

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КІЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ  
імені Ігоря СІКОРСЬКОГО»  
Навчально-науковий фізико-технічний інститут  
Кафедра математичних методів захисту інформації**

## **ДКР. Варіант №3**

**Роботу виконав:  
Юрчук Олексій, ФІ-52МН**

26 листопада 2025 р.  
м. Київ

# **Завдання № 1**

## **1.1 Вступні відомості**

**Постановка задачі:**

1. Створіть репозиторій у системі контролю версій Git/GitHub;
2. Реалізувати атаку з малою експонентою на основі китайської теореми про лишки.
3. Реалізувати атаку ”зустріч посередині” та порівняти її швидкодію з повним перебором можливих відкритих текстів.
4. Оформити звіт до комп’ютерного практикуму.