

**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

|  |
| --- |
| **РТУ МИРЭА** |
|  |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** |
|  |
| КБ-2 «Информационно-аналитические системы кибербезопасности» |

**ОТЧЕТ О ВЫПОЛНЕНИ ЛАБОРАТОРНОЙ РАБОТЫ №1**

**В РАМКАХ ДИСЦИПЛИНЫ «МЕТОДЫ И СРЕДСТВА КРИПТОРГАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»**

Выполнил:

Студент 3-ого курса

Учебной группы БИСО-02-22

Зубарев В.С.

8 ЗАДАНИЙ 8 РАЗНЫХ ИСХОДНЫХ ТЕКСТОВ

Определяем ключ, который заложен в программе

Текст не больше 10 слов

Сначала сохраняем файл как тхт и потом выходим потом снова вызываем файл и шифруем

Каждое задание 3 эксперимента

Перебор от 3 до 10

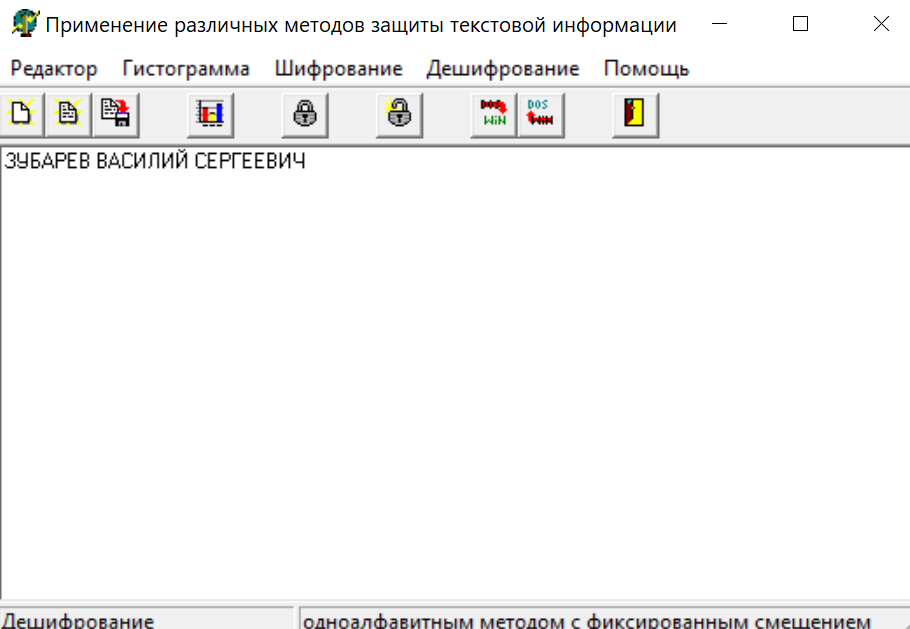
Задание 9 для изученных методов создать абсолютно стойкий шифр

Вывод – кол-во вариантов ключей для каждого из методов

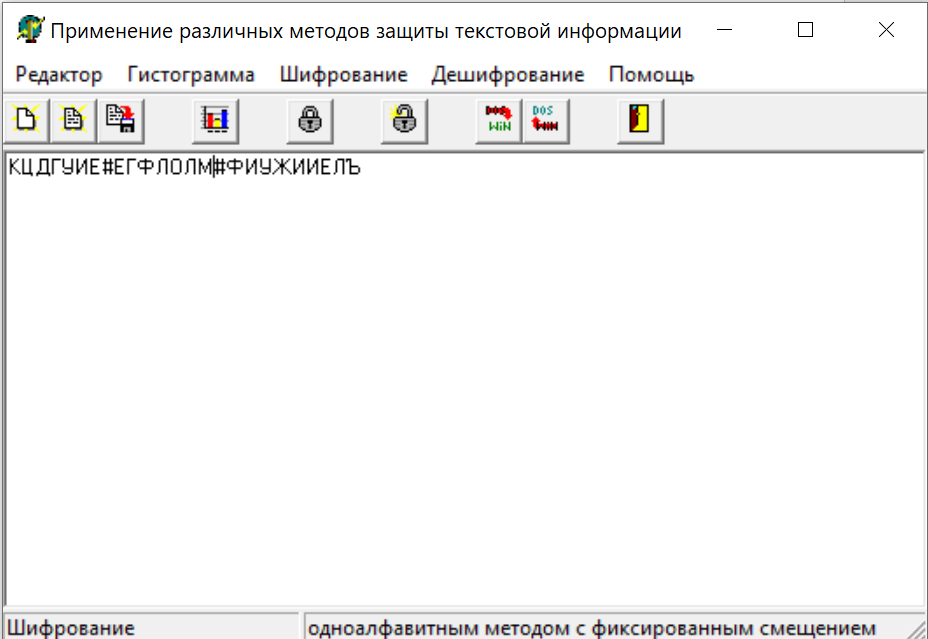
1. Ознакомиться с описанием лабораторной работы и заданием.

2. Для одно алфавитного метода с фиксированным смещением определить установленное в программе смещение.

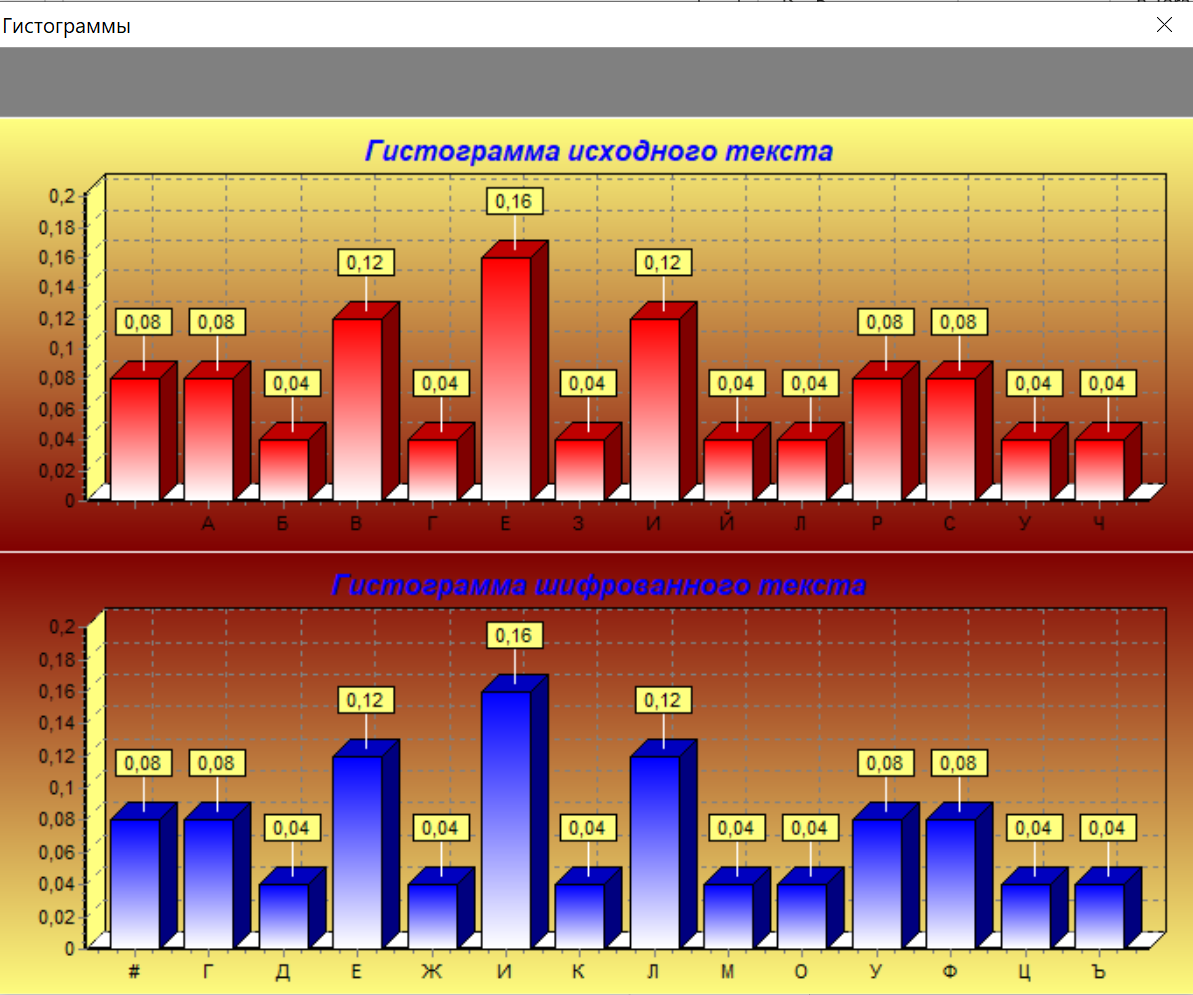
Эксперимент 1



1- исходный текст



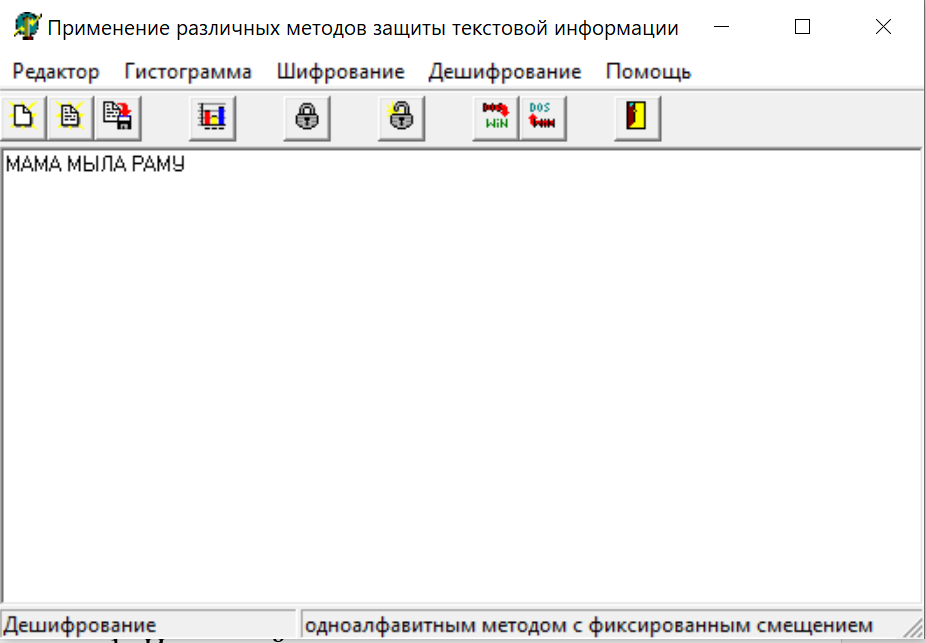
2- исходный текст



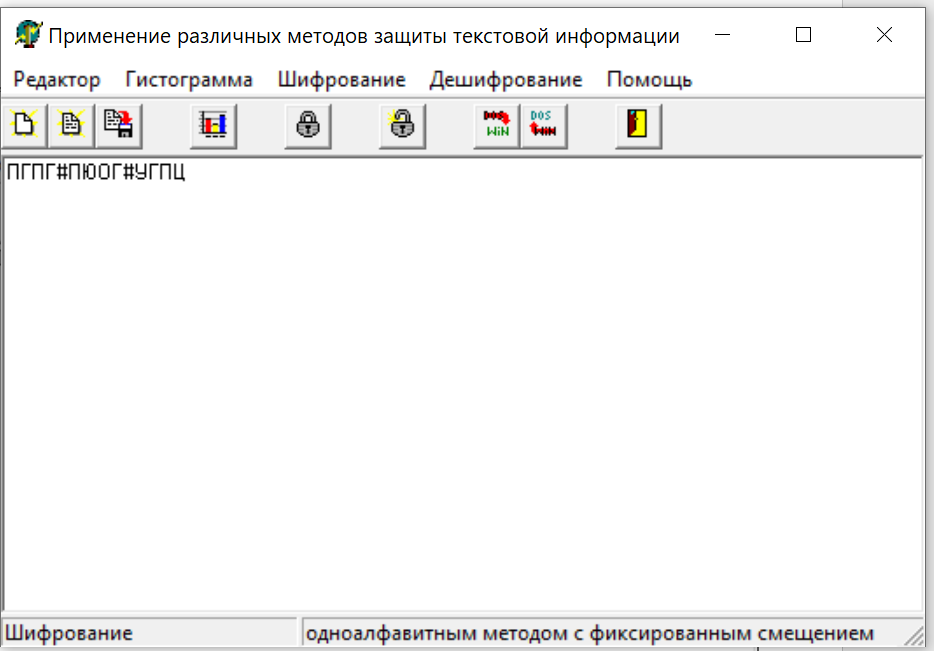
* Описать и объяснить процесс дешифрования.

Так как зашифрованный текст повторяет структуру открытого текста, соответственно распределение зашифрованных символов такое же, как и открытом тексте. На моем примере буква «Е» смещается преобразовалась в «И». По формуле 200 = (197 + к), тогда к = 3

