К семинару

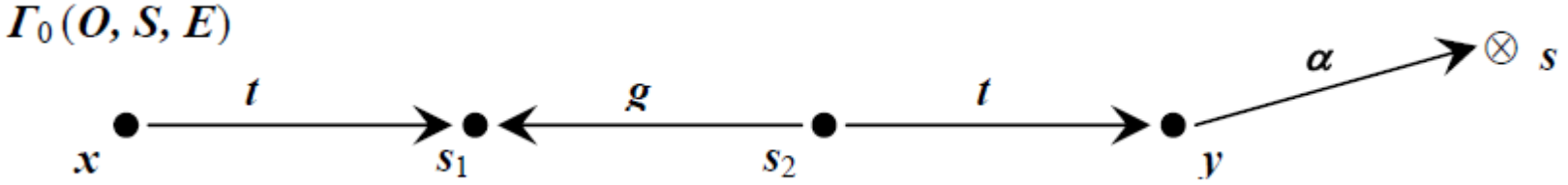
Описать модель и команды модели Take-Grant в терминах модели HRU.

Переформулировать правила и основные теоремы модели Take-Grant для права “Own” – как замены объединения правил “tg”

Рассмотреть изменение правил NWD и NRU на противоположные NRD и NWU – какими свойствами будет обладать эта мандатная модель и для каких целей безопасности может быть использована.

Задание 1.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$, в которой сущности x и y связаны tg-путем.

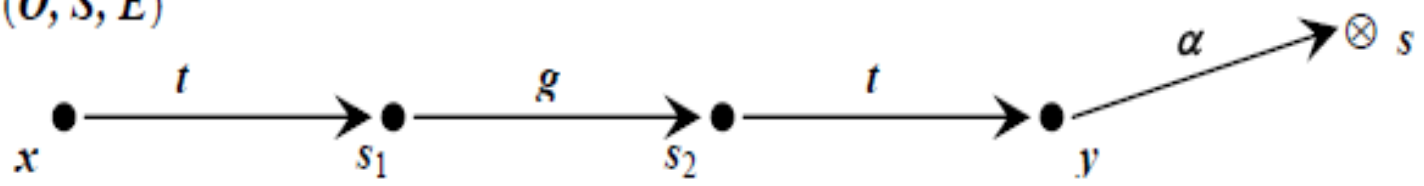


Задание: построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.

Задание 2.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$, в которой сущности x и y связаны tg-путем.

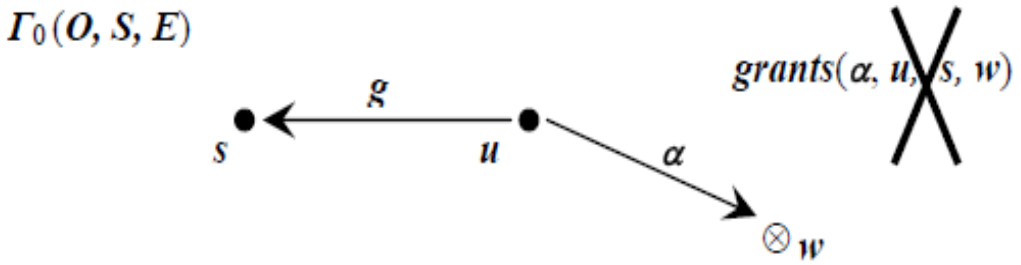
$\Gamma_0(O, S, E)$



Задание: построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.

Задание 3.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0(O, S, E)$.



Установленная для системы политика безопасности запрещает любым субъектам (владельцам) предоставлять право α на "свои" объекты другим субъектам (но не запрещает субъектам, которые владеют правами t ("брать") на какие-либо субъекты, брать у них права на их объекты).

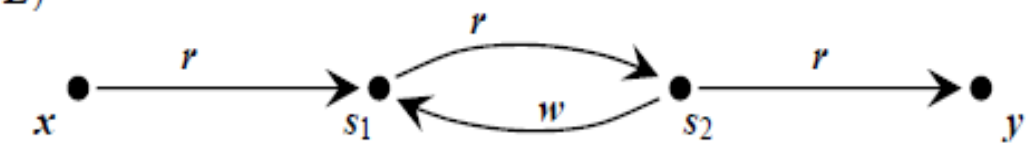
Кроме субъекта s, субъект u может быть связан tg-путем с другими субъектами.

Задание: построить систему команд получения субъектом s прав доступа α на объект w от субъекта u, при условии того, что команда $grants(\alpha, u, s, w)$ не может быть задействована.

Задание 4.

Пусть имеется система субъектов и объектов доступа, представленная Графом доступов $\Gamma_0 (O, S, E)$.

$\Gamma_0 (O, S, E)$



Пусть неявные каналы чтения, генерируемые различными командами "де-факто" имеют следующую стоимость: - $r_{spy} = 1$, $r_{post} = 2$, $r_{find} = 3$ и $r_{pass} = 4$.

Задание: Применяя команды "де-факто", сгенерировать все возможные неявные каналы чтения субъектом x информации из субъекта y, и сравнить их стоимость.

