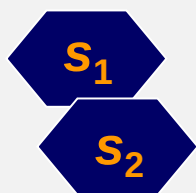
Иерархический тематический классификатор – множество рубрик T_n , на котором посредством корневого дерева установлено отношение частичного порядка элементов $\leq$

Модели безопасности на основе тематической политики доступа

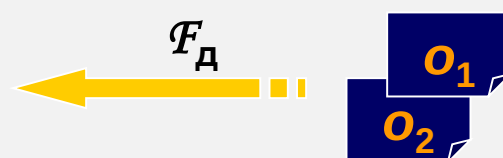
Иерархическая тематическая классификация

Иерархический тематический классификатор – множество рубрик T_i , на котором посредством корневого дерева установлено отношение частичного порядка элементов $\leq$

Множество S
субъектов доступа



Множество S
объектов доступа



Монорубрицованная классификация

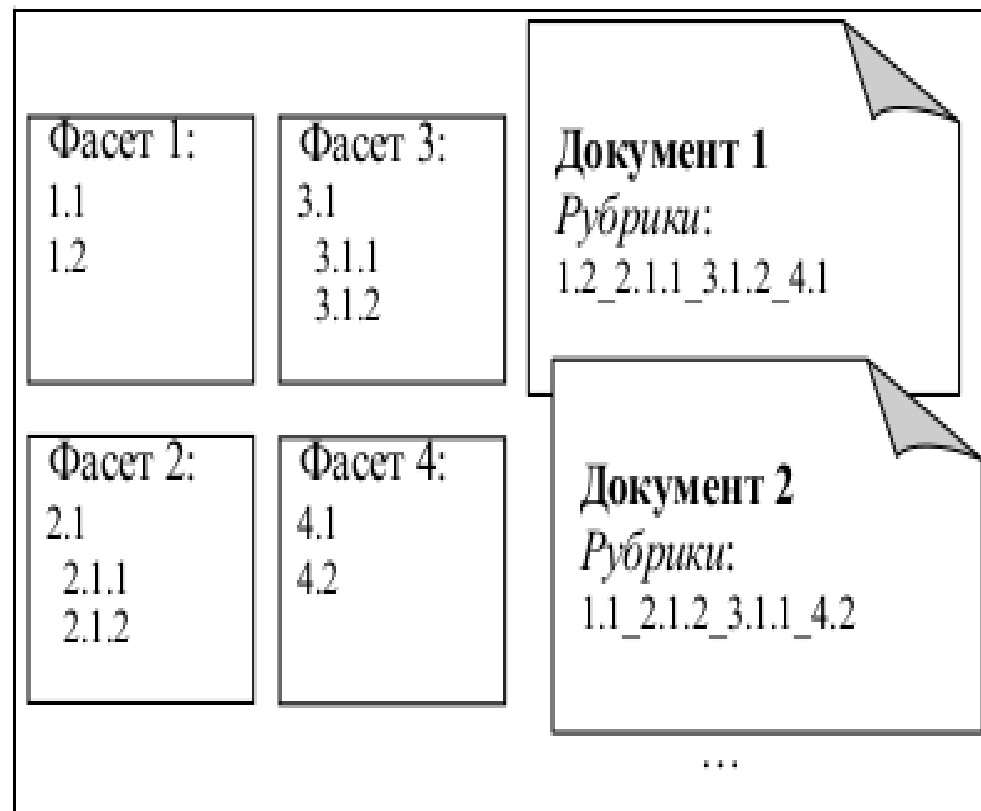
$F_{имн}[X_i] = \tau_i \cup \{\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_l}\}$, где $\tau_{i_k} \leq \tau_i$, $X_i \in S \cup O$, $l < M$.

Мультирубрицированная классификация

$F_{имл}[X_i] = \{\tau_{i_1}, \tau_{i_2}, \dots, \tau_{i_l}\} \cup \{\tau_{i_{11}}, \tau_{i_{12}}, \dots, \tau_{i_{21}}, \tau_{i_{22}}, \dots, \tau_{i_{l1}}, \tau_{i_{l2}}, \dots\} \wedge \tau_{im} \leq \tau_{in}$
 $\wedge \bigvee_i \{\tau_{k_1}, \tau_{k_2}, \dots, \tau_{k_L}\} = \emptyset, \tau_{ik} \leq \tau_{ikj}$

Модели безопасности на основе тематической политики доступа

Основу **фасетной классификации** составляет определенное количество **тематических блоков-фасет**, отражающих логику соответствующей предметной сферы (например: "материал" - "конструкция" - "нагрузки" ИЛИ "время" - "место" - "состав" - "действие" и т. д.). Каждый фасет, в свою очередь, представляет **классификационную подсистему тематик (рубрик) иерархического типа**.