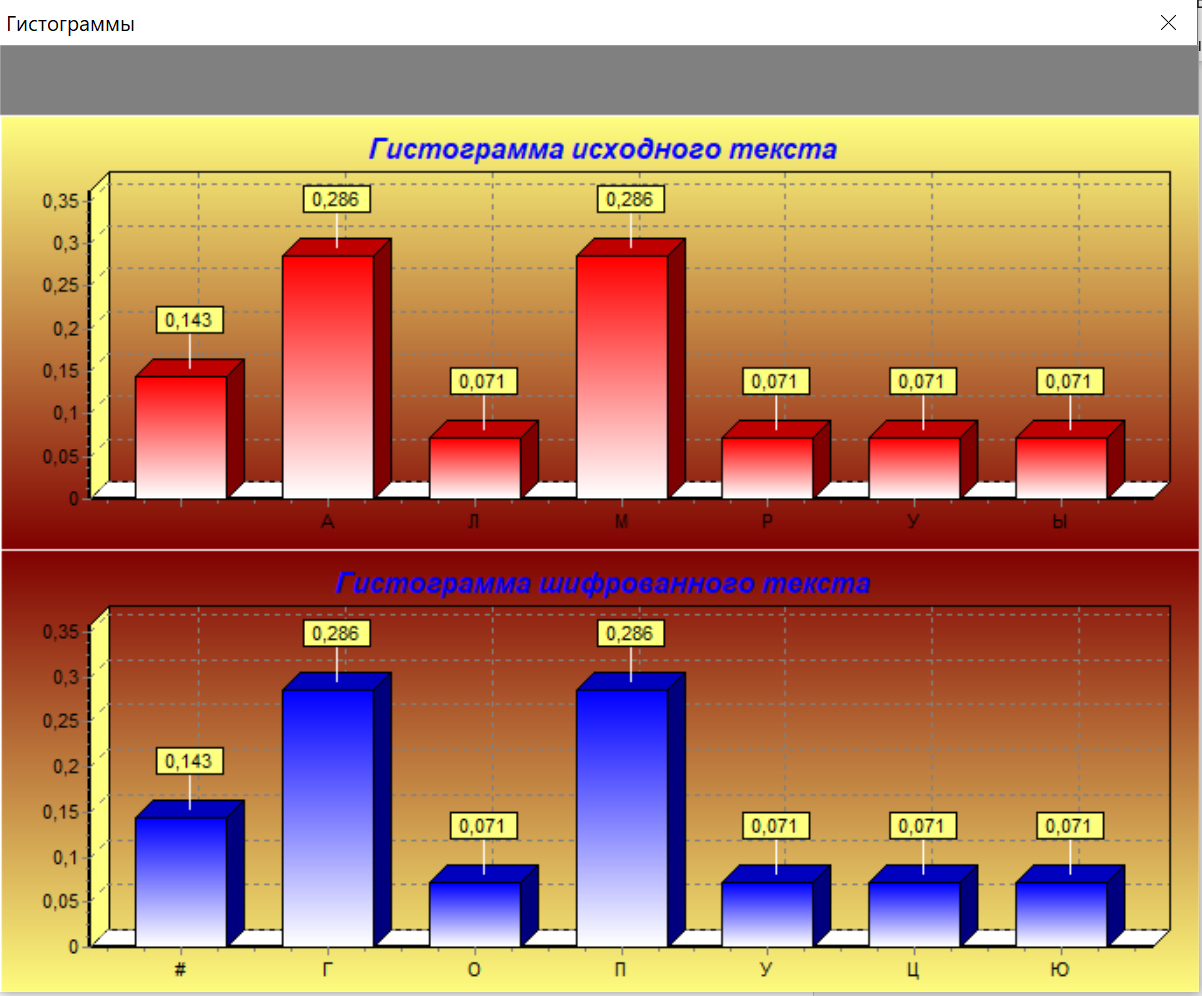
Эксперимент 2



1- Исходный текст

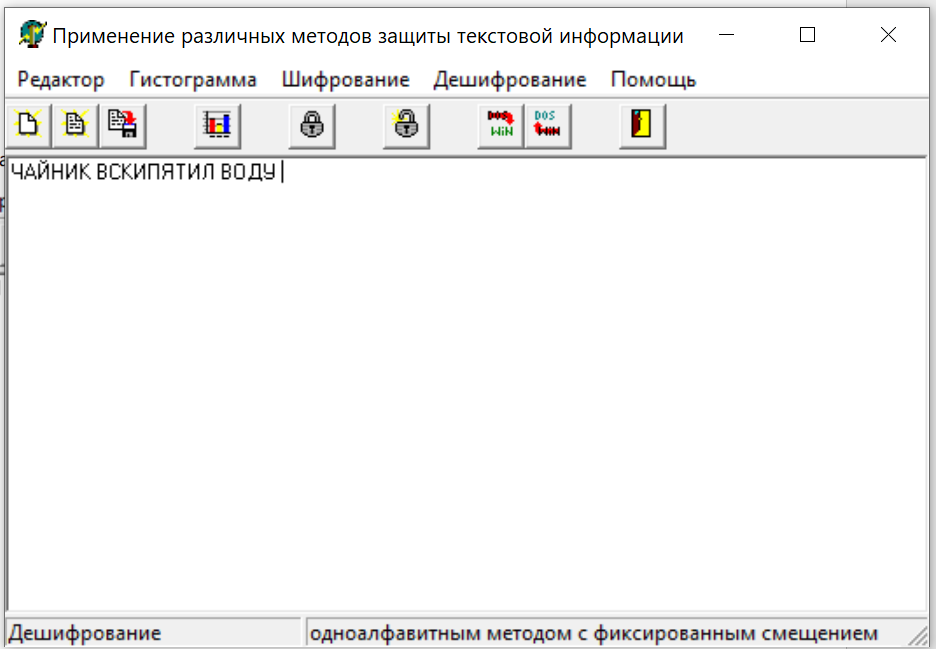


2 – Зашифрованный текст

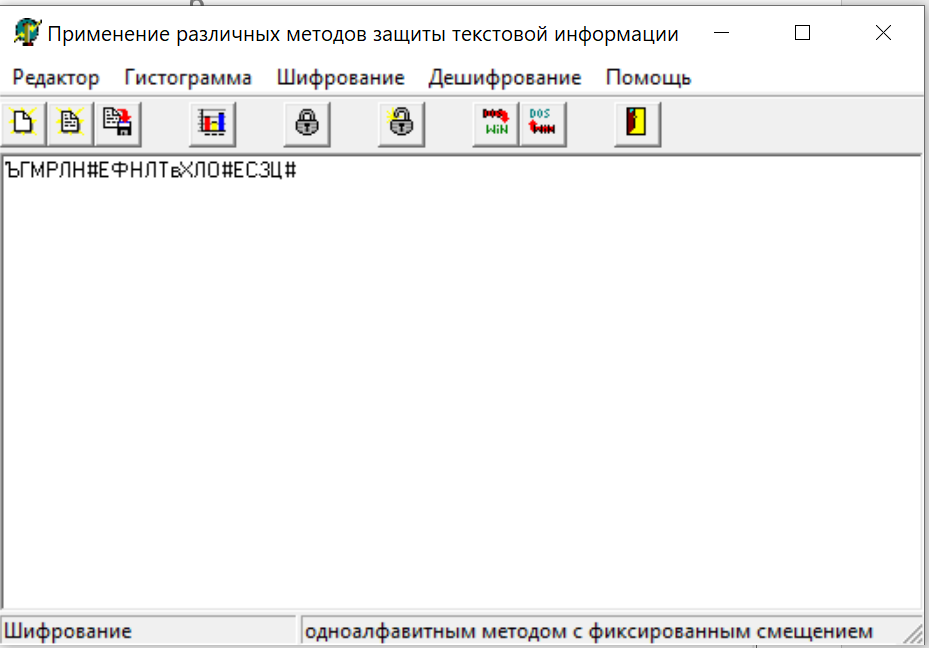


3 - Гистограммы

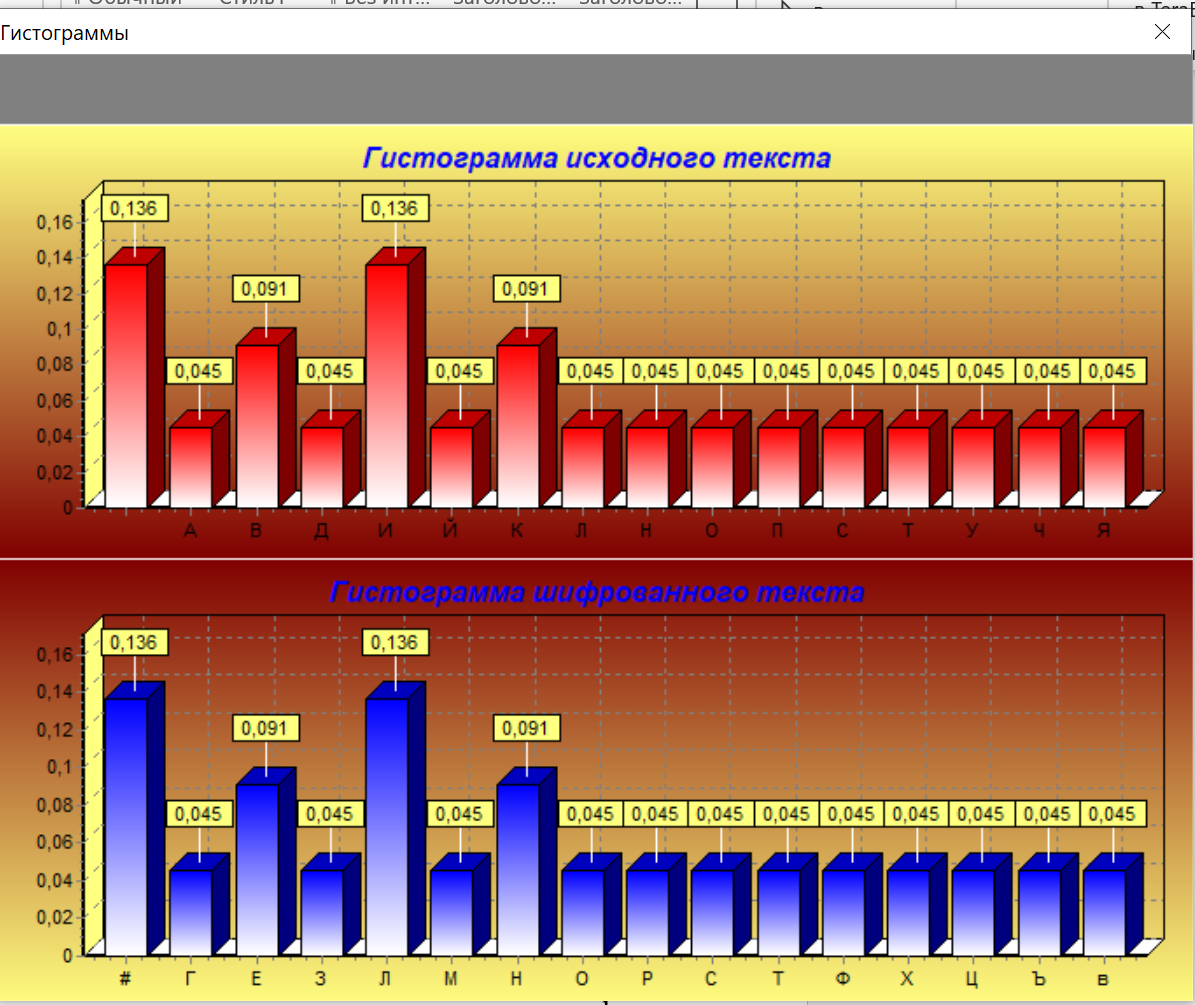
Эксперимент 3



1- Исходный текст



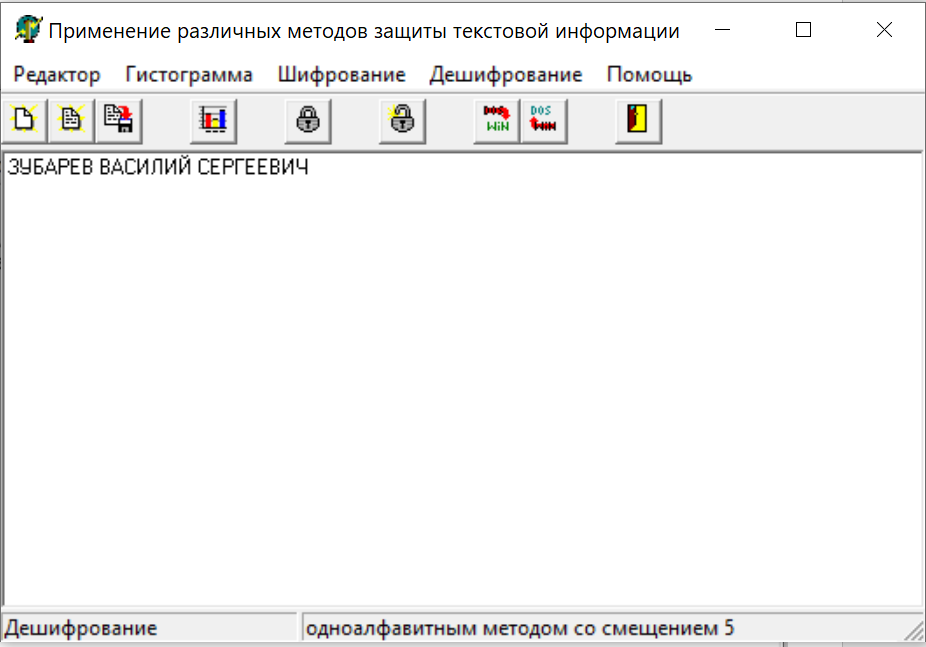
2 – зашифрованный текст



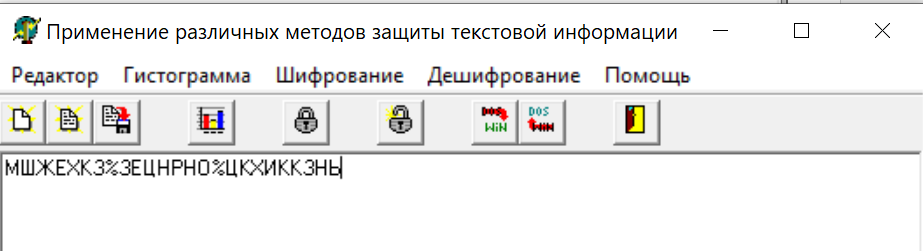
3 - Гистограммы

3. Для одно алфавитного метода с задаваемым смещением (шифр Цезаря)

