Теоретичні основи захисту інформації

Самостійна робота №1

Перевірив:

_____

Виконав:

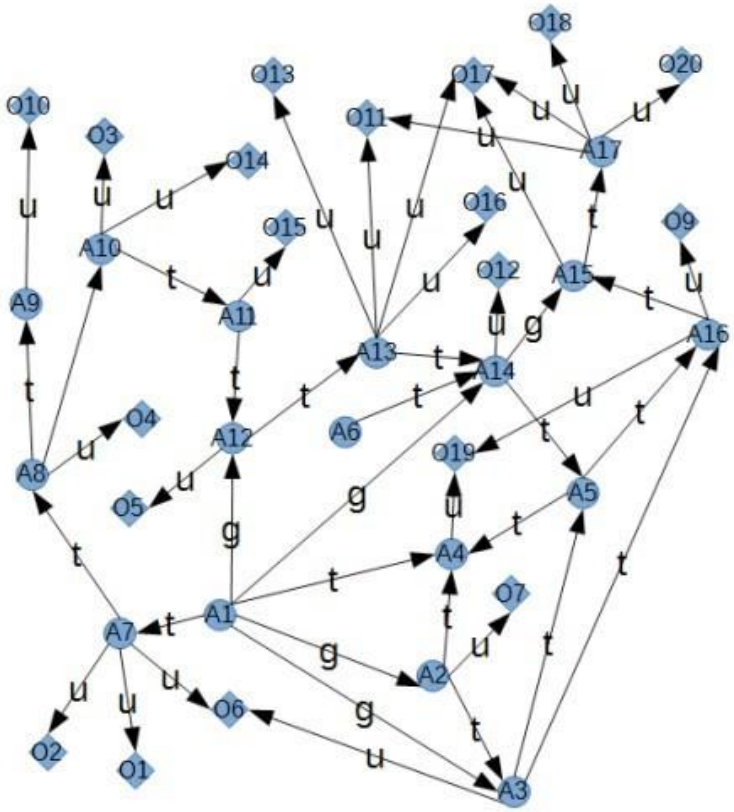
студент II курсу

групи ФБ-01

Сахній Н.Р.

Завдання 1.

Відповідно моделі Take-Grant у графі стану системи знайдіть по два приклади сценаріїв санкціонованого отримання та викрадення прав. Опишіть ці сценарії та сформулюйте, які умови роблять їх можливими.



Завдання №1

I Отримання прав

1. grant(α, A_1, A_{12}, obj)

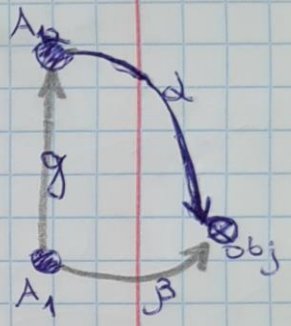
Умова виконання:

$A_1 \in S$, $(A_1, A_{12}, g) \in E$,

$(A_{12}, obj, \beta) \in E$

$A_1 \neq obj$, $\alpha \subseteq \beta$

obj - деякий об'єкт, на який суб'єкт A_1 має право β



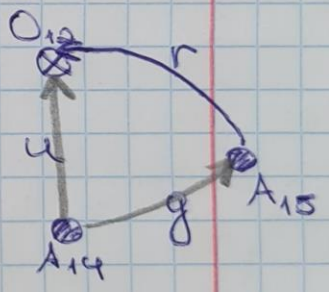
2. grant(r, A_{14}, A_{15}, O_{12})

Умова виконання:

$A_{14} \in S$, $(A_{14}, A_{15}, g) \in E$

$(A_{15}, O_{12}, u) \in E$

$A_{14} \neq O_{12}$, $r \subseteq u$



I Викреслення прав

1. take(α, A_3, A_5, obs)

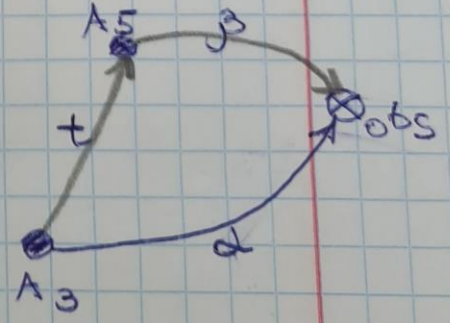
Умова виконання:

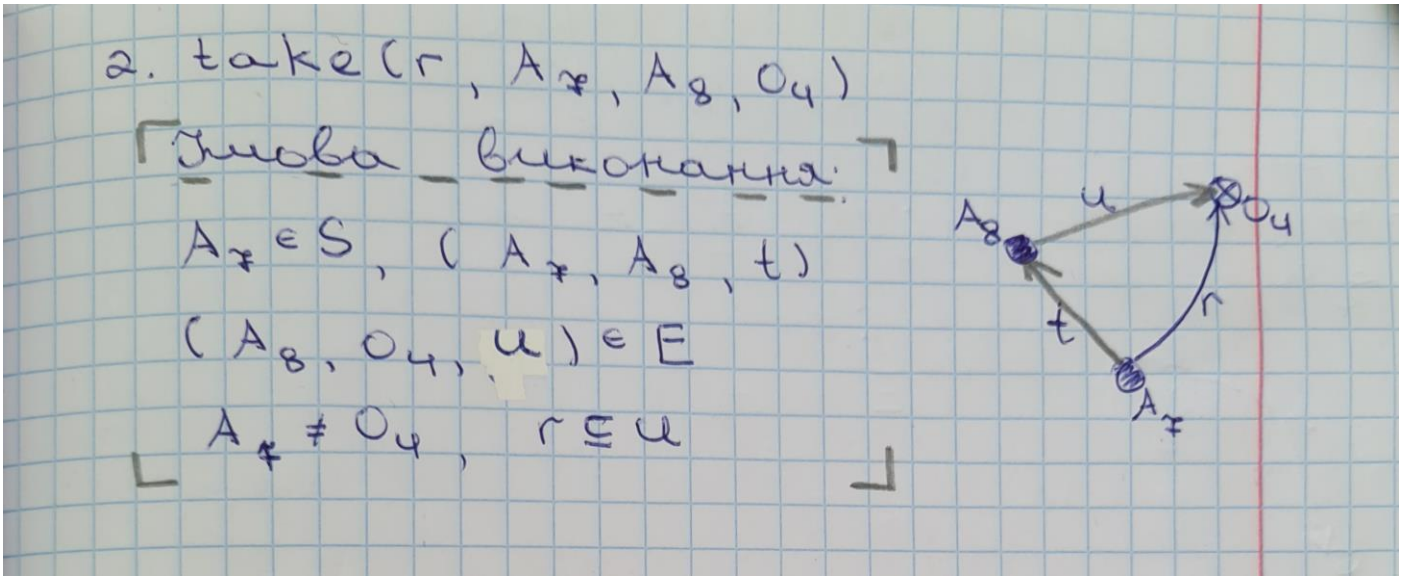
$A_3 \in S$, $(A_3, A_5, t) \in E$

$(A_5, obs, \beta) \in E$

$A_3 \neq obs$, $\alpha \subseteq \beta$

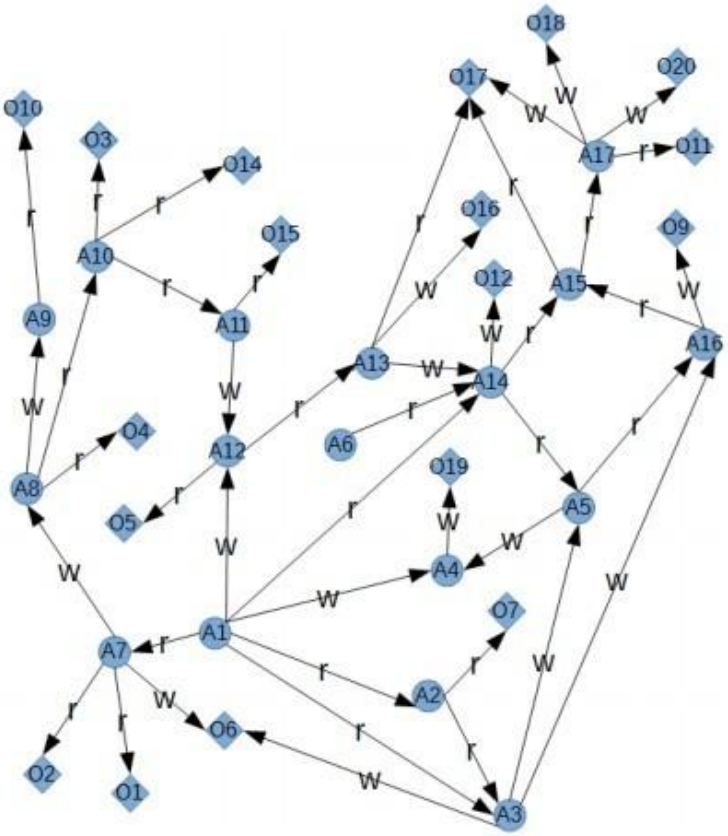
obs - деякий об'єкт, на який суб'єкт A_5 має право β