Модели безопасности на основе тематической политики доступа

Общее правило тематического доступа

Документ доступен сотруднику, если он не содержит рубрик, запрещенных (не разрешенных) для данного сотрудника

Недопустимы доступы (вызывающие опасные потоки)

- от сущностей x_1 с более широкой тематикой к сущностям x_2 с более узкой тематикой

$$(x_1 \rightarrow x_2) \quad F[x_1] \geq F[x_2]$$

- между сущностями x_1 и x_2 с несравнимой тематикой

$$(x_1 \leftrightarrow x_2) \quad F[x_1] \geq \leq F[x_2]$$

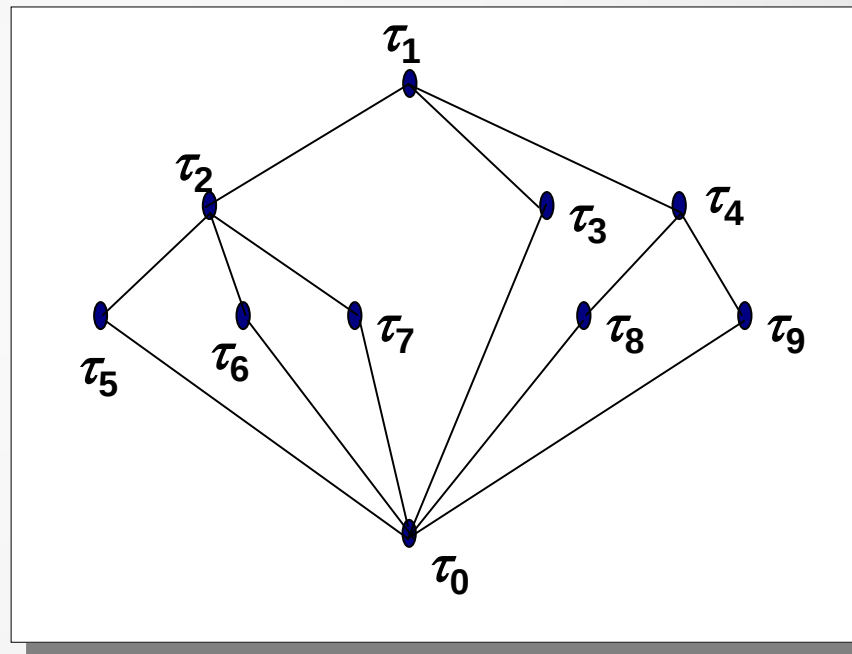
Тематические решетки

1. При дескрипторной тематической классификации -

решетка $\Lambda_d(P_d, \subseteq, \cup, \cap)$ подмножеств множества $T_d = \{\tau_1, \tau_2, \dots, \tau_M\}$, где $P_d = F_d[x] \subseteq T_d$, $x \in S \cup O$

2. На иерархическом рубрикаторе (монорубрицрованной классификации)

- решетка $\Lambda_i(T_{i\emptyset}, \leq, \sup_i, \inf_i)$ на корневом дереве рубрикатора $T_i = \{\tau_1, \tau_2, \dots, \tau_M\}$ путем добавления вершины τ_0 (с пустой тематикой) и замыкания на нее всех листовых вершин



- и решетка $\Lambda_i(T^l, \subseteq, \cup_{ил}, \cap)$ листовых подмножеств вершин на корневом дереве рубрикатора.
- Решетки $\Lambda_i(T_{i\emptyset}, \leq, \sup_i, \inf_i)$ и $\Lambda_i(T^l, \subseteq, \cup_{ил}, \cap)$ изоморфны

Тематические решетки

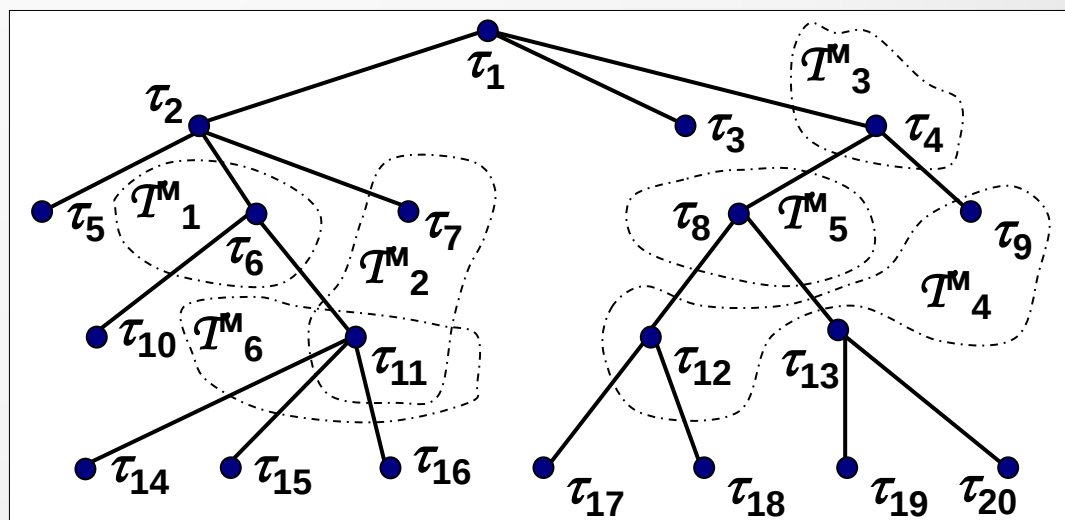
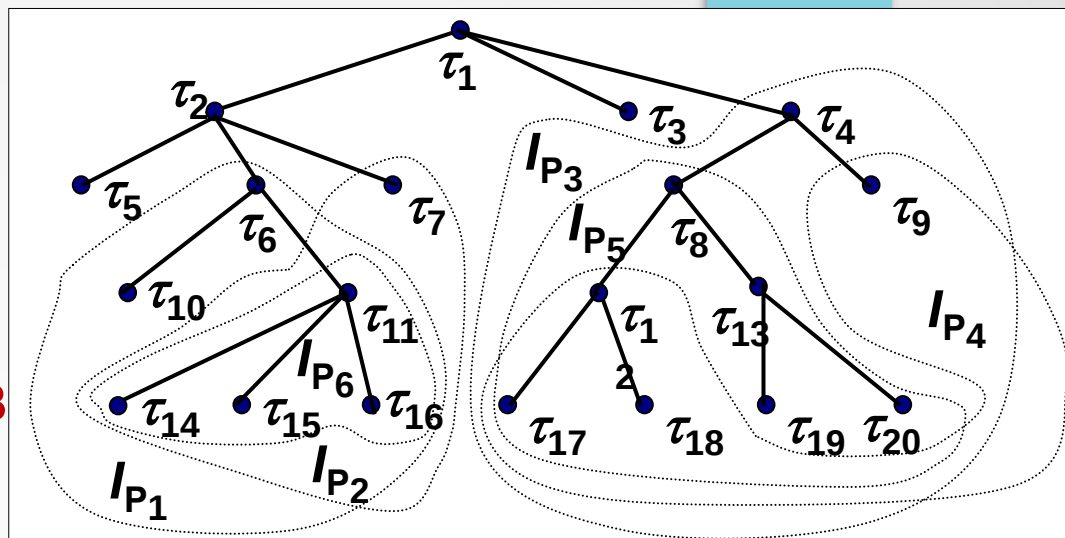
3. На иерархическом рубрикаторе

(при мультирубрицированной классификации)

- решетка $\Lambda_{\text{и}}(I_{\text{P}}, \subseteq, \cup_{\text{ир}}, \cap)$
рубрикаторных идеалов

$$I_{\text{P}2} \subseteq I_{\text{P}6}, I_{\text{P}2} \subseteq I_{\text{P}1}, I_{\text{P}4} \subseteq I_{\text{P}3}, \\ I_{\text{P}5} \subseteq I_{\text{P}3}, I_{\text{P}6} = I_{\text{P}1} \cap I_{\text{P}2}, \\ I_{\text{P}3} = I_{\text{P}4} \cup_{\text{ир}} I_{\text{P}5}$$

- решетка мультирубрик
 $\Lambda_{\text{и}}(T^{\text{M}}, \leq_{\text{M}}, \cup_{\text{M}}, \cap_{\text{M}})$



Тематические решетки

Определение 1.

Мультирубрика T^M_j доминирует над мультирубрикой

$$T^M_j - \{\tau^{(j)}_1, \tau^{(j)}_2, \dots, \tau^{(j)}_J\} \leq \{\tau^{(i)}_1, \tau^{(i)}_2, \dots, \tau^{(i)}_J\}$$

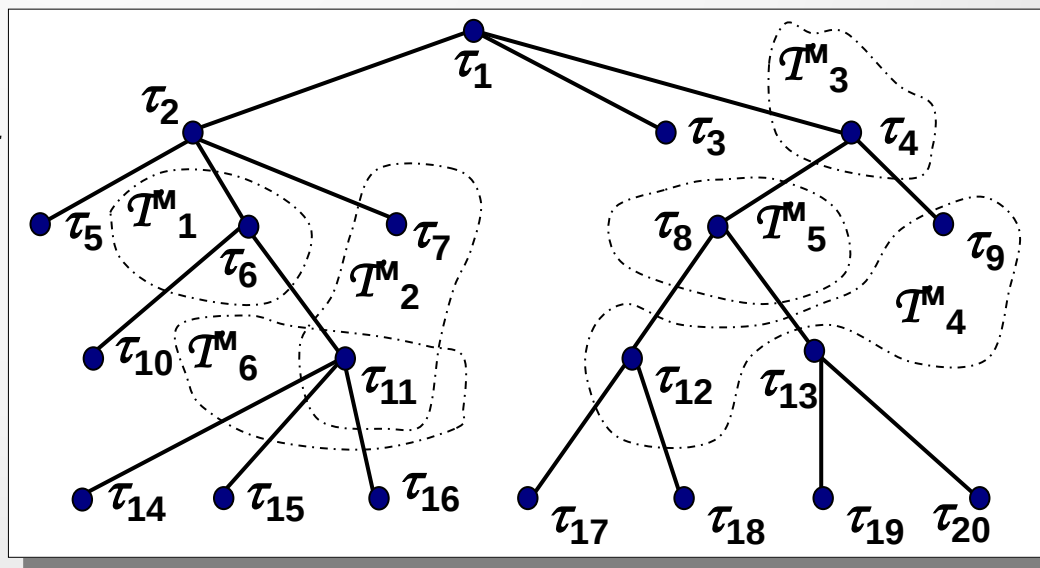
в том и только в том случае, когда для любого $m=1, \dots, J$ существует $k=1, \dots, I$ такое, что $\tau^{(j)}_m \leq \tau^{(i)}_k$

(вершина $\tau^{(j)}_m$ подчинена по корневому дереву вершине $\tau^{(i)}_k$):

$$T^M_2 \leq_M T^M_6, \quad T^M_4 \leq_M T^M_3, \quad T^M_5 \leq_M T^M_3, \\ T^M_6 = T^M_1 \cap_M T^M_2, \quad T^M_3 = T^M_4 \cup_M T^M_5$$

$$\forall \tau^{(j)}_m \in T^M_j,$$

$$\forall \exists \tau^{(i)}_k \in T^M_i \wedge \tau^{(j)}_m \leq \tau^{(i)}_k.$$



Решетка мультирубрик $\Lambda_n(\mathcal{T}^M, \leq_M, \cup_M, \cap_M)$

Определение 2.

Объединением $\cup_M$ мультирубрик

$$\mathcal{T}^M_i = \{\tau^{(i)}_1, \tau^{(i)}_2, \dots, \tau^{(i)}_l\} \text{ и } \mathcal{T}^M_j = \{\tau^{(j)}_1, \tau^{(j)}_2, \dots, \tau^{(j)}_j\}$$

называется операция формирования множества вершин иерархического рубрикатора $\mathcal{T}^{M\cup} = \mathcal{T}^M_i \cup_M \mathcal{T}^M_j$ на основе следующего алгоритма:

1) Формируется теоретико-множественное объединение множеств вершин, составляющих мультирубрики –

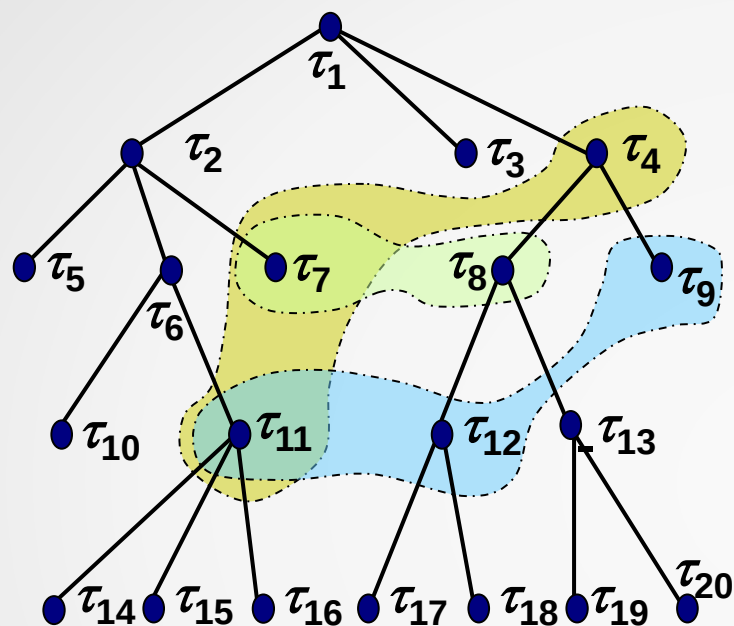
$$\mathcal{T}^\cup = \{\tau^{(i)}_1, \tau^{(i)}_2, \dots, \tau^{(i)}_l\} \cup \{\tau^{(j)}_1, \tau^{(j)}_2, \dots, \tau^{(j)}_j\};$$

2) Формируется набор вершин $\mathcal{T}^{M\cup'}$ путем исключения из него тех вершин из $\mathcal{T}^\cup$, которые доминируются хотя бы одной вершиной из того же набора

$$\mathcal{T}^\cup - (\tau_k \in \mathcal{T}^\cup \wedge \tau_k \in \mathcal{T}^{M\cup}) \equiv (\exists \tau_m \in \mathcal{T}^\cup \wedge \tau_m \leq \tau_k);$$

3) Формируется итоговый набор вершин $\mathcal{T}^{M\cup}$ путем добавления в него результатов иерархического сжатия по всем подмножествам набора вершин $\mathcal{T}^{M\cup'}$ и одновременным исключением соответствующих наборов сыновей при непустом результате сжатия

Решетка мультирубрик $\Lambda_n(\mathcal{T}^M, \leq_M, \cup_M, \cap_M)$



$$\{\tau_7, \tau_8\} \cup_M \{\tau_{11}, \tau_{12}, \tau_9\}$$

$$1) \{\tau_7, \tau_8, \tau_{11}, \tau_{12}, \tau_9\}$$

$$2) \{\tau_7, \tau_8, \tau_{11}, \tau_9\}$$

$$3) \{\tau_{11}, \tau_7, \tau_4\}$$

Лемма 1. Множество рубрик $\mathcal{T}^{M\cup} = \mathcal{T}^M_i \cup_M \mathcal{T}^M_j$, формируемое на основе объединения мультирубрик по определению 2,

а) является мультирубрикой;

б) доминирует над мультирубриками $\mathcal{T}^M_i$ и $\mathcal{T}^M_j$,

$$\text{т.е. } \mathcal{T}^M_i \leq \mathcal{T}^{M\cup} \wedge \mathcal{T}^M_j \leq \mathcal{T}^{M\cup};$$

с) является наименьшей верхней границей мультирубрик $\mathcal{T}^M_i$ и $\mathcal{T}^M_j$.

Решетка мультирубрик $\Lambda_n(\mathcal{T}^M, \leq_M, \cup_M, \cap_M)$

Определение 3.