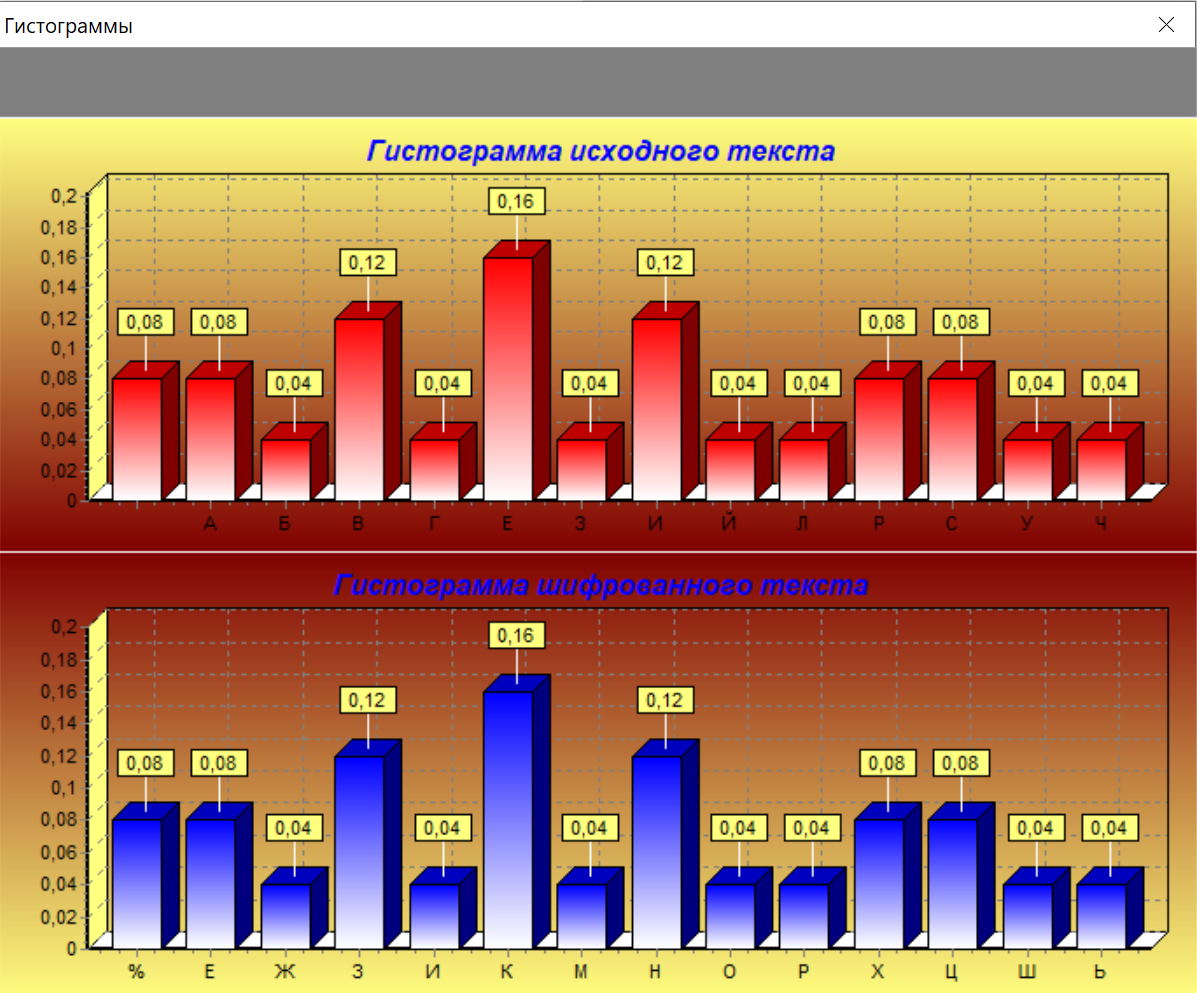
Эксперимент 1



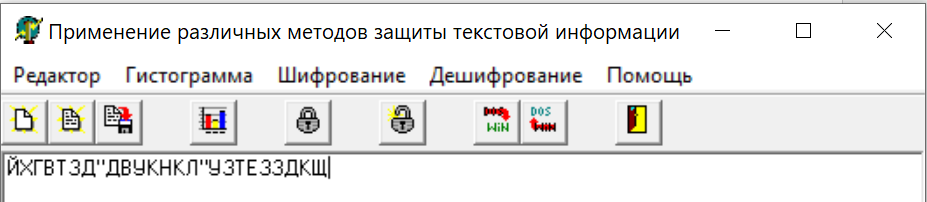
1- Исходный текст



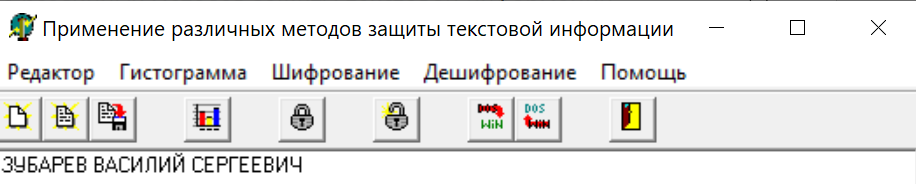
2 – Зашифрованный текст (смещение 5)



3 – Гистограммы

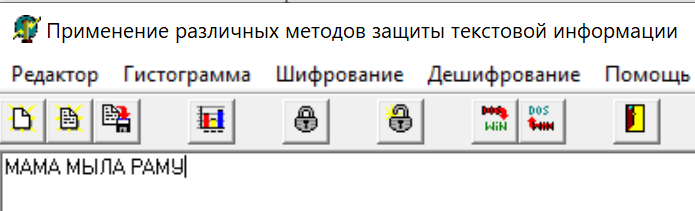


4 – Дешифрование подбором смещения (расшифровка со смещением 3)

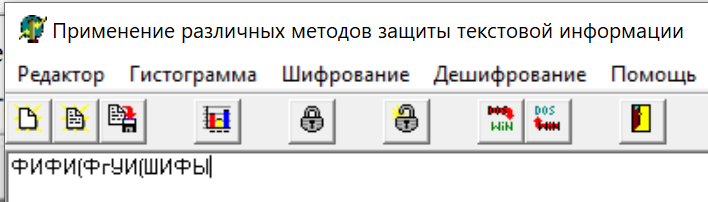


5 – Дешифрование подбором смещения (расшифровка со смещением 5)

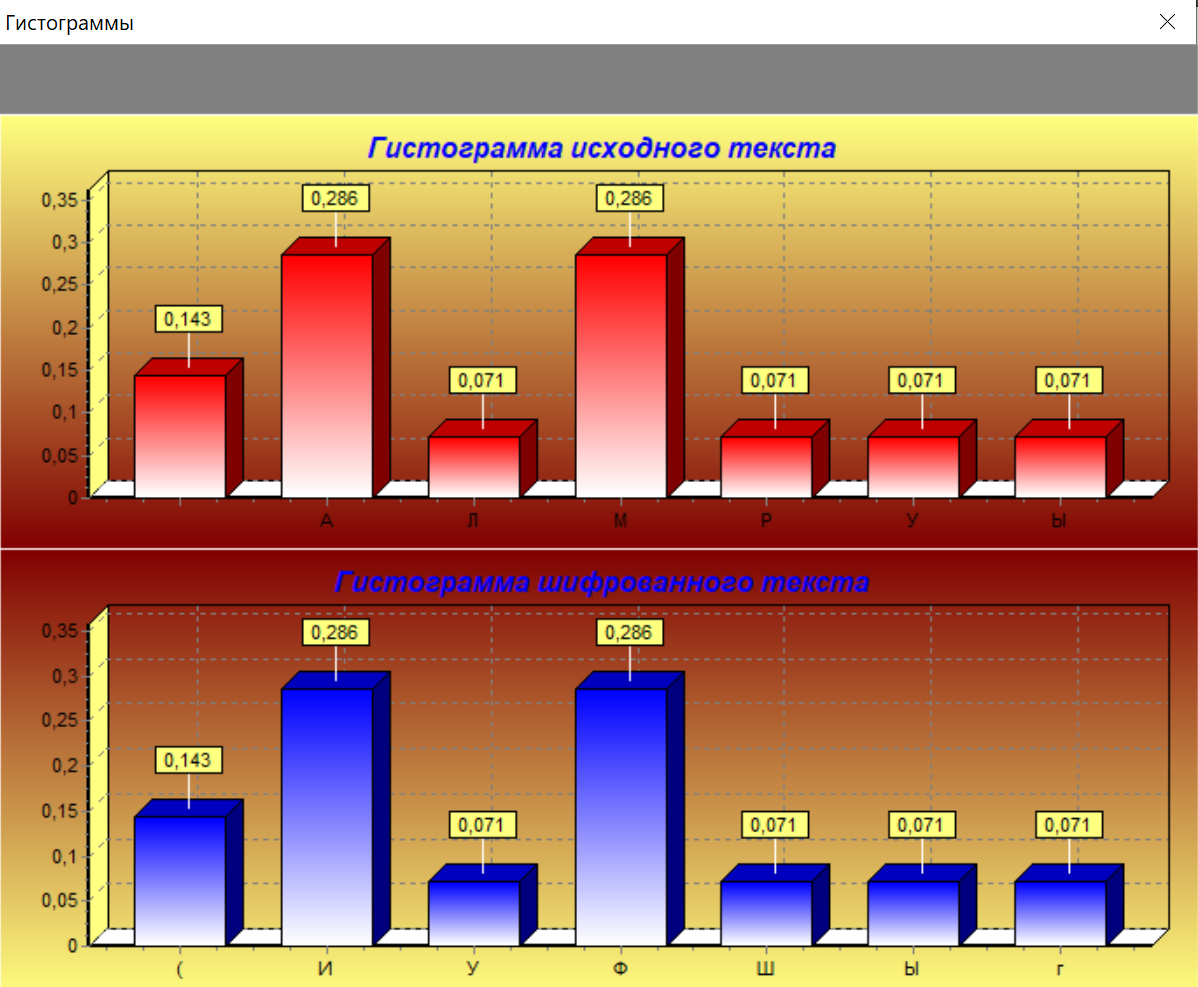
Эксперимент 2



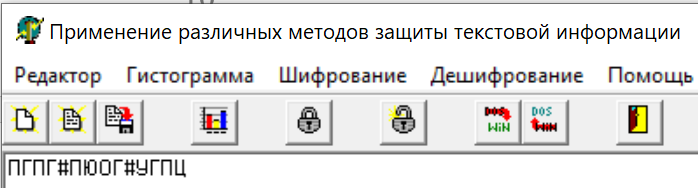
1- Исходный текст



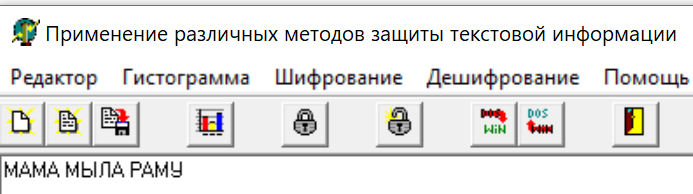
2 – Зашифрованный текст (смещение 8)



3 – Гистограммы

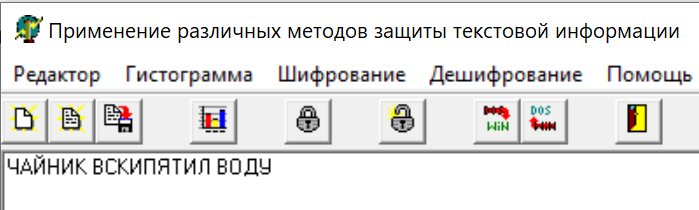


4 – Дешифрование подбором смещения (расшифровка со смещением 5)

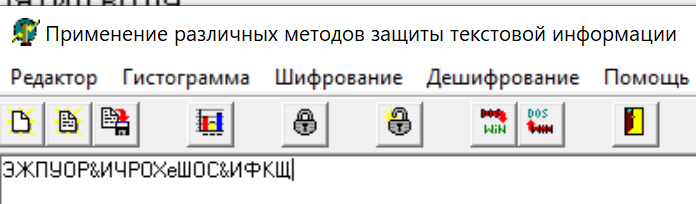


5 – Дешифрование подбором смещения (расшифровка со смещением 8)

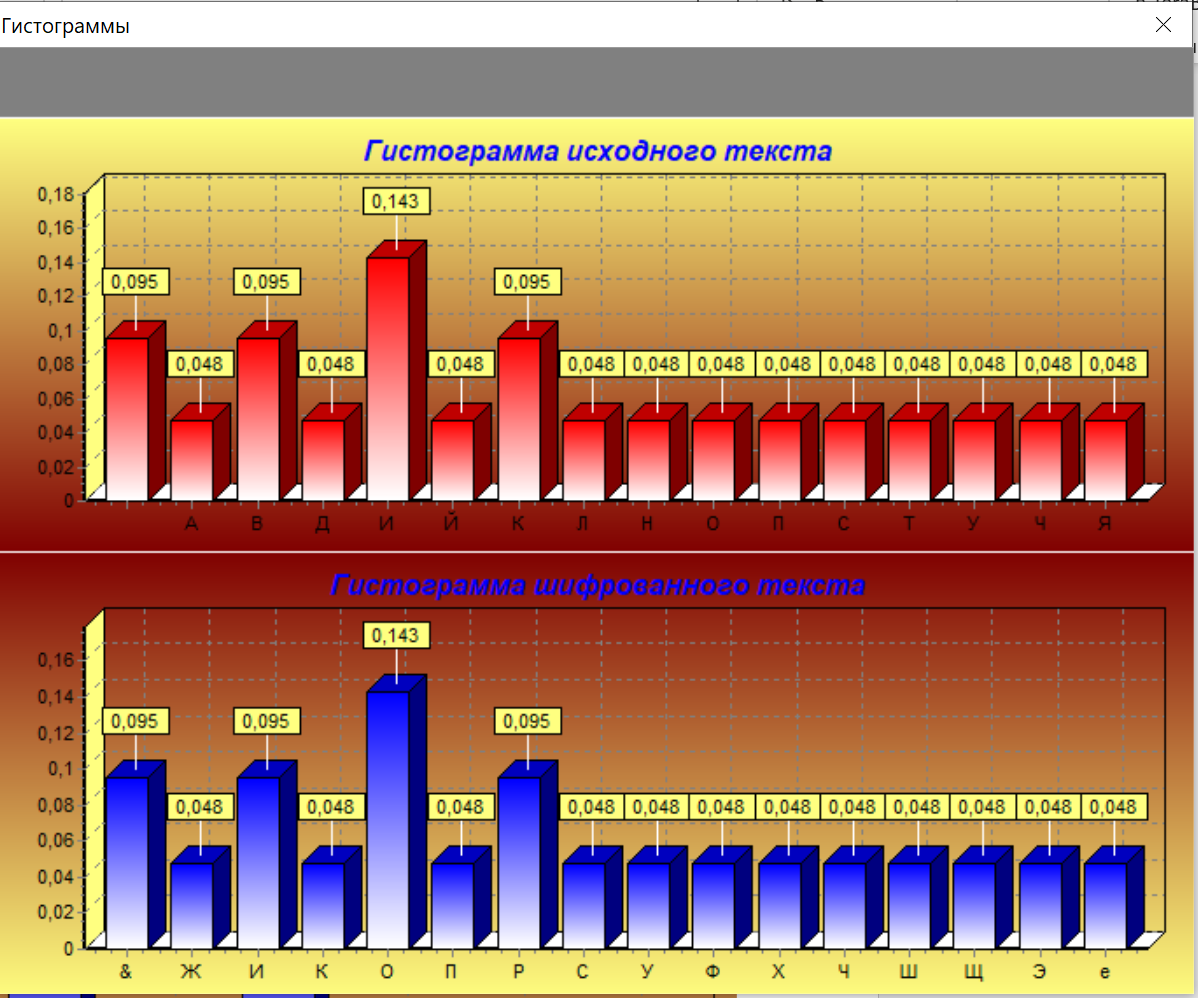
Эксперимент 3



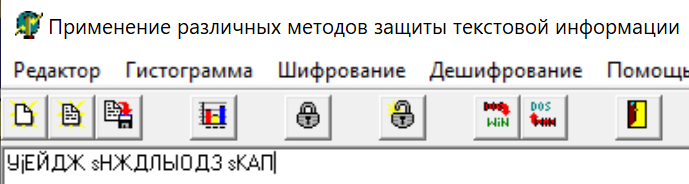
1- Исходный текст



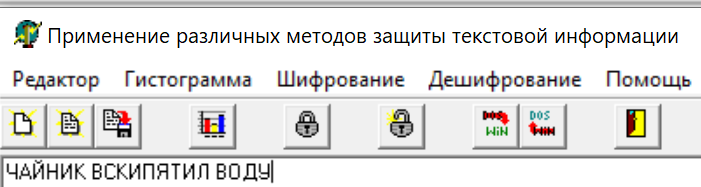
2 – Зашифрованный текст (смещение 6)



