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

Звіт до
комп'ютерного практикуму №1

Оформлення звіту:
Дигас Богдан, ФІ-52мн
Юрчук Олексій, ФІ-52мн

15 вересня 2025 р.
м. Київ

Мета роботи: Ознайомлення з принципами баєсівського підходу в криптоаналізі, побудова детерміністичної та стохастичної вирішуючих функцій для моделей схем шифрування та криптоаналіз моделей шифрів за допомогою програмної реалізації, зокрема здійснення порвіняльного аналізу вирішуючих функцій.

Постановка задачі:

1. Створіть репозиторій у системі контролю версій Git/GitHub;
2. Реалізуйте алгоритми програмно та представите результати побудови детермінованих та стохастичних вирішальних функцій у вигляді таблиць. Для цього необхідно:
   (а) обчислити розподіли $P(C)$ та $P(M, C)$;
   (б) на основі цих розподілів обчислити $P(M|C)$;
   (в) побудова оптимальних детермінованих та стохастичних вирішальних функцій зводиться до максимізації $P(M|C)$.
3. Розрахуйте середні втрати, проведіть порівняльний аналіз функцій прийняття рішень.
4. Підготувати звіт для комп'ютерного практикуму.

ВАРІАНТ 15: