МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Теоретичні основи захисту інформації

Модульна контрольна робота – Частина 2

Перевірив:

_____

Виконав:

студент II курсу

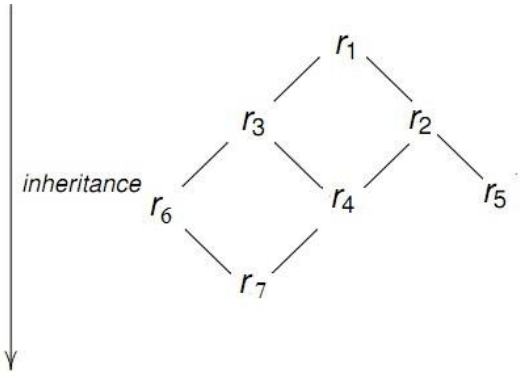
групи ФБ-01

Сахній Н.Р.

Завдання 1.

Для системи з рольовим керуванням доступом с заданим призначенням ролей і повноважень та ієрархією ролей знайти повноваження користувачів у вигляді матриці доступу.

$F_{UR}=\{(u_1;r_2),(u_2;r_2,r_3),(u_3;r_4),(u_4;r_5,r_6),(u_5;r_7\}$ та $F_{PR}=\{(r_2,p_1),(r_3,p_2),(r_4,p_3),(r_5,p_4),(r_6,p_5)\}$



	p_1	p_2	p_3	p_4	p_5
u_1	✖				
u_2	✖	✖			
u_3	✖	✖	✖		
u_4	✖	✖		✖	✖
u_5	✖	✖	✖		✖

Завдання 2.

Дана матриця доступу для деякої системи з рольовим керуванням доступом із заданою ієрархією ролей. Відомо, що користувач C має роль r_4. Також, будь який користувач може мати більше, аніж одну роль. Враховуючи принцип найменших повноважень, знайти розподіл ролейта повноважень для даної системи.

User Assignment

User	Role
A	r_2 r_6
B	r_5
C	r_4
D	r_6
E	r_3 r_4
F	r_3
G	r_2

×

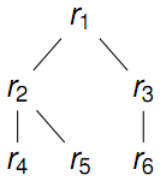
Permission Assignment

Role	Permission
r_1	
r_2	p_1 p_3
r_3	p_2
r_4	p_5 p_7 (p_1 p_3)
r_5	p_6 (p_1 p_3)
r_6	p_8 p_4 (p_2)

=

Access Matrix

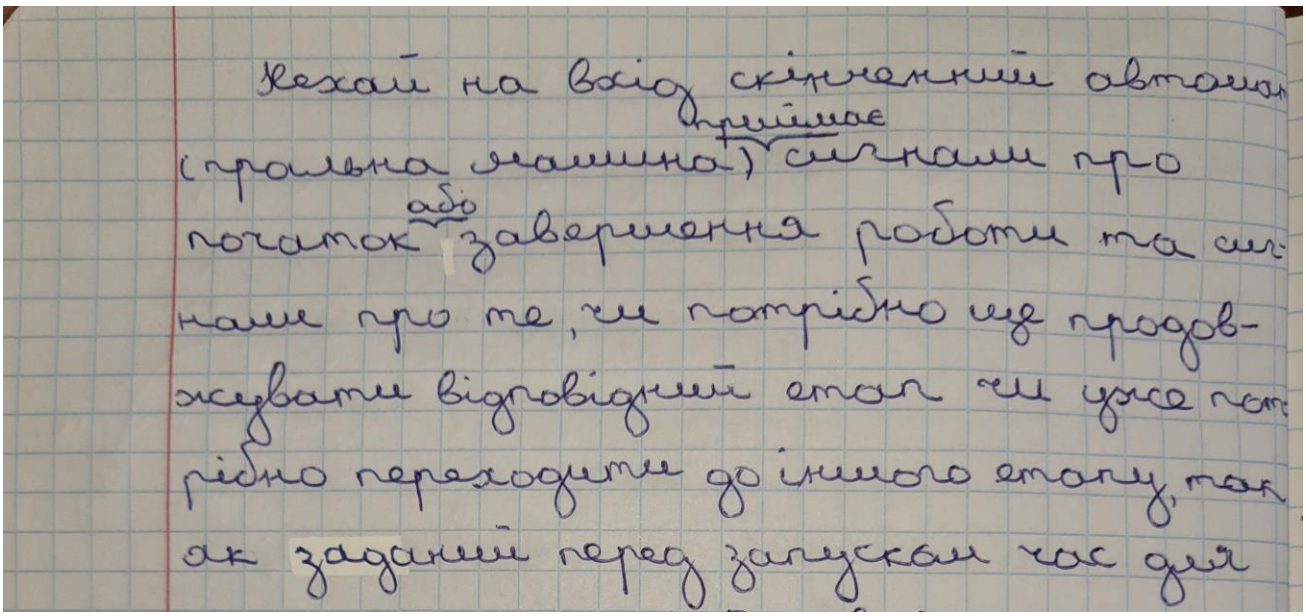
	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
A	×	×	×	×				×
B	×		×			×		
C	×		×		×		×	
D		×		×				×
E	×	×	×		×		×	
F		×						
G	×		×					



* У червоних дужках записанні повноваження, які були успадкувані від батьківських ролей

Завдання 3.

Пральна машина виконує цикл прання, що складається з послідовності чотирьох етапів: замочування, прання, полоскання та віджиму. Термін кожного етапу (A:0..180хв, B:20..90 хв, C:10..30 хв, D:0..10 хв) задається перед запуском процесу прання. Пристрій керування також має кнопки START та STOP. Записати модель детермінованого скінченного автомату, який описує алгоритм роботи пральної машини.


Нехай на вхід скінченний автомат (пральна машина) приймає сигнали про початок або завершення роботи та сигнали про те, чи потрібно ще продовжувати відповідний етап чи уже потрібно переходити до іншого етапу, так як заданий перед запуском час для

даного стану виїмок. У залежності від отриманого на вхід значення автомат буде переключатися в один із станів або ж може залишитися в поточному стані. А на виході автомат може видавати значення: 0 (нуль, якщо стан не змінився) та 1 (один, якщо стан змінився).

$M = (S, X, Y, f, g, S_0)$ – скінченний автомат

- $S = \{T_0, A, B, C, D\}$ – множина станів

T_0 – початковий стан; B – прання

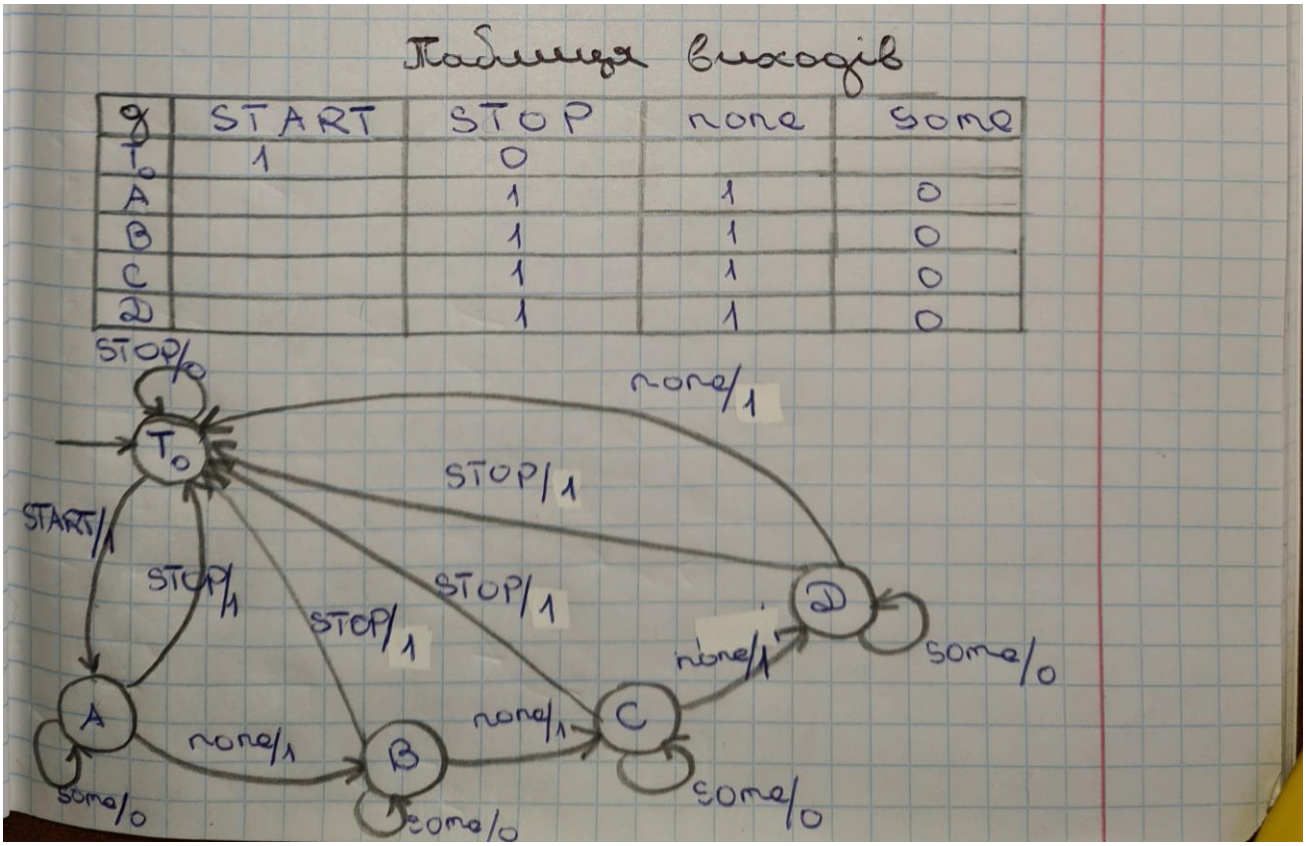
A – замочування; D – відсим

C – полоскання

- $X = \{$START, STOP, none, some$\}$ (час не виїмок) (час уже виїмок) ↖ вхідний алфавіт
- $Y = \{0, 1\}$ – вихідний алфавіт
- $f: S \times X \to S$ – функція переходів
- $g: S \times X \to Y$ – функція виходів

Таблиця переходів

f	START	STOP	none	some
T_0	A	T_0		
A		T_0	B	A
B		T_0	C	B
C		T_0	D	C
D		T_0	T_0	D



Завдання 4-5.

Наведено чотири приклади криптографічних протоколів. Для кожного з них на основі формальних моделей визначте його захищеність та, при наявності, вкажіть вразливості.
(*Відповідні скінченні автомати наводити не потрібно!*)

1. Аліса (A) бажає спілкуватися з Бобом (B) застосовуючи лише надійні криптографічні засоби. Обидві сторони мають поділюваний ключ K, який буде використовуватись для автентифікації. Щоб впевнитись, що Боб є той самий Боб, якого знає Аліса, вона генерує деяке випадковечисло R_A (відповідної довжини) та надсилає Бобу. Якщо Боб є той самий Боб, який знає вірний ключ K, він після цього надсилає Алісі $\{R_B, Hash(A,B,R_A,R_B,K)\}$, де Hash – надійна криптографічна геш-функція. Після чого Аліса надсилає Бобу $\{R_B, Hash(R_A,R_B,K)\}$. В результатісторони можуть впевнитись, що спілкуються з тим самим суб'єктом.

У загальному випадку (якщо не враховувати геш-функцію, яка використовується у даному випадку) описаний вище криптографічний протокол можна вважати безпечним, так як зловмисник не знає ключ K та не в змозі вгадати геш-функцію шифрування і також не може примусити іншу сторону зашифрувати обране повідомлення чи застосувати певну геш-функції.

2. Аліса генерує деяке випадкове число R_A (відповідної довжини) та надсилає Бобу $\{R_A,A\}$. Боб після цього надсилає Алісі $\{R_B, cRYPT_K(R_A)\}$, де cRYPT – надійна функція шифрування з ключем K. Після чого Аліса надсилає Бобу $\{cRYPT_K(R_B)\}$.

На відміну від двохфакторної автентифікації на основі протоколу

запит-відповідь, у якому для встановлення зв'язку виконується п'ять кроків, а у нашому випадку число кроків зменшене до трьох, то існуватиме вразливість дзеркальної атаки, тобто зловмисник зможе відкрити декілька сеансів і повторити виклик надсилання {cRYPT$_K$(R_B)}, у результаті чого отримати коректне значення {cRYPT$_K$}.

3. Аліса, генерує деяке випадкове число R (відповідної довжини) та надсилає Бобу результат обчислення K xor R. Боб здійснює зворотне перетворення з ключем та надсилає Алісі отримане значення R.

Якщо в Єви (прослуховувача) є можливість редагувати інформацію, яку передають Аліса та Боб, то в неї є можливість виконати повноцінну атаку "людина посередині" відповідно до протоколу Діффі – Геллмана:

Таким чином, Єва може видати себе за іншу особу, у даному випадку Боба.

4. Аліса та Боб мають, відповідно, пари відкритий/таємний ключ {E_A,D_A} та {E_B,D_B}. Аліса генерує деяке випадкове число R_A (відповідної довжини) та надсилає Бобу результат шифрування його відкритим ключем E_B(R_A,A), який у відповідь надсилає Алісі результат шифрування її відкритим ключем E_A(R_A,R_B,K_S). K_S – ключ сеансу, який генерує Боб. Завершує автентифікацію Аліса, надсилаючи Бобу результат шифрування отриманим ключем K_S(R_B).

Даний протокол схожий на протокол Діффі – Геллмана і якщо вважати, що так як у нашому випадку Аліса і Боб уже мають пару відкритого закритого ключа, тобто вони уже не повинні обмінюватися ними, то такий криптографічний протокол можна вважати захищеним у відповідності до загальних критеріїв, яким повинен відповідати протоколи автентифікації.