3 – Гистограммы



4 – Дешифрование подбором смещения (расшифровка со смещением 10)



5 – Дешифрование подбором смещения (расшифровка со смещением 6)

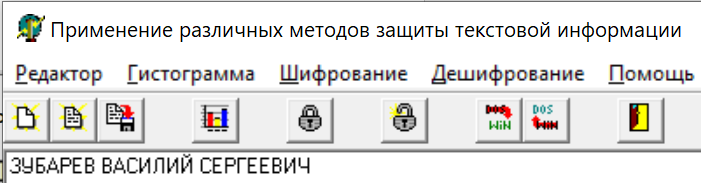
4. Для метода перестановки символов дешифровать зашифрованный файл.

ЗУБАРЕВ ВАСИЛИЙ СЕРГЕЕВИЧ

БУЗЕРАВ ВИСАЙИЛЕС ЕГРИВЕ Ч

БУЗЕРАВ ВИСАЙИЛЕС ЕГРИВЕ Ч

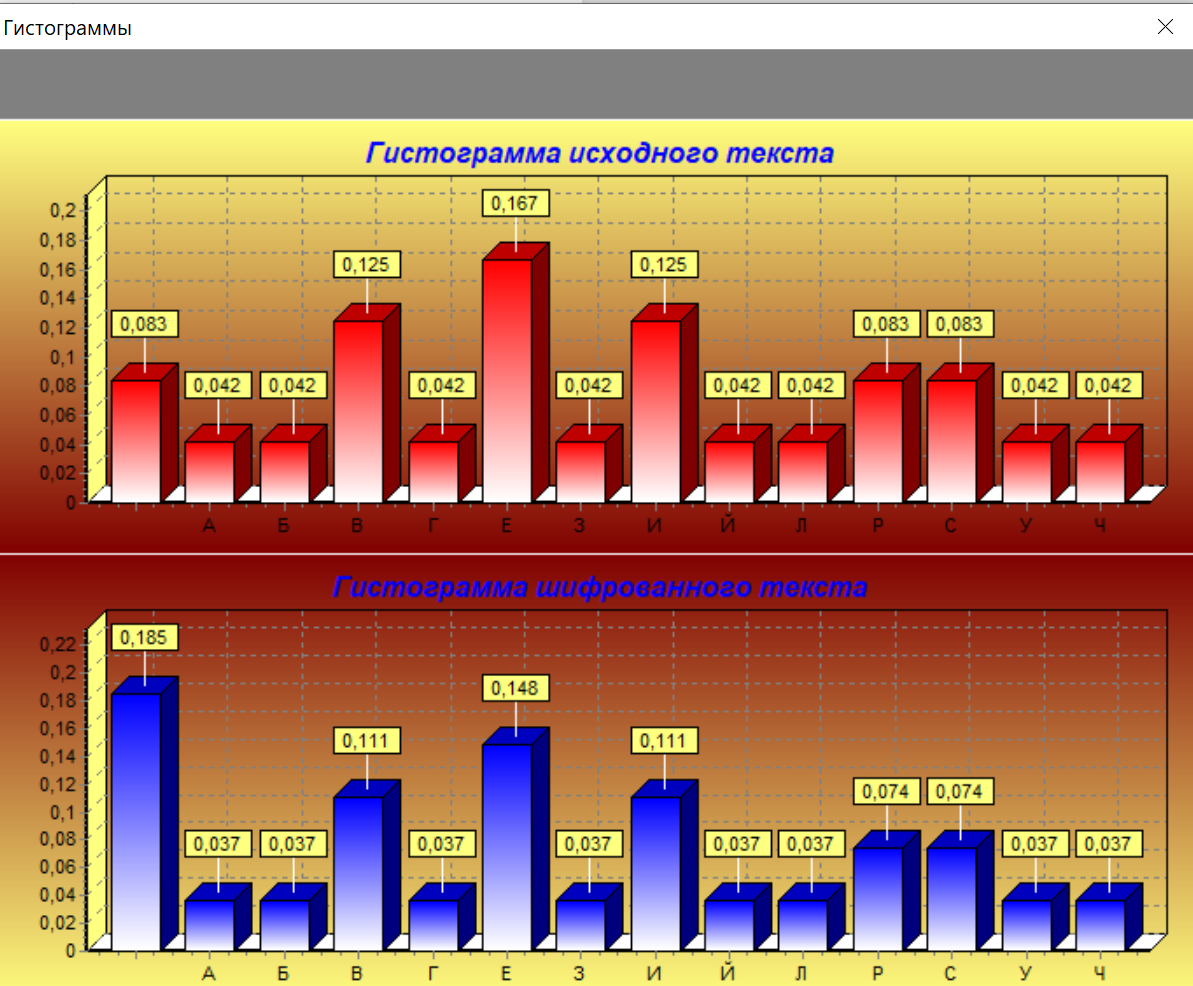
Эксперимент 1



1- Исходный текст



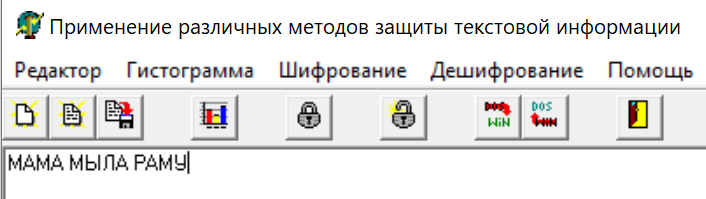
2 – Зашифрованный текст (ключ 321)



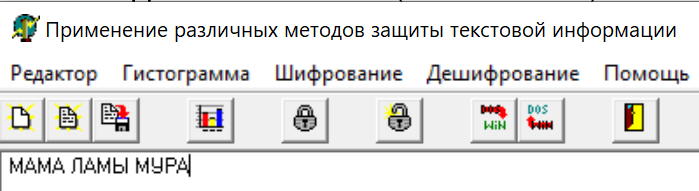
3 – Гистограммы (полезную информацию извлечь нельзя)

Алгоритм перестановки следующий: Выбирается длина ключа (в данном случае 3) весь текст с конца делится на триады и каждому символу в триаде присваивается свой номер (от 1 до 3), далее выбирается порядок перестановки (в данном случае 321),то есть последовательность символов в триаде 123 превращается в 321. Пример ВИЧ (В-1, И-2, Ч-3) превращается в ЧИВ (321)