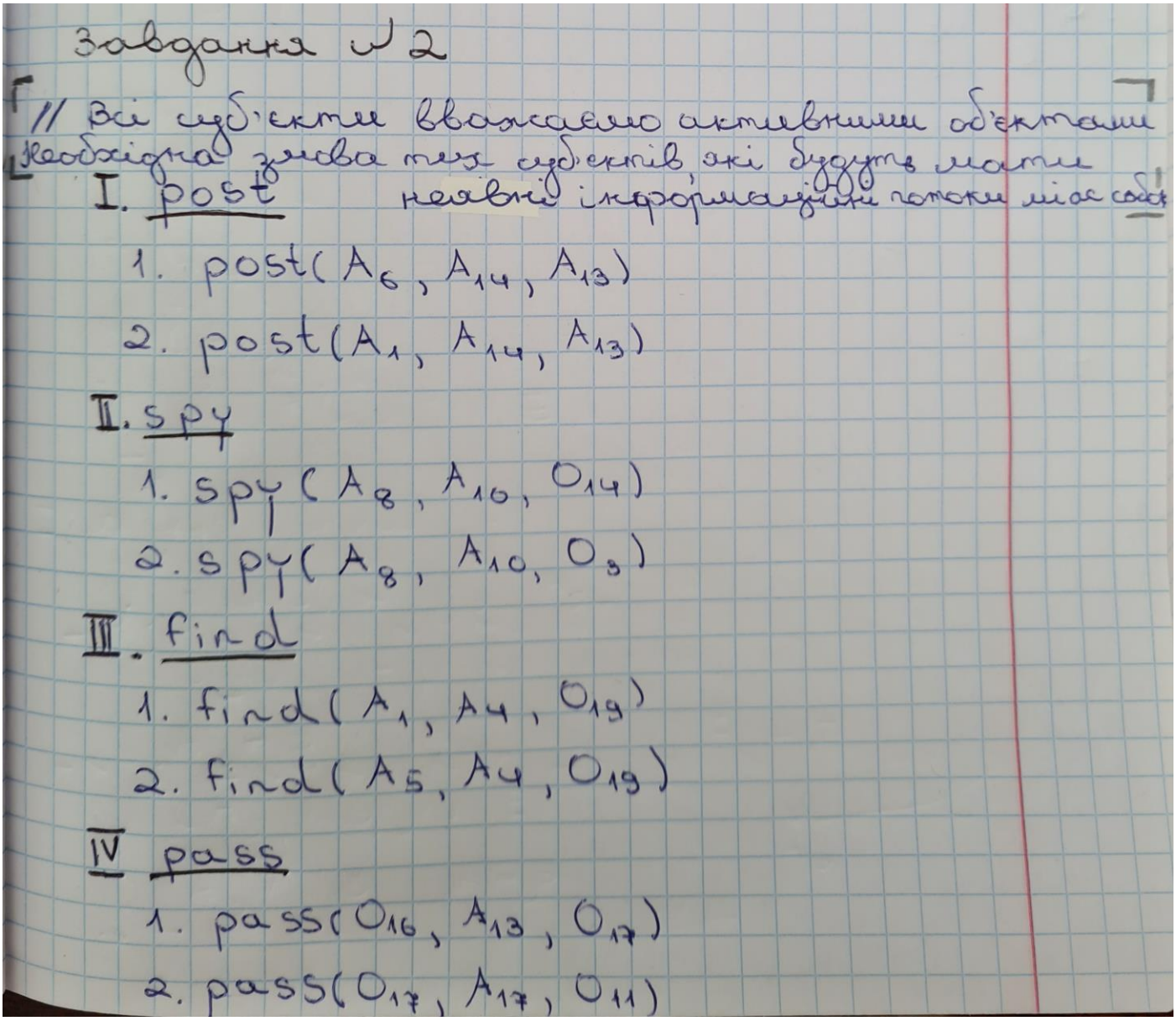




Завдання 2.

Послуговуючись розширеною моделлю Take-Grant та графом стану системи знайдіть по два приклади каналів *post*, *spy*, *find* та *pass*. Задля реалізації вказаних каналів, змова яких суб”єктів необхідна?





Завдання 3.

В деякій системі, що функціонує відповідно моделі MLS, рівні доступу суб'єктів {Sergant, Major, Colonel, Brigadir}, а мітки таємності документів {C,S,TS}. Документи можуть мати категорію {Nuclear, Chemical, Navy, Staff}. Сформулюйте правила роботи з документами в даній системі та запишіть матрицю доступу. При об'єднанні інформації з декількох документів, які мітки отримують вихідні документи? Які суб'єкти можуть виконувати операції по об'єднанню інформації з декількох документів?

1) Нехай наші суб'єкти будуть мати рівні доступу, розподілені наступним чином:
   {Brigadir} – TS
   {Colonel} та {Major} – S
   {Sergant} – C

2) Тоді нехай категорії документів матимуть наступні мітки таємності:
{Nuclear, Chemical} – TS
{Chemical, Navy}, {Navy} – S
{Staff} – C

3) Маємо, що правила роботи з документами будуть такі як далі наведено в таблиці:

Subject	**Integrity**
Brigadir	(TS,{Nuclear, Chemical})
Colonel	(S,{Chemical, Navy})
Major	(S,{Navy})
Sergant	(C,{Staff})

Отже, матриця доступу суб'єктів до категорій об'єктів (документів) матиме вигляд:

A	{Nuclear}	{Chemical}	{Navy}	{Staff}
Brigadir	rw-	rw-	---	---
Colonel	---	rw-	rw-	---
Major	---	---	rw-	---
Sergant	--	---	---	rw-

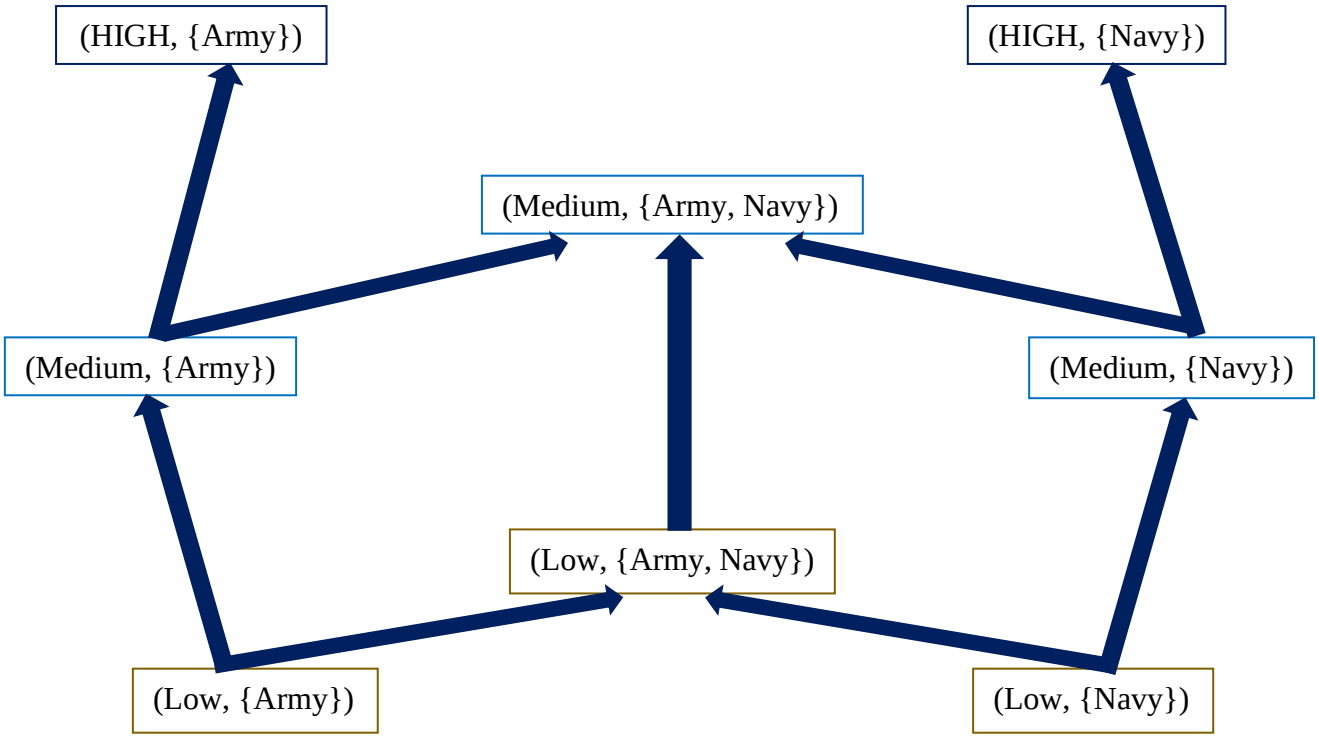
- При об'єднанні інформації з декількох документів, новостворені вихідні документи будуть мати найвищі мітки таємності серед тих об'єктів, що об'єднювалися, а множина тематик буде об'єднаням всіх тематик, що були в документах.
- Суб'єкти можуть виконувати операції по об'єднанню інформації з декількох документів, якщо їхня мітка доступності є на рівень вищої, ніж мітка таємності об'єктів (документів)

Завдання 4.

Рівні цілісності в системі {Low, Medium, High}. Категорії документів Navy та Army. Атрибути суб'єктів та об"єктів наведено у таблицях:

Subject	**Integrity**		**Object**	**Integrity**
Colonel	(HIGH,{Navy})		Army position	(HIGH,{Army})
Major	(MEDIUM,{Army})		Fleet position	(HIGH,{Navy})
Captain	(MEDIUM,{Army, Navy})		Number of army units	(MEDIUM,{Army})
Soldier	(LOW,{Army, Navy})		Number of navy units	(MEDIUM,{Navy})
			Cost of army units	(LOW,{Army})
			Cost of navy units	(LOW,{Navy})

Зобразимо **решітку класифікації**:



Послуговуючись моделлю Біби з правилами low-watermark, дайте відповідь на наступні питання:

4.1 Скільки класів захисту буде отримано з n рівнів цілісності та m категорій?
Кількість класів захисту → $n \cdot 2^m$

4.2 Чи може Colonel змінювати кількість navy units?
Так, може

4.3 Чи може Colonel змінювати кількість navy units опісля читання Cost of navy units?
Ні, не може

4.4 Чи зможе Major змінювати кількість army units, після того, як Colonel прочитав ці дані?
Ні, не може

4.5 Чи може Major змінювати Cost of army units, після того, як він прочитав Fleet position?
Ні, не може

4.6 Чи зможе Captain обчислити загальну вартість засобів захисту (army + navy units)?
Ні, не може

4.7 Чи зможе Soldier дізнатися кількість navy units, після того, як він змінив ці дані?
Ні, не може

Завдання 5.

Відповідно моделі Кітайської стіни існують такі класи конфліктів інтересів: {CompanyA,CompanyB}, {CompanyC,CompanyD}, {CompanyE,CompanyF,CompanyG}, {BankA,BankB,BankC}, {BankD,BankE}, {BankF,BankG}.
Для даної послідовності операцій вкажіть, які операції можуть бути виконані, а які – ні.

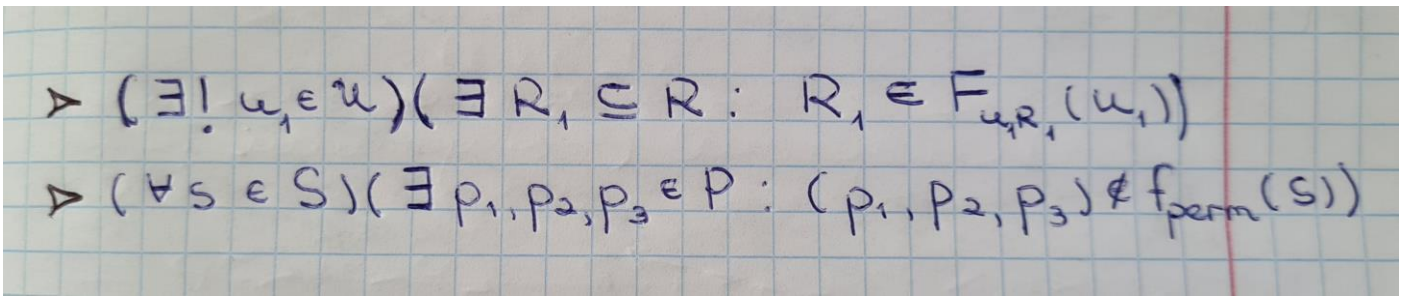
// Суб'єкту надається доступ по читанню, тільки якщо доступ до запитуваної множини ресурсів вже було надано або він не знаходиться у конфлікті інтересів з запитаним класом.

5.1 Read{CA,BB} – *Ні, не може;*
5.2 Read{CD,BB} – *Так, може;*
5.3 Read{CC,BF} – *Так, може;*
5.4 Read{CD,BE} – *Ні, не може;*
5.5 Read{CE,BA} – *Так, може;*
5.6 Read{CA,BG} – *Так, може;*
5.7 Read{CA,BD} – *Так, може;*
5.8 Read{CF,BG} – *Ні, не може;*

Завдання 6.

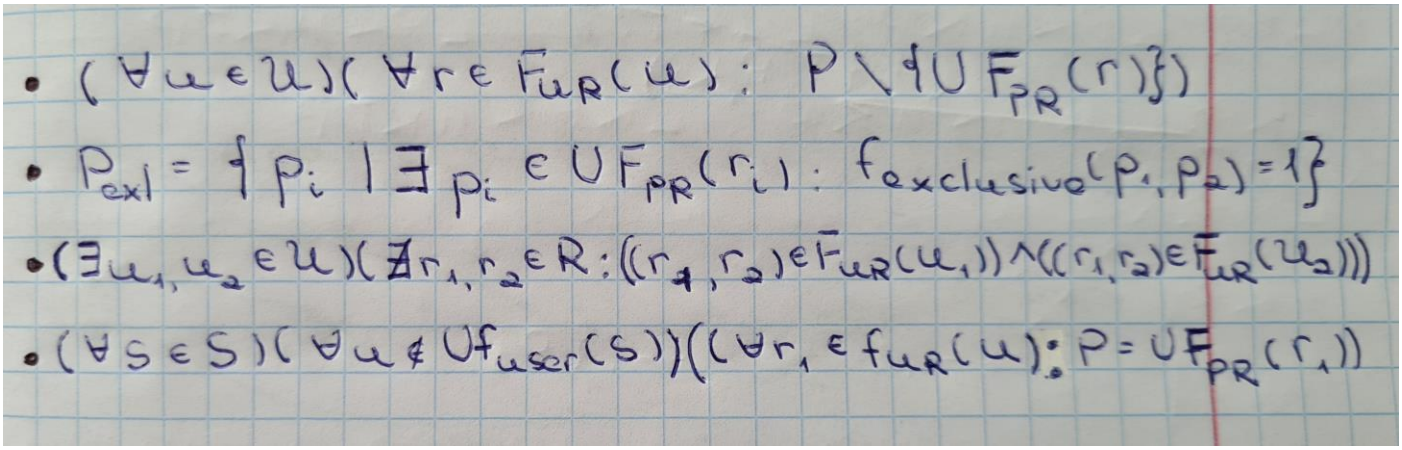
Запишіть модель системи з рольовим керуванням доступом з такими обмеженнями:

- Деяка множина ролей не може належати двом або більше користувачам.
- Використання повноважень (p1, p2, p3) одночасно виключено для всіх активних ролей системи.



Та визначіть для данної системи:

- Яких повноважень немає у жодного користувача.
- Множину повноважень, якими не може володіти користувач, який має роль R1.
- Які ролі не можуть одночасно активувати користувачі u1 та u2.
- Які сукупні повноваження матимуть користувачі, які не мають відкритих сесій.



Завдання 7.

Для вказаного призначення ролей та повноважень наведіть матрицю доступу.

User	**Role**		**Role**	**Permission**
Alice	Radiologist		Nurse	(read, prescription)
Alice	GP		GP	(read, prescription)
Bob	GP		GP	(write, prescription)
Charlie	Radiologist		GP	(read, history)
David	Nurse		Radiologist	(read, history)
			Radiologist	(insert, image scan)

* prescription, history, image scan – об’єкти системи.

Наведемо **матриця доступу:**

A	prescription	history	image scan
Alice	`rw-`	`r--`	`--i`
Bob	`rw-`	`r--`	`---`
Charlie	`---`	`r--`	`--i`
David	`r--`	`---`	`---`

* `r` – read, `w` – write, `i` – insert