Пересечением $\cap_M$ **мультирубрик** $\mathcal{T}_i^M = \{\tau_{i1}^{(i)}, \tau_{i2}^{(i)}, \dots, \tau_{ij}^{(i)}\}$ и $\mathcal{T}_j^M = \{\tau_{j1}^{(j)}, \tau_{j2}^{(j)}, \dots, \tau_{jk}^{(j)}\}$ называется операция формирования множества вершин иерархического рубрикатора $\mathcal{T}^{M\cap} = \mathcal{T}_i^M \cap_M \mathcal{T}_j^M$ на основе следующего алгоритма:

1) Из множества вершин мультирубрики

$\mathcal{T}_i^M = \{\tau_{i1}^{(i)}, \tau_{i2}^{(i)}, \dots, \tau_{ij}^{(i)}\}$ формируются множество вершин $\mathcal{T}^{M'}$, которые доминируются хотя бы одной вершиной из множества вершин другой мультирубрики

$$\mathcal{T}_j^M = \{\tau_{j1}^{(j)}, \tau_{j2}^{(j)}, \dots, \tau_{jk}^{(j)}\};$$

2) Из множества вершин мультирубрики

$\mathcal{T}_j^M = \{\tau_{j1}^{(j)}, \tau_{j2}^{(j)}, \dots, \tau_{jk}^{(j)}\}$ формируются множество вершин $\mathcal{T}^{M'}$, которые доминируются хотя бы одной вершиной из множества вершин первой мультирубрики

$$\mathcal{T}_i^M = \{\tau_{i1}^{(i)}, \tau_{i2}^{(i)}, \dots, \tau_{ij}^{(i)}\};$$

3) Формируется теоретико-множественное объединение

$$\mathcal{T}^{M\cap} = \mathcal{T}^{M'}_i \cup \mathcal{T}^{M'}_j$$

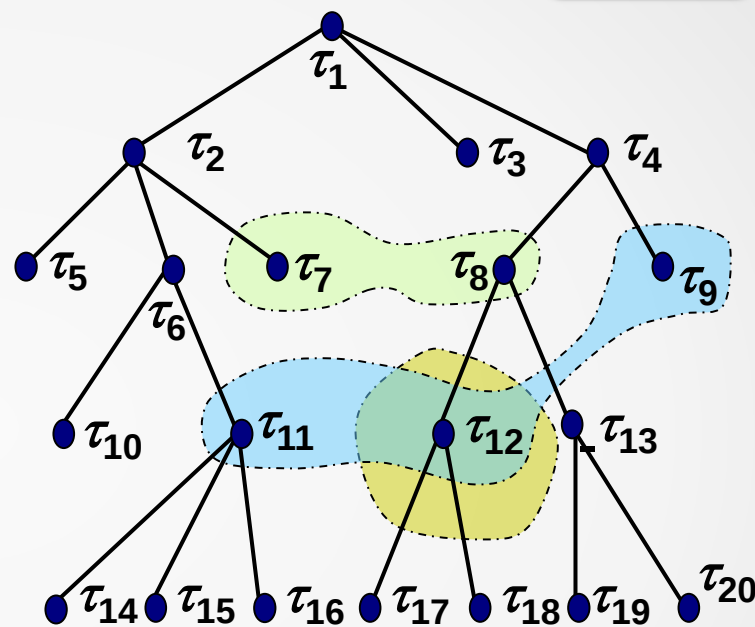
Решетка мультирубрик $\Lambda_{\mathcal{M}}(\mathcal{T}^{\mathcal{M}}, \leq_{\mathcal{M}}, \cup_{\mathcal{M}}, \cap_{\mathcal{M}})$

$$\{\tau_7, \tau_8\} \cap_{\mathcal{M}} \{\tau_{11}, \tau_{12}, \tau_9\}$$

$$1) \{\tau_7, \tau_8\} \rightarrow \emptyset$$

$$2) \{\tau_{11}, \tau_{12}, \tau_9\} \rightarrow \{\tau_{12}\}$$

$$3) \emptyset \cup \{\tau_{12}\} = \{\tau_{12}\}$$



Лемма 2. Множество рубрик $\mathcal{T}^{\mathcal{M}\cap} = \mathcal{T}^{\mathcal{M}_i} \cap_{\mathcal{M}} \mathcal{T}^{\mathcal{M}_j}$, формируемое на основе пересечения мультирубрик по определению 3,

а) является мультирубрикой;

б) доминируется мультирубриками $\mathcal{T}^{\mathcal{M}_i}$ и $\mathcal{T}^{\mathcal{M}_j}$,

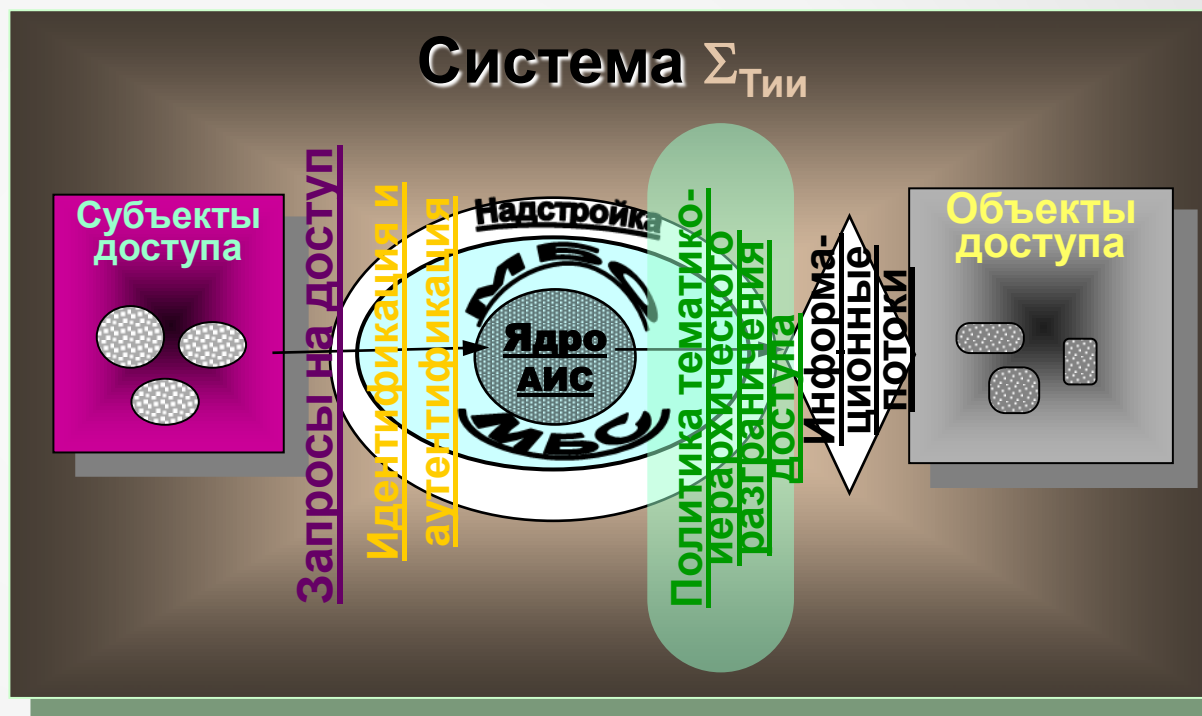
т.е. $\mathcal{T}^{\mathcal{M}\cap} \leq \mathcal{T}^{\mathcal{M}_i} \wedge \mathcal{T}^{\mathcal{M}\cap} \leq \mathcal{T}^{\mathcal{M}_j}$;

с) является наибольшей нижней границей мультирубрик $\mathcal{T}^{\mathcal{M}_i}$ и $\mathcal{T}^{\mathcal{M}_j}$.

Модель тематико-иерархического разграничения доступа

1. Компьютерная система $\Sigma_{\text{Тии}}$ представляется совокупностью субъектов и объектов доступа.

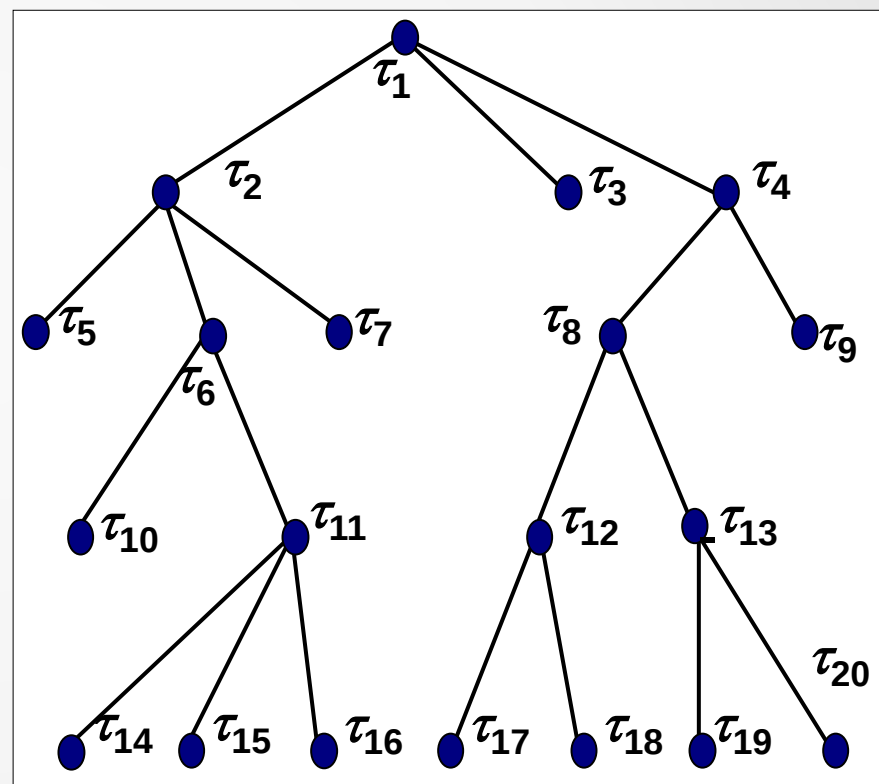
В системе $\Sigma_{\text{Тии}}$ действует МБО, санкционирующий запросы субъектов на доступ к объектам, и МБС, управляющий инициализацией субъектов



Модель тематико-иерархического разграничения доступа

2. Информационно-логическая схема предметной области системы $\Sigma_{\text{ТИИ}}$ представляется тематическим иерархическим классификатором (рубрикатором).

Рубрикатор включает конечное множество тематических рубрик $T_{\text{и}} = \{\tau_1, \tau_2, \dots, \tau_M\}$, на котором установлен частичный порядок, задаваемый корневым деревом



Модель тематико-иерархического разграничения доступа

3. Множество сущностей системы $X = S \cup O$ тематически классифицируется на основе отображения на множество мультирубрик T^M , определенных на корневом дереве иерархического рубрикатора.

Существует функция тематического окрашивания f_M , которая в каждый момент времени для любой сущности системы $x \in X$ определяет соответствующую ей мультирубрику:

$$f_M[x] = T^M_i, \quad T^M_i \in T^M.$$

4. Тематический критерий безопасности.

Система $\Sigma_{\text{Тии}}$ безопасна тогда и только тогда, когда в ней отсутствуют потоки следующих видов:

- от сущностей с более широкой тематикой к сущностям с более узкой тематикой;*
- между несравнимыми по тематике сущностями.*

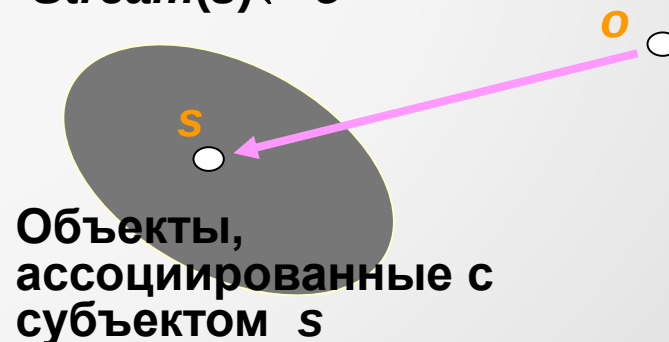
Модель тематико-иерархического разграничения доступа

5. Переходы системы $\Sigma_{\text{Тии}}$, обусловленные запросами и осуществлением доступов существующих субъектов к существующим объектам, санкционируются МБО на основе следующих правил:

Правило 1.

Доступ субъекта s к объекту o , вызывающий поток по чтению $\text{Stream}(s) \leftarrow o$, неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта: $f_m[s] \geq f_m[o]$

Чтение (r) из объекта
 $\text{Stream}(s) \leftarrow o$



Модель тематико-иерархического разграничения доступа

Правило 2.

*Доступ субъекта s к объекту o , вызывающий поток по записи **$Stream(s) \rightarrow o$** , неопасен и может быть МБО разрешен тогда и только тогда, когда мультирубрика объекта доминирует над мультирубрикой субъекта:*

$$f_m[o] \geq f_m[s]$$

Запись (w) в объект **$Stream(s) \rightarrow o$**



Модель тематико-иерархического разграничения доступа

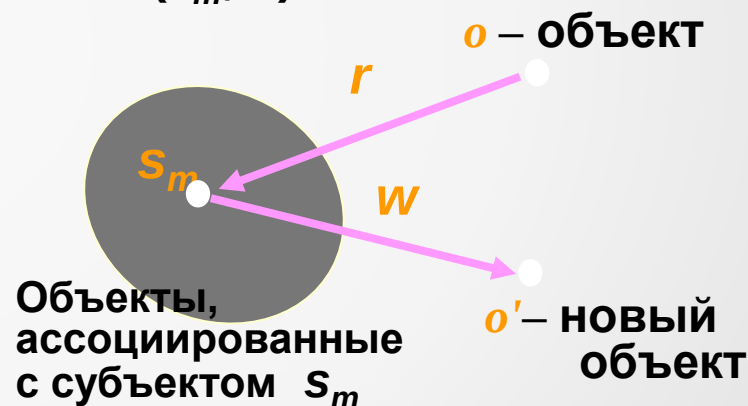
6. Переходы системы $\Sigma_{\text{Тии}}$, связанные с порождением новых объектов и субъектов доступа, санкционируются МБО и МБС на основе следующих правил:

Правило 3.

Порождение субъектом s нового объекта o' , в том числе и за счет чтения из другого объекта o , неопасно и может быть МБО разрешено тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта o , при этом МБО присваивает новому объекту o' мультирубрику, равную или доминирующую над мультирубрикой субъекта:

$$f_M[o] \leq f_M[s] \leq f_M[o']$$

Создание нового объекта
 $Create(s_m, o) \rightarrow o'$



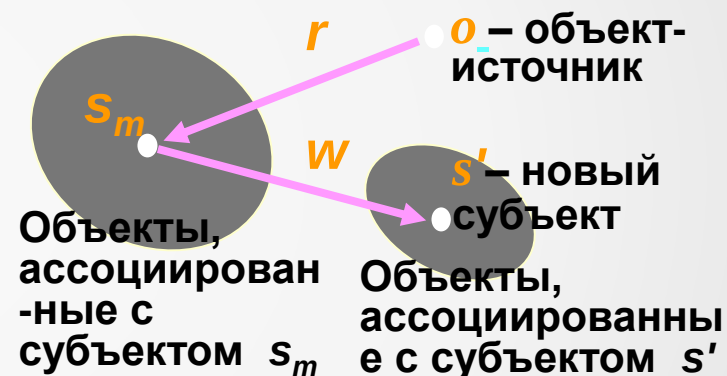
Модель тематико-иерархического разграничения доступа

Правило 4.