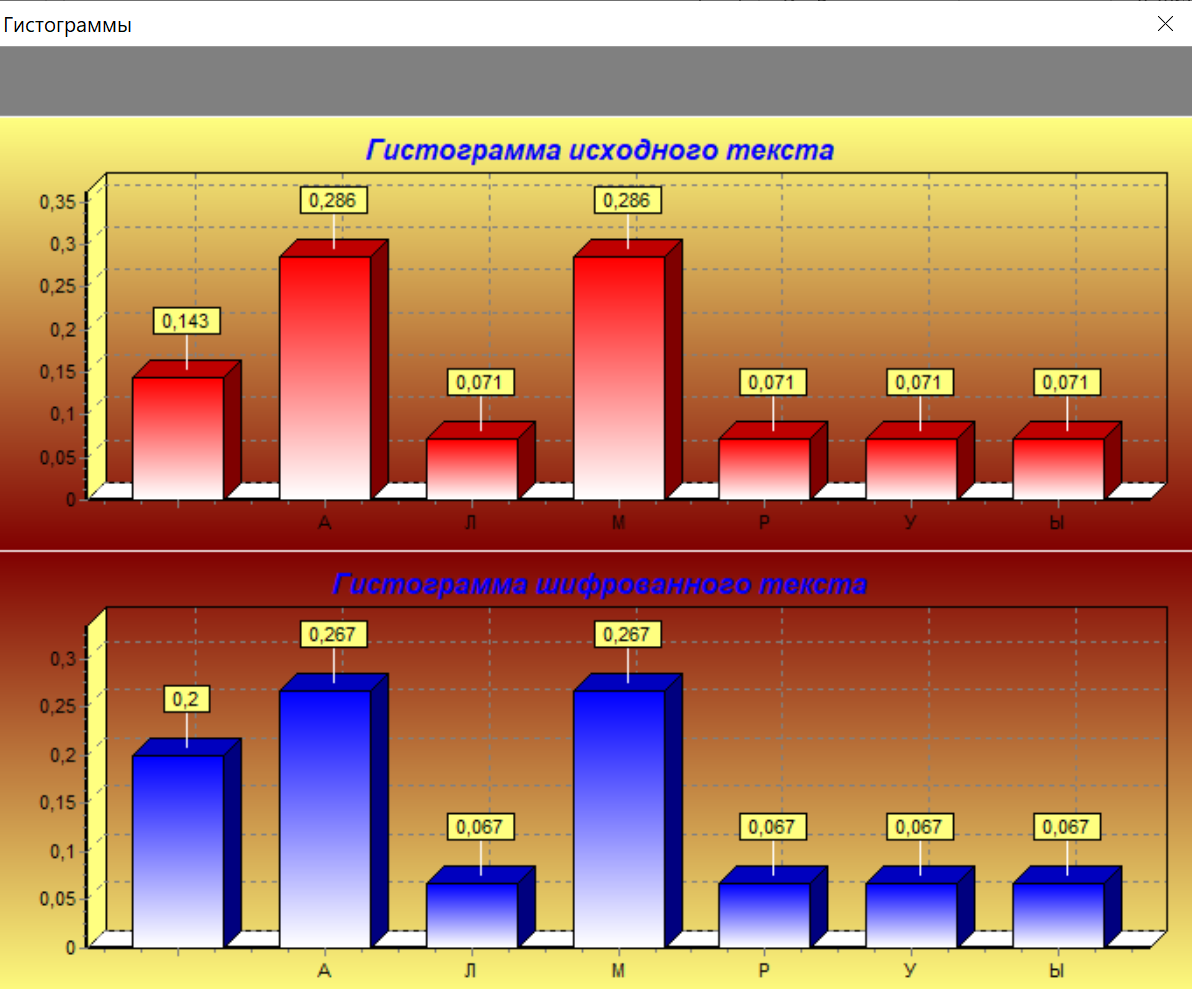
Эксперимент 2



1- Исходный текст

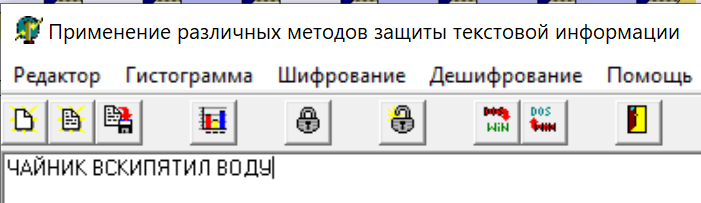


2 – Зашифрованный текст (ключ 53412)

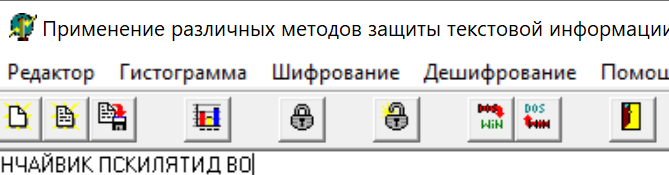


3 – Гистограммы (полезную информацию извлечь нельзя)

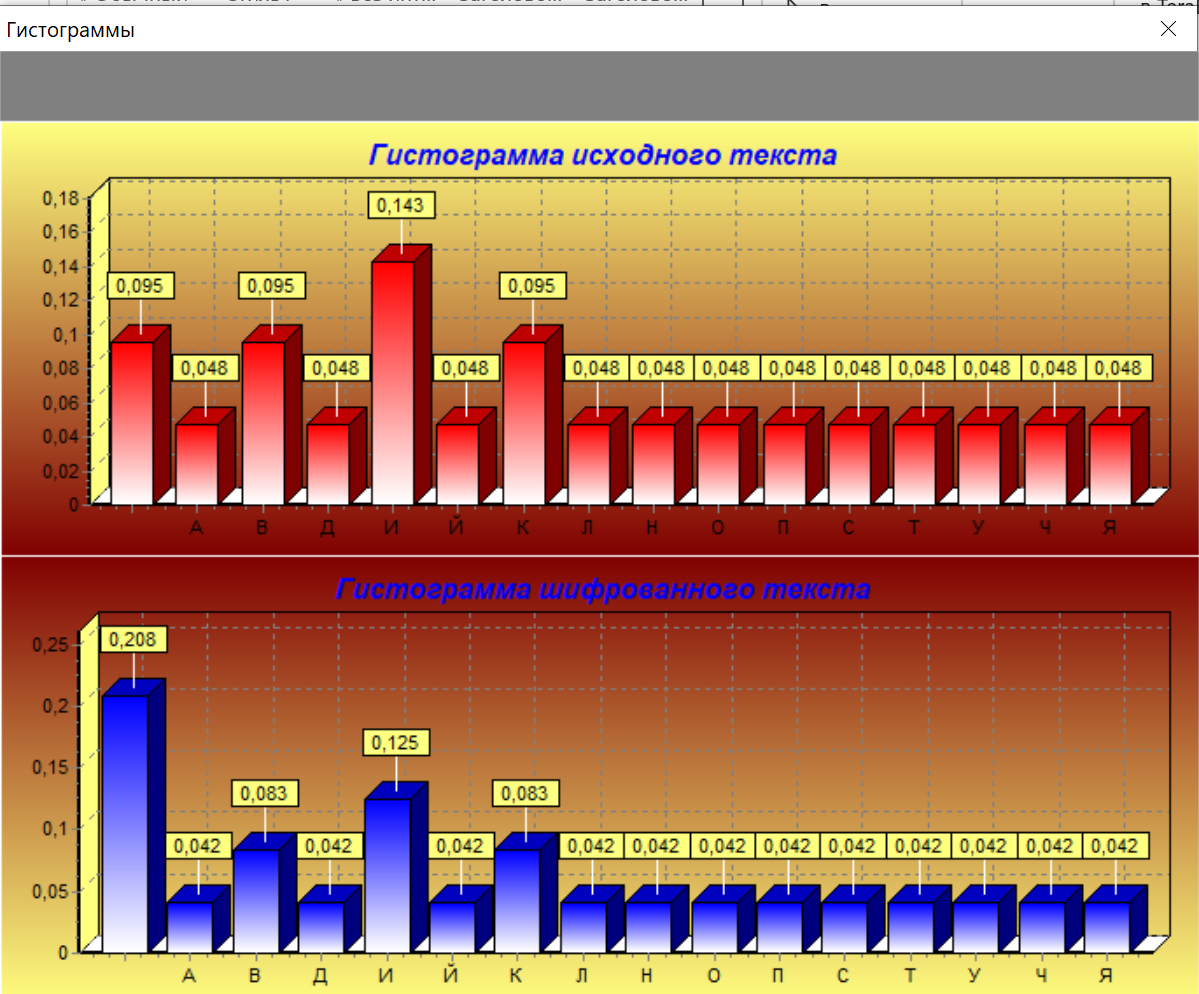
Эксперимент 3



1- Исходный текст



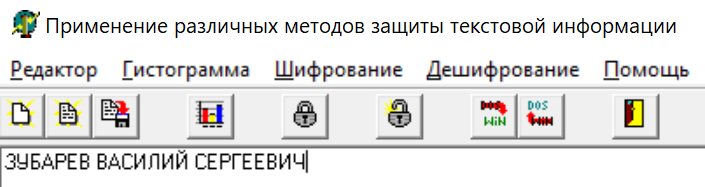
2 – Зашифрованный текст (ключ 2341)



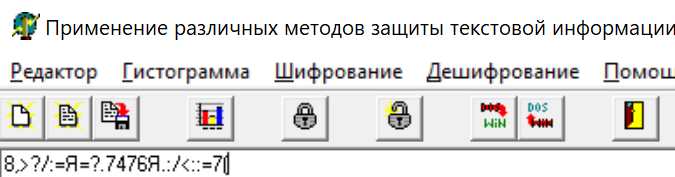
3 – Гистограммы (полезную информацию извлечь нельзя)

5. Для инверсного кодирования (по дополнению до 255)

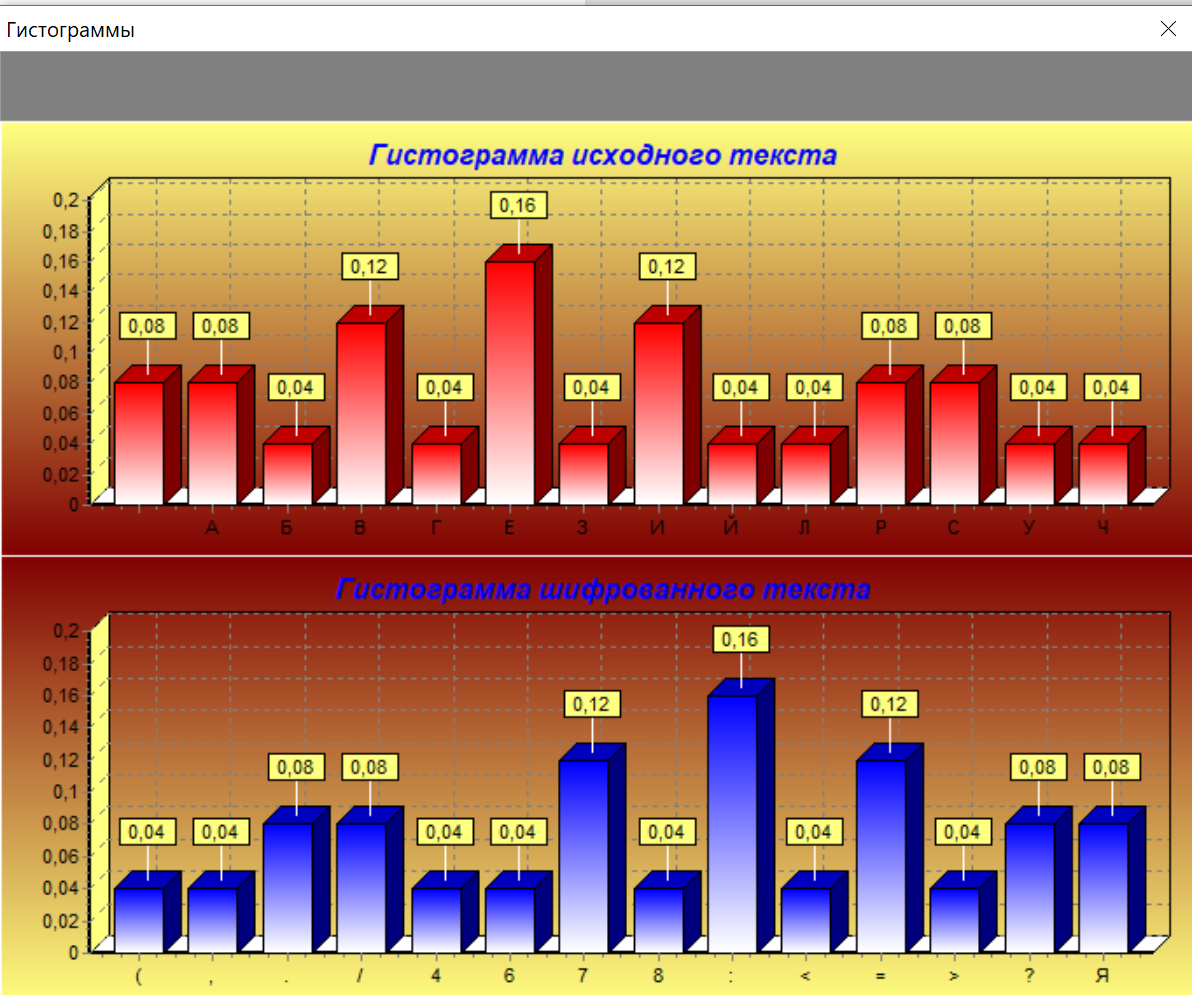
Эксперимент 1



1- Исходный текст



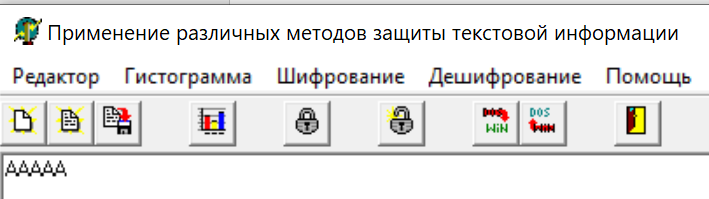
2 – Зашифрованный текст (ключ 2341)



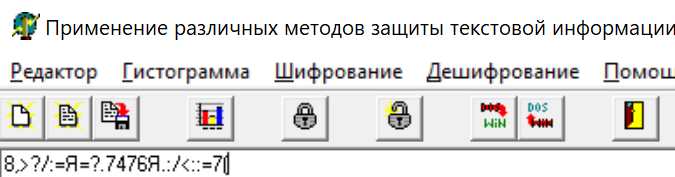
3 – Гистограммы Тш=N-T0 (на примере 58=255-197)

В данном случае N=255, так как нумерация начинается с 0, а количество символов алфавита нумеруется с 1

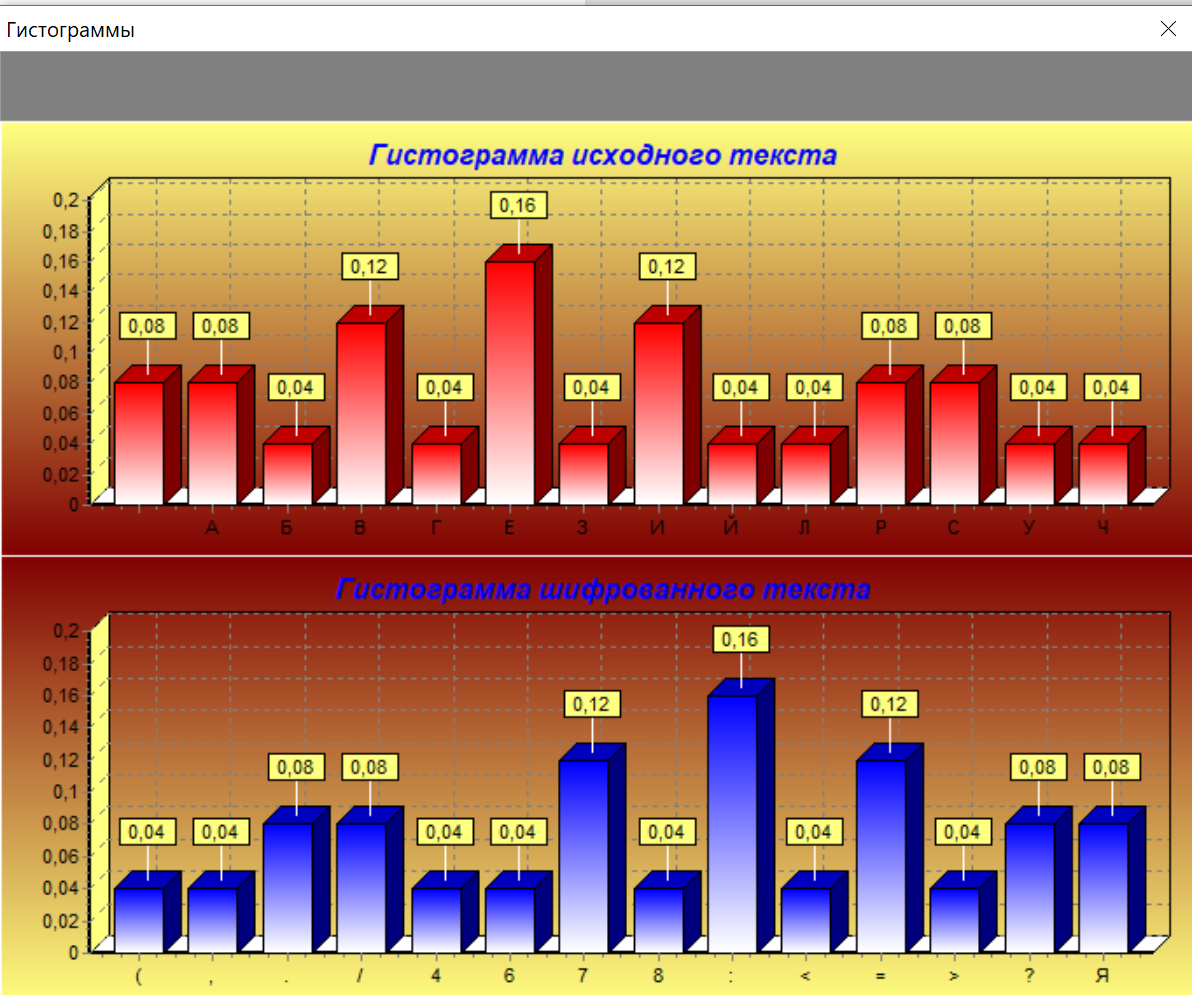
Эксперимент 1



1- Исходный текст



2 – Зашифрованный текст (ключ 2341)



3 – Гистограммы Тш=N-T0 (на примере 58=255-197)

6. Для многоалфавитного шифрования с фиксированным ключом определите, сколько одно алфавитных методов и с каким смещением используется в программе.

7. Для многоалфавитного шифрования с ключом фиксированной длины: выполните шифрование и определите по гистограмме, какое смещение получает каждый символ для файла, состоящего из строки одинаковых символов; выполните шифрование и расшифрование для файла произвольного текста; просмотрите и опишите гистограммы исходного и зашифрованного текстов; ответьте, какую информацию можно получить из гистограмм.

8. Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично п. 7