МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

**Дисципліна “Системи та засоби криптоаналізу”**

**Звіт до лабораторної роботи № 3**

на тему “ Дослідження криптоаналітичних атак на афінний шифр. Частина 1**”**

Студент ПІБ

Варіант №

Група

Перевірила Лаврик Т.В

**Суми 20\_\_\_**

**ЗВІТ**

1. (5 б.) Програмний код, який шифрує введену з клавіатури українською мовою інформацію за допомогою афінної системи підстановок Цезаря. Ключ шифрування (a, b) і зашифрований текст зберегти для звіту.

Текст програми

Скріншоти з результатами роботи програми (мінімум 3 різні тексти)

1. (3 б.) Блок-схема алгоритму реалізації методу повного перебору.

Блок-схема

1. (5 б.) Програмний код методу повного перебору.

Текст програми

Скріншоти з результатами роботи програми (мінімум 3 різні шифротексти)