Задание 5.

Пусть имеется мандатная система доступа $\Sigma(v_0, Q, \mathcal{F}_T)$, в которой решетка уровней безопасности Λ_L является линейной и имеет три уровня – l_1, l_2, l_3; $l_1 > l_2 > l_3$; $l_1 > l_3$.

Пусть имеется следующая система субъектов (пользователей) доступа:

u_1 – администратор системы;
u_2 – руководитель предприятия;
u_3 – делопроизводитель;
u_4 – user, т.е. рядовой непривилегированный пользователь.

Пусть имеется следующая система объектов доступа:

o_1 – системное ПО;
o_2 – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";
o_3 – документ "Приказ о поощрении работников по случаю Дня Предприятия";
o_4 – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).

Обосновать и составить систему уровней допусков пользователей, грифов секретности объектов доступа и матрицу доступа $A[u,o]$.

Задание 6.

Пусть имеется мандатная система доступа $\Sigma(v_0, Q, \mathcal{F}_T)$, в которой решетка уровней безопасности Λ_L является линейной и имеет три уровня – l_1, l_2, l_3; $l_1 > l_2 > l_3$; $l_1 > l_3$.

Пусть имеется следующая система субъектов (пользователей) доступа:

u_1 – администратор системы;
u_2 – руководитель предприятия;
u_3 – делопроизводитель;
u_4 – user, т.е. рядовой непривилегированный пользователь.

Пусть имеется следующая система объектов доступа:

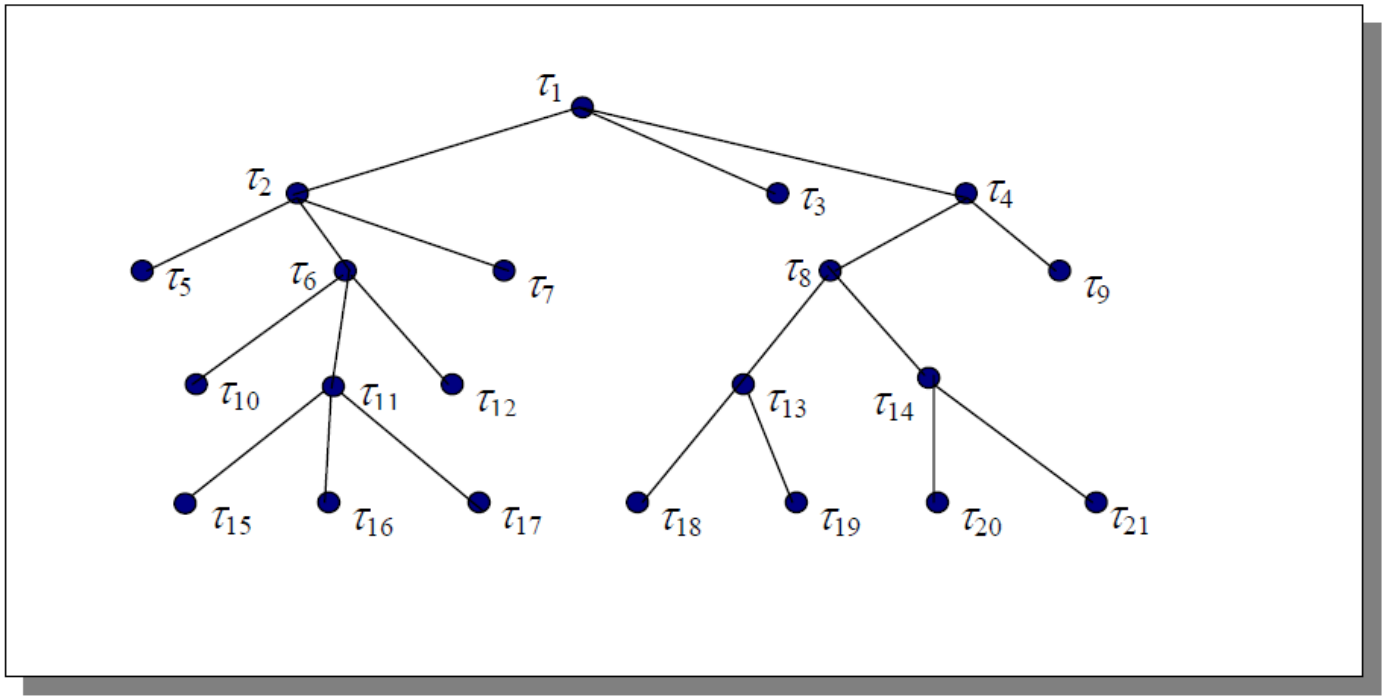
o_1 – системное ПО;
o_2 – документ "Стратегия выхода предприятия на новые рынки сбыта продукции";
o_3 – документ "Приказ о поощрении работников по случаю Дня Предприятия";
o_4 – АИС "Борей" (прием, обработка и исполнение заказов клиентов) (ПО и БД).

Составить и обосновать систему допусков и грифов секретности для двух состояний системы:

Состояние I – Подготовка (разработка) документа o_2.
Состояние II – Документ o_2 утвержден и введен в действие.

Задание 7.

Пусть имеется иерархический тематический рубрикатор. Для тематической классификации сущностей системы (субъектов и объектов доступа) использованы мультирубрики:

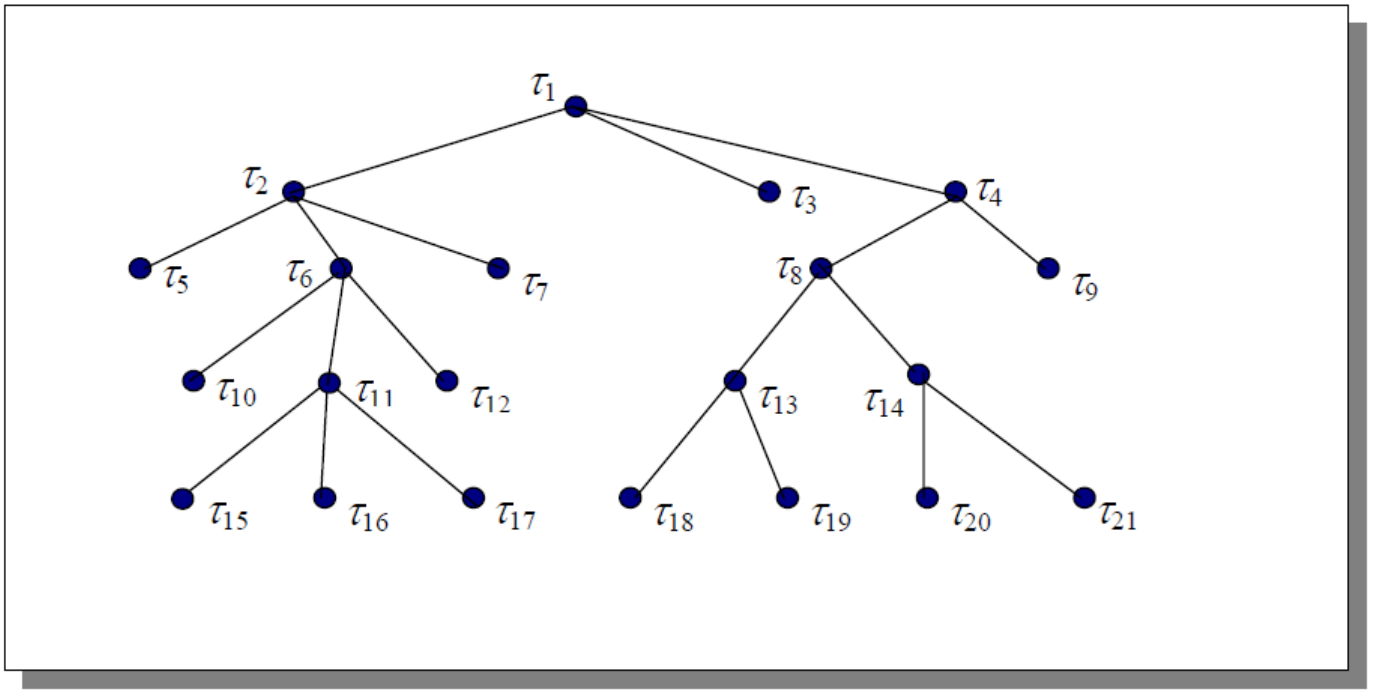


$\mathcal{T}^{M}_1 = \{\tau_5, \tau_6\}$; $\mathcal{T}^{M}_2 = \{\tau_{11}, \tau_{12}\}$; $\mathcal{T}^{M}_3 = \{\tau_3, \tau_8\}$; $\mathcal{T}^{M}_4 = \{\tau_6, \tau_8\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$; $\mathcal{T}^{M}_6 = \{\tau_{13}, \tau_9\}$;
$\mathcal{T}^{M}_7 = \{\tau_{15}, \tau_{16}, \tau_{14}\}$.

Определить отношения доминирования (уже, шире, несравнимо) между следующими мультирубриками:
$\mathcal{T}^{M}_2$ и $\mathcal{T}^{M}_1$; $\mathcal{T}^{M}_7$ и $\mathcal{T}^{M}_4$; $\mathcal{T}^{M}_5$ и $\mathcal{T}^{M}_3$; $\mathcal{T}^{M}_6$ и $\mathcal{T}^{M}_4$.

Задание 8.

Пусть имеется иерархический тематический рубрикатор. Для тематической классификации сущностей системы (субъектов и объектов доступа) использованы мультирубрики:



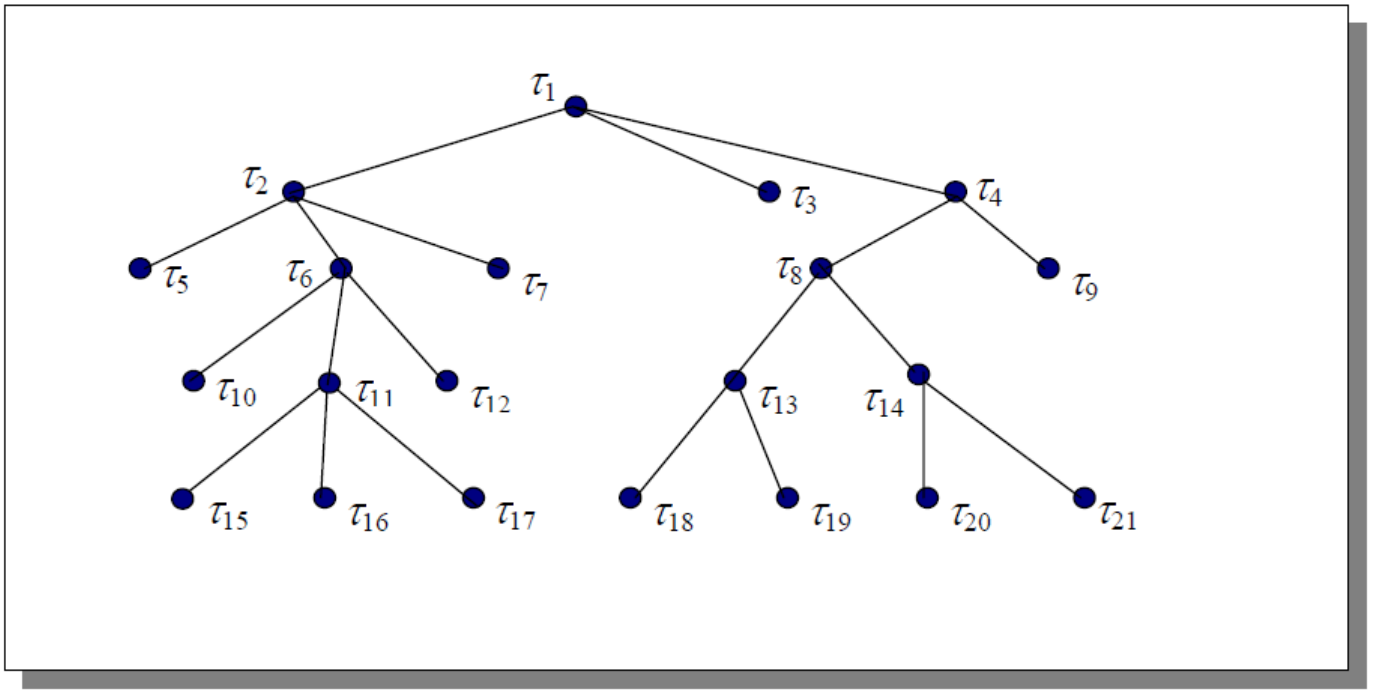
$\mathcal{T}^{M}_1 = \{\tau_5, \tau_6\}$; $\mathcal{T}^{M}_2 = \{\tau_{11}, \tau_{12}\}$; $\mathcal{T}^{M}_3 = \{\tau_3, \tau_8\}$; $\mathcal{T}^{M}_4 = \{\tau_6, \tau_8\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$; $\mathcal{T}^{M}_6 = \{\tau_{13}, \tau_9\}$;
$\mathcal{T}^{M}_7 = \{\tau_{15}, \tau_{16}, \tau_{14}\}$.

Построить объединение следующих мультирубрик:

$\mathcal{T}^{M}_3 \cup_M \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_4 \cup_M \mathcal{T}^{M}_6$; $\mathcal{T}^{M}_2 \cup_M \mathcal{T}^{M}_3$; $\mathcal{T}^{M}_1 \cup_M \mathcal{T}^{M}_2$; $\mathcal{T}^{M}_4 \cup_M \mathcal{T}^{M}_7$.

Задание 9.

Пусть имеется иерархический тематический рубрикатор. Для тематической классификации сущностей системы (субъектов и объектов доступа) использованы мультирубрики:



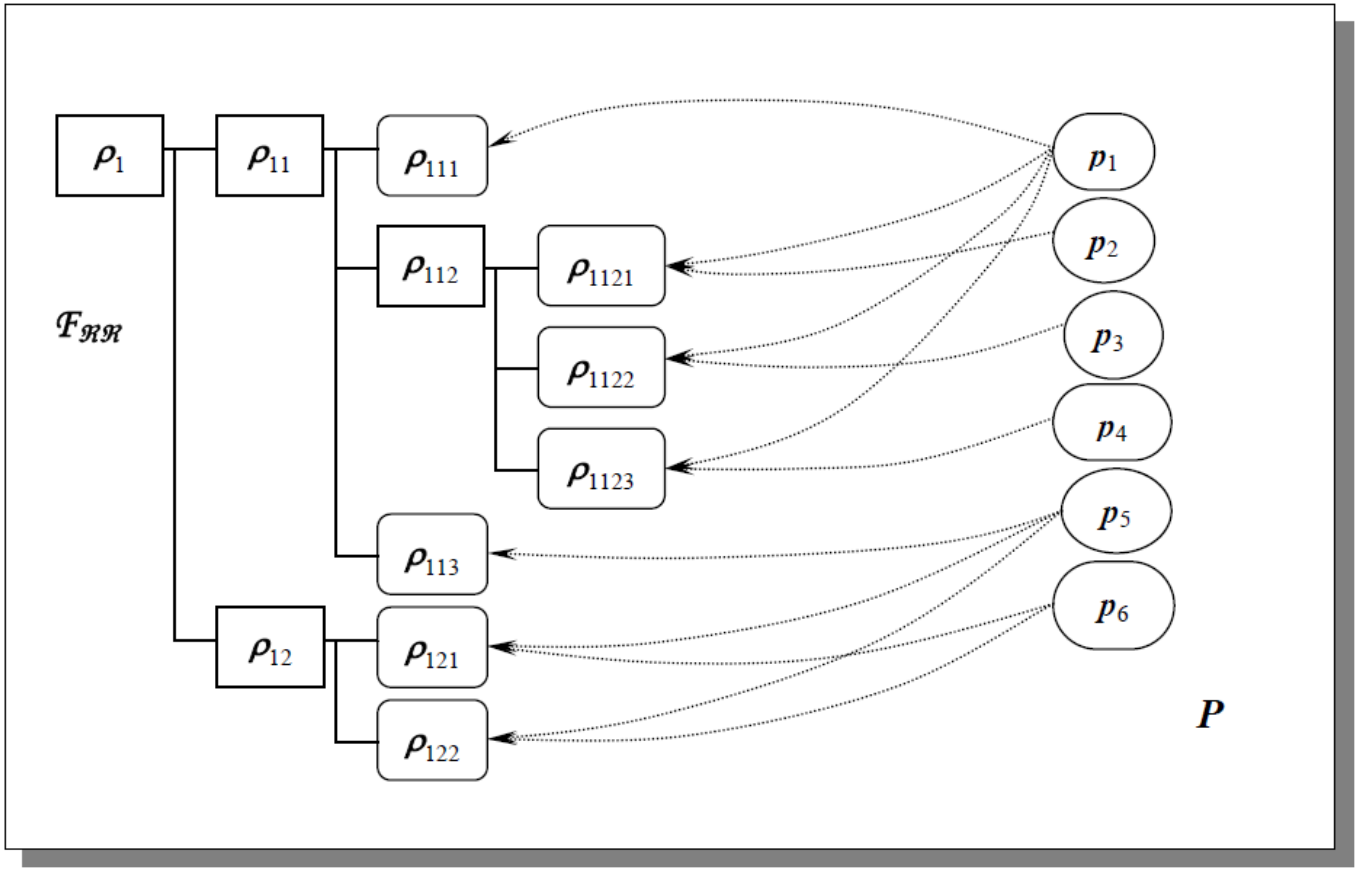
$\mathcal{T}^{M}_1 = \{\tau_5, \tau_6\}$; $\mathcal{T}^{M}_2 = \{\tau_{11}, \tau_{12}\}$; $\mathcal{T}^{M}_3 = \{\tau_3, \tau_8\}$; $\mathcal{T}^{M}_4 = \{\tau_6, \tau_8\}$; $\mathcal{T}^{M}_5 = \{\tau_{12}, \tau_{13}\}$; $\mathcal{T}^{M}_6 = \{\tau_{13}, \tau_9\}$;
$\mathcal{T}^{M}_7 = \{\tau_{15}, \tau_{16}, \tau_{14}\}$.

Построить пересечение следующих мультирубрик:

$\mathcal{T}^{M}_3 \cap_M \mathcal{T}^{M}_5$; $\mathcal{T}^{M}_4 \cap_M \mathcal{T}^{M}_6$; $\mathcal{T}^{M}_2 \cap_M \mathcal{T}^{M}_3$; $\mathcal{T}^{M}_1 \cap_M \mathcal{T}^{M}_2$; $\mathcal{T}^{M}_4 \cap_M \mathcal{T}^{M}_7$.

Задание 10.

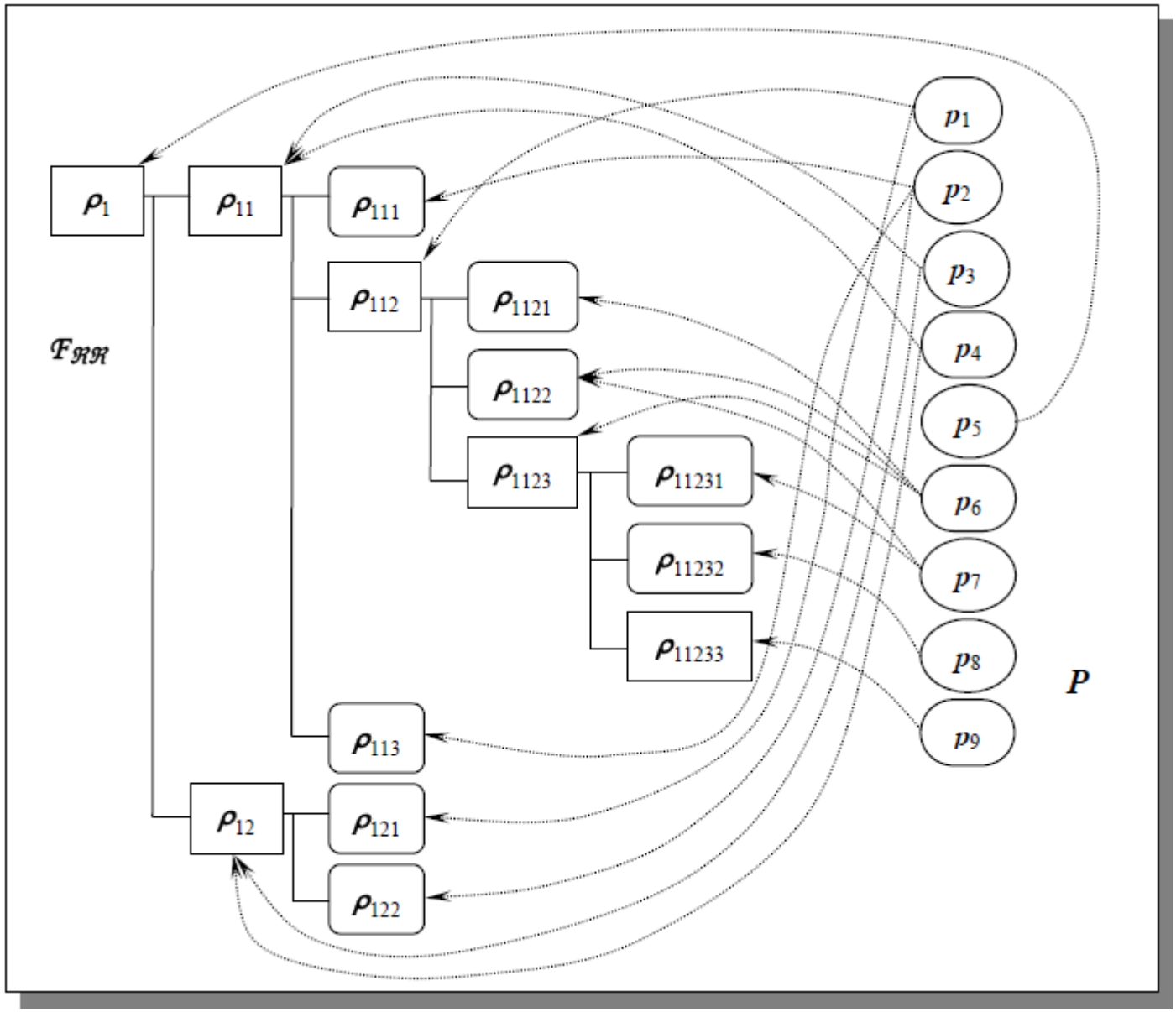
Пусть имеется система иерархически организованных ролей $\mathcal{R}$ ($\rho \in \mathcal{R}$), представленная на рис. Ролям назначены полномочия из конечного множества P ($p \in P$).



Определить тип наделения ролей полномочиями (листовой таксономический, листовой нетаксономический, иерархически охватный).

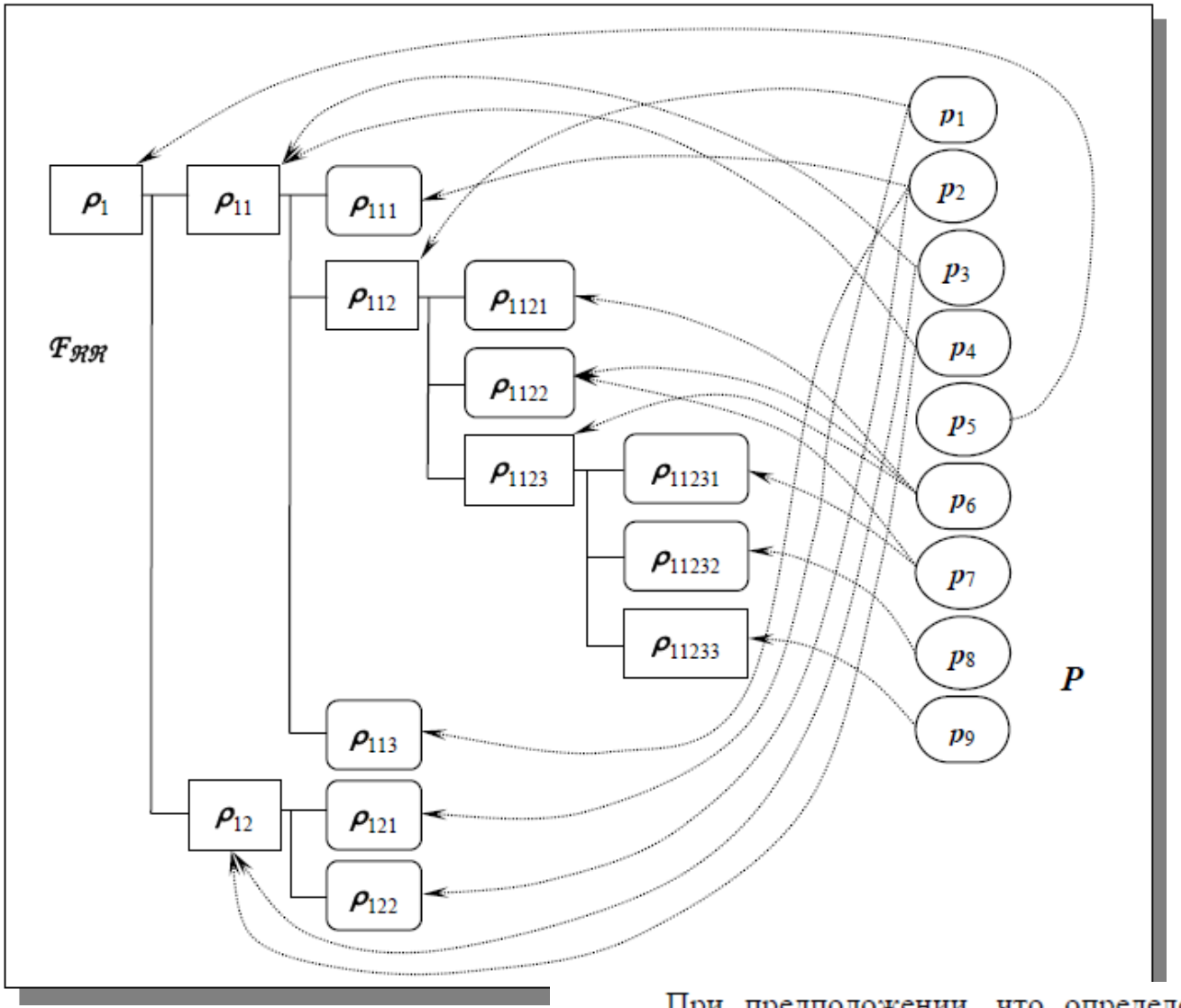
Определить полномочия роли ρ_{11}.

Задание 11.



Определить полномочия роли ρ_{11}.

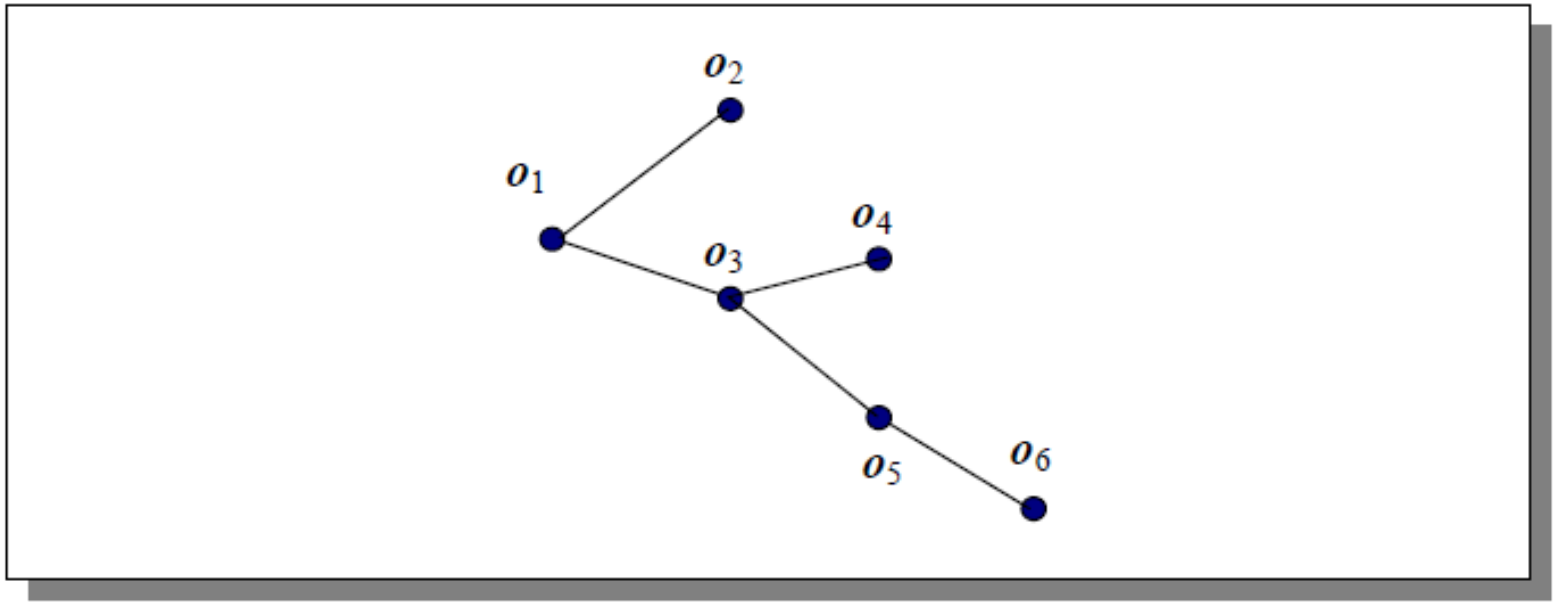
Задание 12.



При предположении, что определенные полномочия могут быть назначены только ролям определенного уровня иерархии, определить возможный порядок (отношение доминирования) на множестве полномочий.

Задание 13.

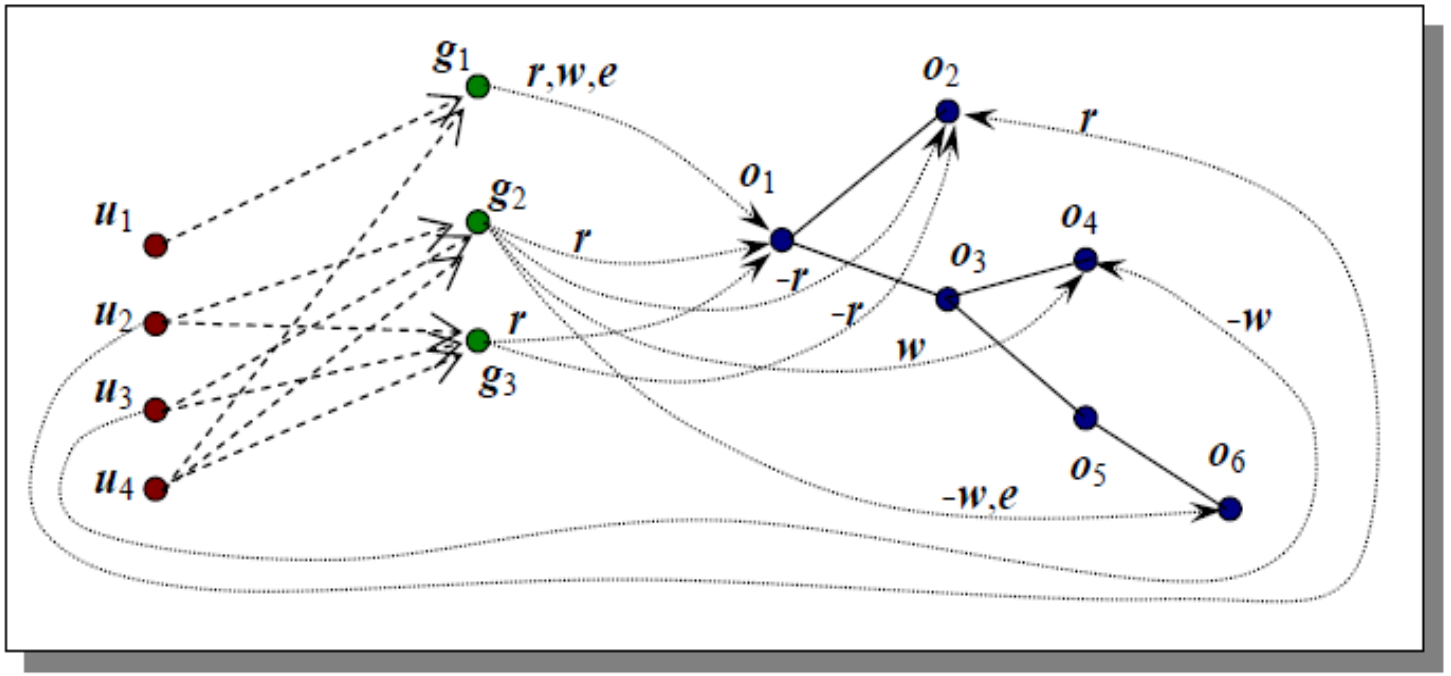
Пусть имеется иерархически организованная система объектов доступа.



Составить матрицу смежности объектов доступа **H** (строка – куда; столбец – кто входит; диагональные элементы равны 0) и матрицу итоговой достижимости $\mathbf{H}^S$ (за один шаг, за два шага и т.д.).

Задание 14.

Пусть имеется иерархически организованная система объектов доступа, четыре пользователя u_1, u_2, u_3 и u_4, объединенных в три рабочих группы g_1, g_2 и g_3. Вхождение пользователей в рабочие группы, групповые и индивидуальные назначения доступа показаны на рис.



Задание. Приведите матричные соотношения и определите итоговые права доступа пользователей по чтению и записи.

Задание 15, 16.

Пусть имеется два субъекта: s_1 (доверенный пользователь, *admin*) и s_2 (обычный пользователь, *user*).

Пусть имеется два каталога (объекты) o_1 и o_2, владельцами которых являются пользователи s_1 и s_2, соответственно. В каталоге имеется объект o_3 с секретной информацией.

Права доступа в системе заданы исходным состоянием матрицы доступа:

	o_1 - secret	o_2 - no secret	o_3 - secret
s_1	*own,r,w,e*	*r,w,e*	*own,r,w,e*
s_2	-	*own,r,w,e*	-

	o_1 - secret	o_2 - no secret	o_3 - secret
s_1	*own,r,w,e*	*r*	*own,r,w,e*
s_2	-	*own,r,w,e*	-

Задание. По классическому сценарию атаки с помощью троянской программы в системах, функционирующих на основе модели **HRU**, постройте систему команд перехода и соответствующие изменения матрицы доступа.