Задача 1

Система в моделі HRU задана початковим станом та набором команд. Зробіть висновок відносно безпеки даної системи.

A	O_1	O_2	O_3	O_4
S_1	r_2r_3	r_1r_4	r_3r_4	r_1r_3
S_2	r_1r_2	r_2r_4	r_1r_4	r_1r_3
S_3	r_2r_3	r_1r_2	r_1r_3	r_3r_4
S_4	r_2r_4	r_1r_3	r_2r_3	r_1r_4

command 1: if r_2 in $A[S_3,O_1]$ and r_2 in $A[S_2,O_2]$
{enter r_4 in $A[S_4,O_3]$; enter r_3 in $A[S_3,O_3]$;}

command 2: if r_4 in $A[S_1,O_2]$ and r_3 in $A[S_3,O_3]$
{enter r_4 in $A[S_4,O_4]$; delete r_3 from $A[S_2,O_2]$;}

command 3: if r_3 in $A[S_3,O_1]$ and r_3 in $A[S_2,O_3]$
{enter r_2 in $A[S_2,O_2]$; enter r_1 in $A[S_1,O_1]$;}

command 4: if r_3 in $A[S_3,O_3]$ and r_4 in $A[S_1,O_2]$
{enter r_3 in $A[S_2,O_2]$; enter r_1 in $A[S_2,O_3]$;}

Задача 2

Нехай в моделі MLS решітка рівнів таємності (L<=M<=H) та множина тематик (A,B,C,D).
Відобразіть графічно співвідношення між елементами LAC, LBD, MA, MAB, HB, HAC.
Вкажіть найменшу верхню та найбільшу нижню границі для даного набору елементів.

Задача 3

Результат виконання команди `ls -l` для деякого каталогу:

```
-rw-r--r-- 1 usr1 root 123  Mar 20 20:16 file1
-rw-rw---- 1 usr2 grp1 456  Mar 20 20:17 file2
dr--rwx--- 2 usr1 grp2 4096 Mar 20 20:16 notes
-rw-r-x--x 1 usr2 grp2 111  Mar 20 20:17 script.sh
```

Користувач *usr1* є членом групи *grp1*, а користувач *usr2* – членом груп *grp1* і *grp2*.
Подайте інформацію про права доступу (*own, r, w, x*) суб'єктів (користувачів і груп) до об'єктів (файлів і каталогів) у вигляді матриці доступу.

Задача 4

Деякий каталог у файловій системі містить такі файли (підкаталогів немає):

aardvark	feret	koala	porpoise	unicorn
bober	grunion	llama	quacker	vicuna
bonefish	hyena	marmot	rabbit	weasel
dingo	ibex	nuthatch	seehorse	yak
emu	jellyfish	ostrich	tuna	zebu

Яким буде вміст файлу *mypets* після виконання у цьому каталозі послідовності команд:

```
ls *[ab]*e* > mypets
ls [mry]* >> mypets
```

Задача 5

Індексний дескриптор (i-node) у системі Linux містить 12 дискових адрес для блоків даних, а також по одній адресі непрямих блоків першого, другого і третього рівнів. Чому дорівнює максимальний розмір файлу, якщо кожний непрямий блок містить до 256 дискових адрес, а розмір дискового блоку дорівнює 1 кбайт?

Задача 6

Наведено текст умовної програми:

```
#include <string.h>
main (int argc, char *argv[]) {
    char str1[10];
    strcpy (str1, argv[1]);
}
```

Які вразливості може мати дана програма?
Опишіть механізми експлуатації даних вразливостей.

Задача 7

Нехай для автентифікації на деякому сайті користувач вводить значення змінних $username та $passwd, які підставляються у SQL - запит "select * from users where username='$username' and passwd='$passwd'".
Позитивне рішення щодо автентифікації приймається, якщо у БД знайдено не нульову кількість відповідних записів.
Припустимо, зловмисник знає username одного з користувачів (наприклад, vasia). Напишіть вхідні дані, які б могли дати можливість обійти автентифікацію та поясніть сценарій такої атаки.

Задача 8

Побудуйте систему RSA, взявши $p=13, q=17, e=23$. Підпишіть вибране вами повідомлення.

Задача 9

Побудуйте повний період лінійної рекурентної послідовності, згенерованої лінійним регістром зсуву з характеристичним поліномом $x^3 + x^2 + 1$, починаючи з довільного ненульового стану.

Задача 10

Сформуйте спільний секретний ключ у схемі Діффі-Хеллмана, якщо $p=43, \alpha=3$, $k_A=5, k_B=7$. Опишіть покроково дії обох учасників схеми (Аліси та Боба) та результати їх обчислень.

Задача 11

Список дискреційного керування доступом до деякого файлу у файловій системі NTFS (ОС Windows 7) містить такі елементи:

DENY GENERIC_READ, GENERIC_WRITE група *Youngsters*
ALLOW READ користувач *Mishko*
ALLOW GENERIC_READ група *Programmers*

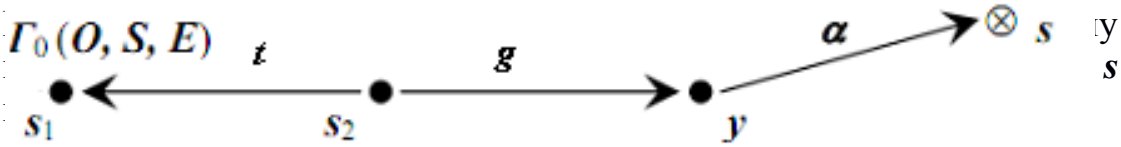
Чи зможе користувач *Mishko* прочитати вміст файлу, якщо він є членом груп *Programmers* і *Youngsters*? Відповідь обґрунтуйте.

Задача 12

Описати команди створення файлу, створення процесу, передачі прав зчитування на файл і передачі прав володіння у термінах моделі HRU.

Задача 13

Є система суб'єктів і об'єктів доступу, що подана графом доступів $\Gamma_0(O, S, E)$, у якій сутності s_1 і y пов'язані tg-шляхом:



Задача 14

За допомогою традиційної системи розмежування доступу Linux призначити права доступу користувачів u_1, u_2, u_3, u_4 до файлів o_1, o_2, o_3, o_4 згідно з заданою матрицею доступу:

	o_1	o_2	o_3	o_4
u_1	***r w***	***r***	***r***	**---**
u_2	***r***	***r w***	**---**	***r***
u_3	***r***	***r***	**---**	***r w***
u_4	***r***	***r***	***r***	**---**

При цьому визначити власника і групу для кожного з файлів. Кожний з користувачів є членом власної групи, яка має таку ж назву, як і ім'я користувача. Крім того, у системі є ***root*** і його відповідна група. Чи потрібно для реалізації заданих правил розмежування доступу вводити додаткові групи, додавати користувачів до інших груп? Хто з користувачів і по відношенню до яких об'єктів може порушити політику безпеки? Як виключити або зменшити таку можливість?

Задача 15

Записати формальну модель RBAC-системи з додатковими умовами:

- Не може існувати ролей, на які не авторизовано жодного користувача.
- Жоден з непривілейованих користувачів (U1) не може відкрити сеанс з набором повноважень, що включає множину P1.

Задача 16

Скількома способами можна вибрати набір довгострокових ключових елементів для шифру ДСТУ ГОСТ 28147-2009? Розгляньте випадки, коли ДКЕ можуть бути довільними відображеннями або повинні бути бієкціями.

Задача 17

Нехай явно призначені користувачам права доступу представлено в вигляді матриці **A**, а права доступу для груп — матриці **F**. Приналежність користувачів до груп задана матрицею **G**. Також задано матриці явних заборон, відповідно — **A1** и **F1**.
Напишіть формулу обчислення ефективних прав. (Враховуйте, що заборони мають пріоритет над явними дозволами.)