Инициализация субъектом s нового субъекта s' посредством воздействия на объект источник o неопасна и может быть МБС разрешена тогда и только тогда, когда мультирубрика субъекта доминирует над мультирубрикой объекта-источника, при этом МБС присваивает новому субъекту мультирубрику, тождественную мультирубрике инициализирующего субъекта:

$$f_m[o] \leq f_m[s] \equiv f_m[s']$$

Инициализация нового субъекта $Create(s_m, o) \rightarrow s'$



Модель тематико-иерархического разграничения доступа

7. Переходы системы $\Sigma_{\text{ТИИ}}$, обусловленные запросами на предоставление множественных доступов, санкционируются МБО на основе следующего правила:

Правило 5. *Одновременный множественный доступ субъекта s к объектам $o_1, o_2, \dots$ или субъектов $s_1, s_2, \dots$ к объекту o может быть разрешен (неопасен) тогда и только тогда, когда выполняются следующие условия:*

- при доступе по чтению

$$f_M[s] \geq \cup_M \{ f_M[o_1], f_M[o_2], \dots \}$$

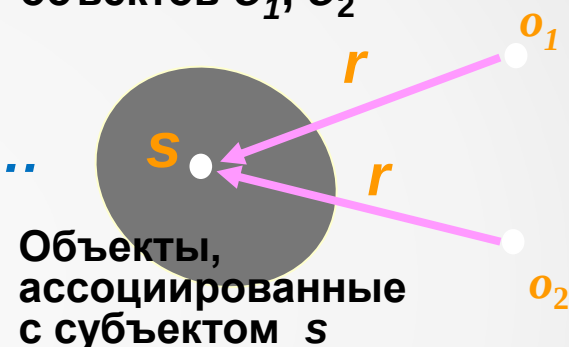
$$f_M[o] \leq \cup_M \{ f_M[s_1], f_M[s_2], \dots \}$$

- при доступе по записи

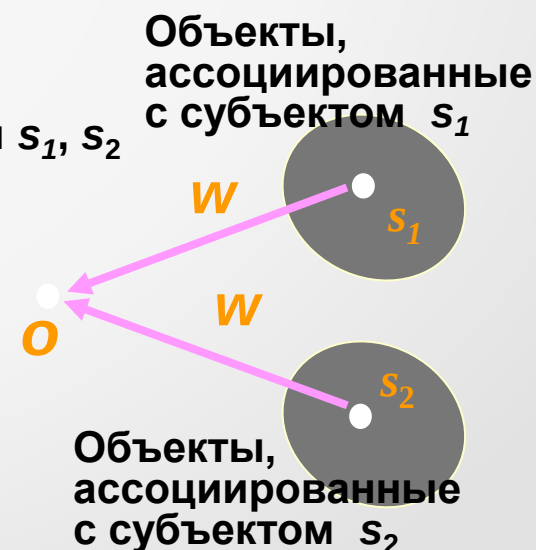
$$f_M[s] \leq \cap_M \{ f_M[o_1], f_M[o_2], \dots \}$$

$$f_M[o] \geq \cap_M \{ f_M[s_1], f_M[s_2], \dots \}$$

Чтение (r) субъектом s из объектов o_1, o_2



Запись (w) субъектами s_1, s_2 в объект o



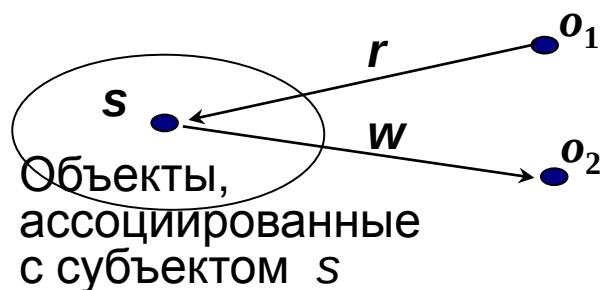
Теорема 1

В системе $\Sigma_{T_{ин}}$ с отображением множества субъектов и объектов доступа на множество тематических мультирубрик, в которой доступы санкционируются по правилам 1, 2, 3, 4 и 5, реализуется множество только таких потоков, которые удовлетворяют тематическому критерию безопасности

Доказательство

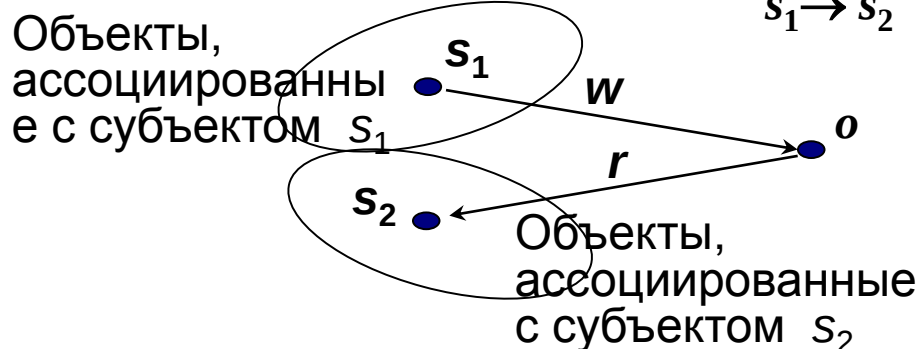
Поток между объектами

$o_1 \rightarrow o_2$



Поток между субъектами

$s_1 \rightarrow s_2$



По условиям теоремы при санкционировании потока $o_1 \rightarrow o_2$ имеем:

$$f_M[s] \geq f_M[o_1] \quad \wedge \quad f_M[o_2] \geq f_M[s]$$

следует, что: $f_M[o_2] \geq f_M[o_1]$

условиям теоремы при санкционировании потока $s_1 \rightarrow s_2$ имеем

$$f_M[s_2] \geq f_M[o]$$

$$f_M[s_2] \geq f_M[s_1]$$

Отсюда

Аналогично по

$$f_M[s_1] \leq f_M[o] \quad \wedge$$

Отсюда следует, что: