

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

Домашня робота №1

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

27 лютого 2026 р.
м. Київ

ЗМІСТ

1		1
2		2
2.1 Умова	2	
2.2 Розв'язання	2	
3		4

Завдання № 1

Завдання № 2

2.1 Умова

Нехай Γ – генератор гами з множиною станів V_n та вихідним алфавітом V_2 , який виробляє за початковим станом s_0 вихідну послідовність $\Gamma_L(s_0)$ довжини L . Покажіть, що існує статистичний критерій, який дозволяє відрізняти цю послідовність, отриману за випадковим рівномірним початковим станом, від сухо випадкової двійкової послідовності довжини L із середньою ймовірністю помилки p_e , використовуючи T двійкових операцій, якщо $\Gamma_{2N} : s_0 \rightarrow (s_0, s_0)$, $p_e = 2^{-N-1}$, $T = N$.

2.2 Розв'язання

З умови можна зробити висновок, що послідовність $\Gamma_{2N} : s_0 \rightarrow (s_0, s_0)$ довжини $2N$ має вигляд:

$$\Gamma_{2N}(s_0) = (\gamma_1, \gamma_2, \dots, \gamma_N, \gamma_1, \gamma_2, \dots, \gamma_N)$$

Тобто **перші N біт повторюються в наступних N бітах.**

Побудова статистичного критерію

Критерій: Для послідовності $x = (x_1, x_2, \dots, x_{2N})$ перевіряємо рівність:

$$D(X) = \sum_{i=1}^N x_i \oplus x_{N+i} = \begin{cases} 0, \Leftrightarrow x_i = x_{N+i}, & \forall i, i = \overline{1, N} \Rightarrow x \in \Gamma_L \\ \neq 0, -\text{random sequence} \end{cases}$$

Висунемо такі гіпотези:

- H_0 : послідовність від генератора Γ
- H_1 : сухо випадкова, рівномірна послідовність

Помилка I роду (хибне відхилення H_0):

$$\alpha = P(H_1 | H_0) = 0$$

Нуль, бо генератор **завжди** видає $(x_1, \dots, x_N) = (x_{N+1}, \dots, x_{2N})$ за умовою.

Помилка II роду (хибне прийняття H_0):

$$\beta = P(H_0 | H_1) = P(x_i = x_{N+i}, \forall i | \text{випадкова})$$

Для випадкової послідовності біти є незалежними одне від одного, тому:

$$\beta = \prod_{i=1}^N P(x_i = x_{N+i}) = \prod_{i=1}^N \frac{1}{2} = 2^{-N}$$

Середня ймовірність помилки обчислюється за Байєсом:

$$p_e = \frac{1}{2} (\alpha + \beta) = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 2^{-N} = 2^{-N-1}$$

Обчислювальна складність цього критерію:

N XOR-ів: $x_i \oplus x_{N+i}$ для $i = 1, \dots, N$, тобто загальна кількість двійкових операцій $T = N$

У висновку можна сказати, що критерій експлуатує детерміновану структурну слабкість генератора – періодичність з періодом N , яка неможлива для справді випадкової послідовності з ймовірністю $1 - 2^{-N}$.

Завдання № 3