**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ “ЛЬВІВСЬКА ПОЛІТЕХНІКА”**

**Кафедра систем штучного інтелекту**



# **Лабораторна робота 1**

з дисципліни

«Технології захисту інформації»

**Виконав:**

студент групи КН-314

Ляшеник Остап

**Викладач:**

Яковина В. С.

2023 р.

**СТВОРЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ЧИСЕЛ**

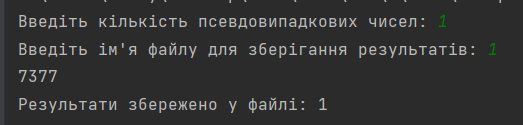
**Мета роботи:** ознайомитись з джерелами та застосуванням випадкових чисел, алгоритмами генерування псевдовипадкових чисел та навчитись створювати програмні генератори псевдовипадкових чисел для використання в системах захисту інформації.

**Завдання:** Згідно до варіанту, наведеного в таблиці, створити програмну реалізацію генератора псевдовипадкових чисел за алгоритмом лінійного порівняння. Програма повинна генерувати послідовність із заданої при вводі кількості псевдовипадкових чисел, результати повинні як виводитись на екран, так і зберігатись у файл. Перевірити період функції генерації, зробити висновок про адекватність вибору параметрів алгоритму. У звіті навести протокол роботи програми, значення періоду функції генерації та зробити висновок про придатність цього генератора для задач криптографії.

**Код програми:**

class LinearCongruentialGenerator:  
 def \_\_init\_\_(self, seed=None):  
 if seed is None:  
 seed = 7 # вказуємо вручну X0  
 self.state = seed  
  
 def generate(self):  
 a = 10\*\*3  
 c = 377  
 m = 2\*\*23 - 1  
 self.state = (a \* self.state + c) % m  
 return self.state  
  
def main():  
 try:  
 n = int(input("Введіть кількість псевдовипадкових чисел: "))  
 filename = input("Введіть ім'я файлу для зберігання результатів: ")  
  
 random\_generator = LinearCongruentialGenerator()  
  
 with open(filename, 'w') as file:  
 for \_ in range(n):  
 random\_number = random\_generator.generate()  
 print(random\_number)  
 file.write(str(random\_number) + '\n')  
  
 print(f"Результати збережено у файлі: {filename}")  
  
 except ValueError:  
 print("Будь ласка, введіть правильне ціле число для кількості псевдовипадкових чисел.")  
  
if \_\_name\_\_ == "\_\_main\_\_":  
 main()

Результати виконання:



**Висновок:** виконуючи цю лабораторну роботу я дізнався як генерувати псевдовипадкові числа