

**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

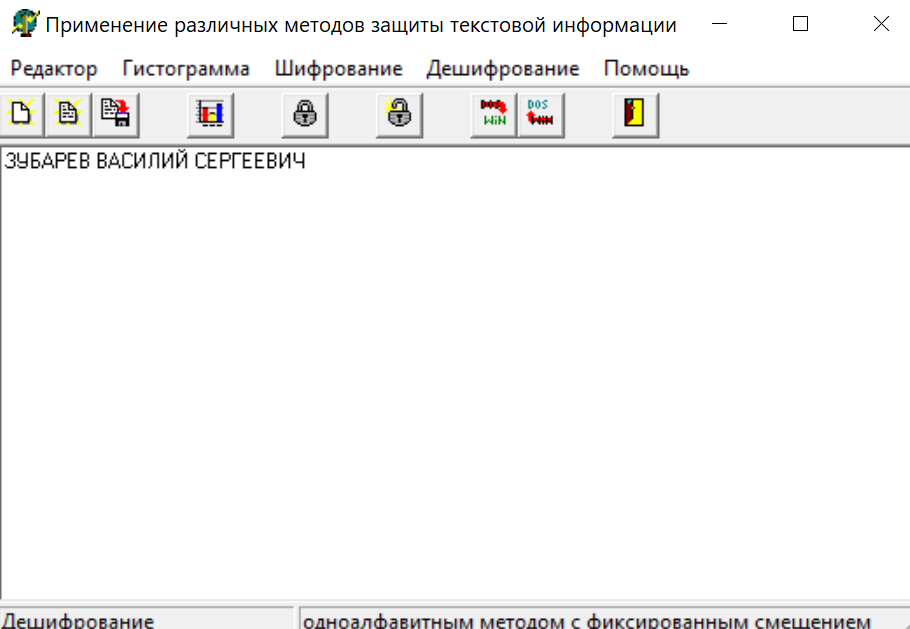
Учебной группы БИСО-02-22

Зубарев В.С.

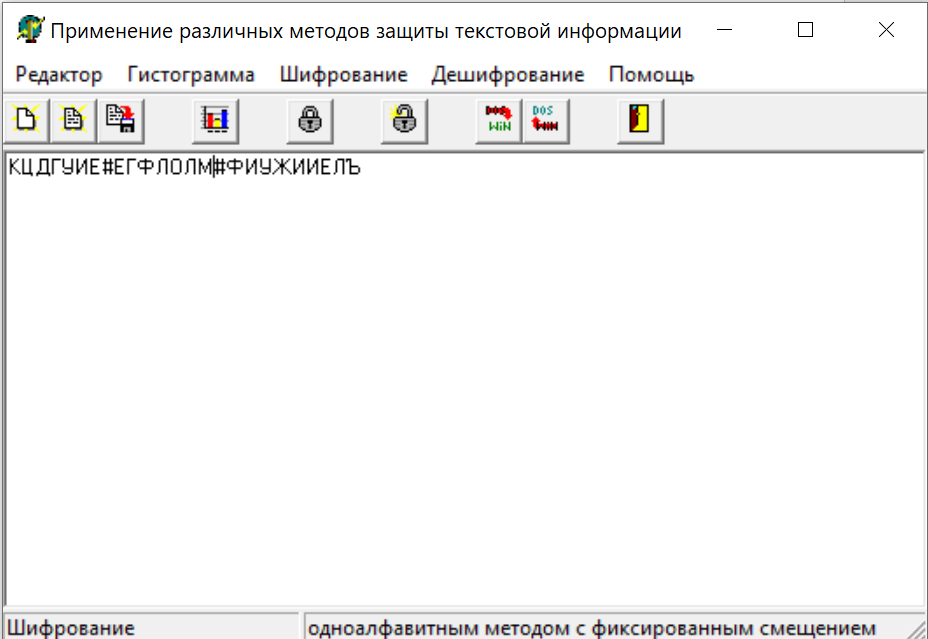
1. Ознакомиться с описанием лабораторной работы и заданием.

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

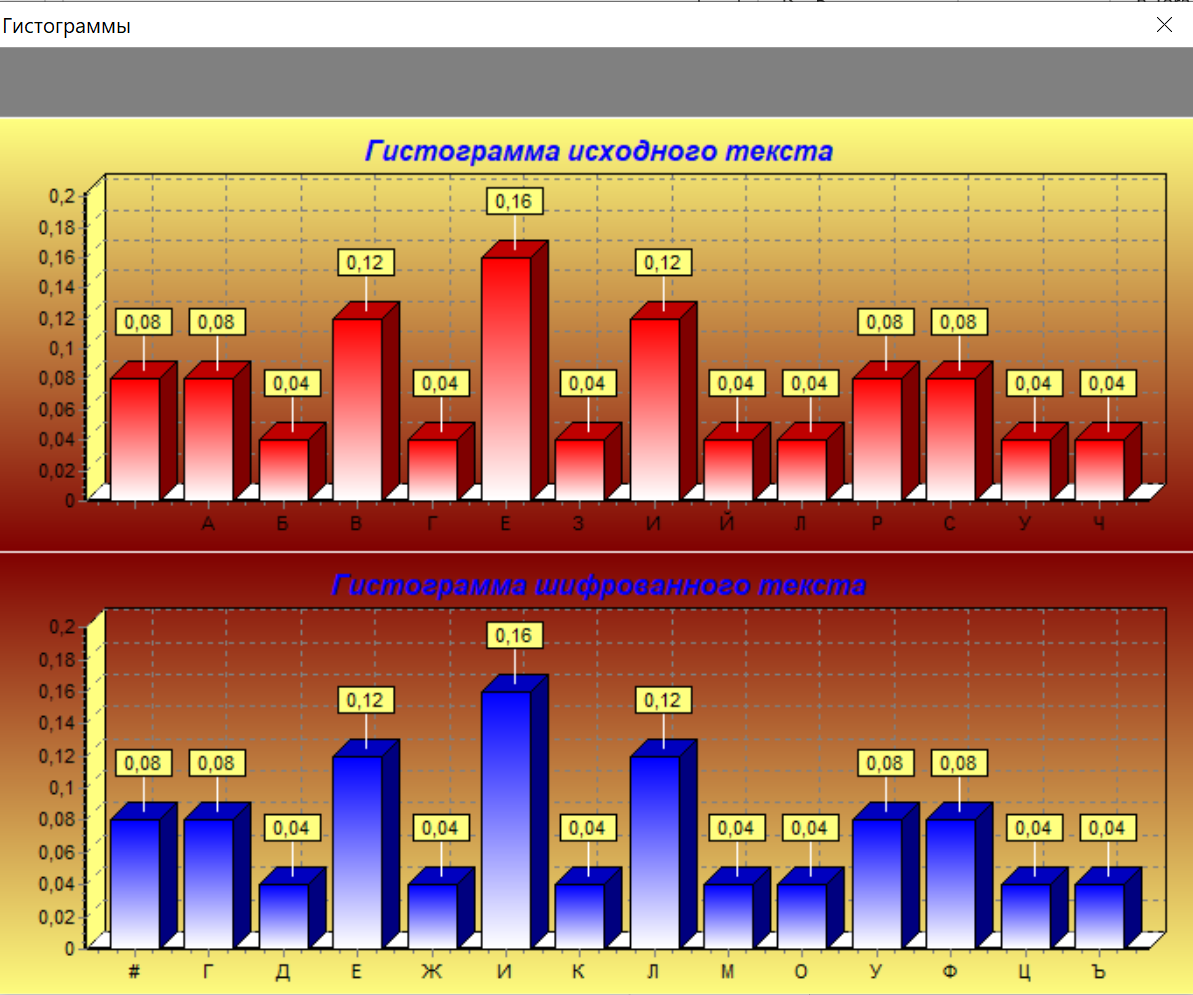
Эксперимент 1



1- исходный текст



2- исходный текст

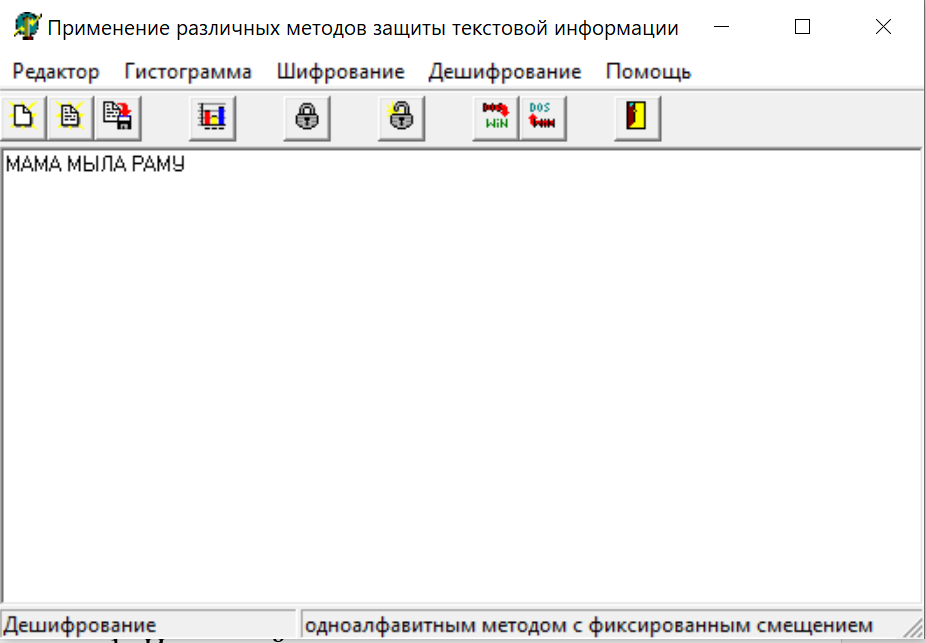


* Описать и объяснить процесс дешифрования.

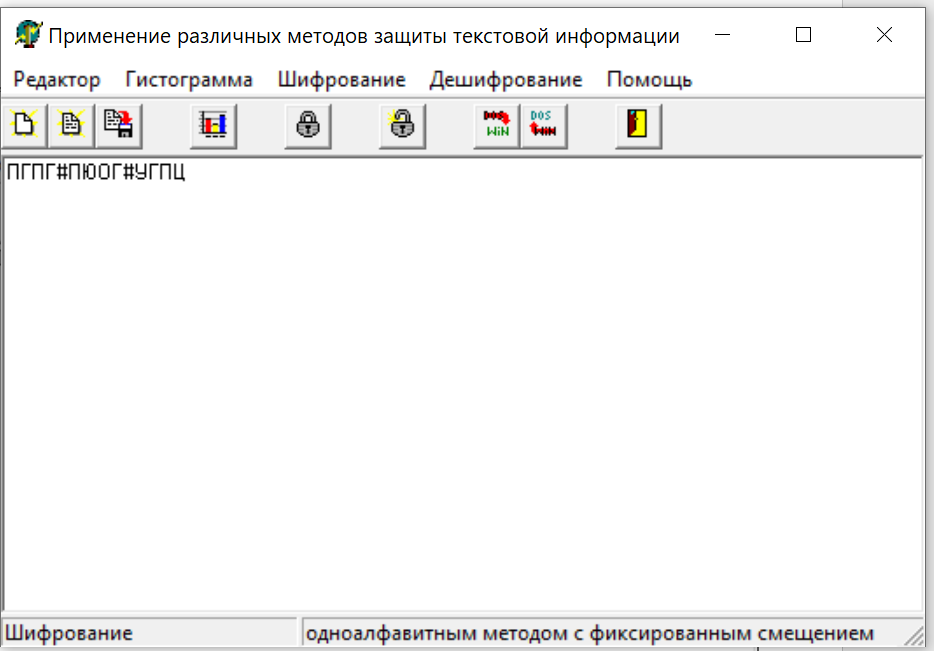
Так как зашифрованный текст повторяет структуру открытого текста, соответственно распределение зашифрованных символов такое же, как и открытом тексте. На моем примере буква «Е» смещается преобразовалась в «И». По формуле 200 = (197 + к), тогда к = 3

Найден ключ к = 3

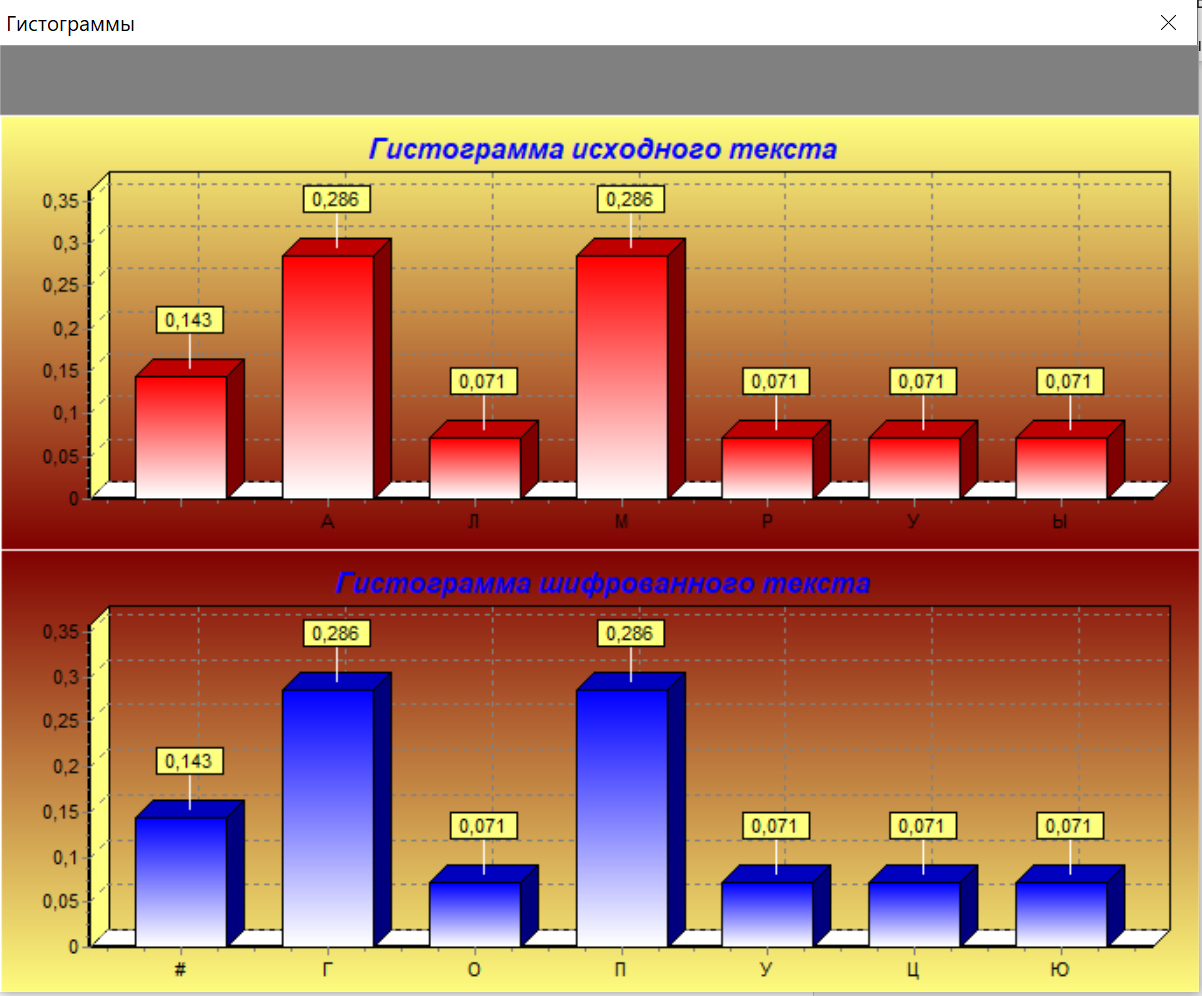
Эксперимент 2



1- Исходный текст

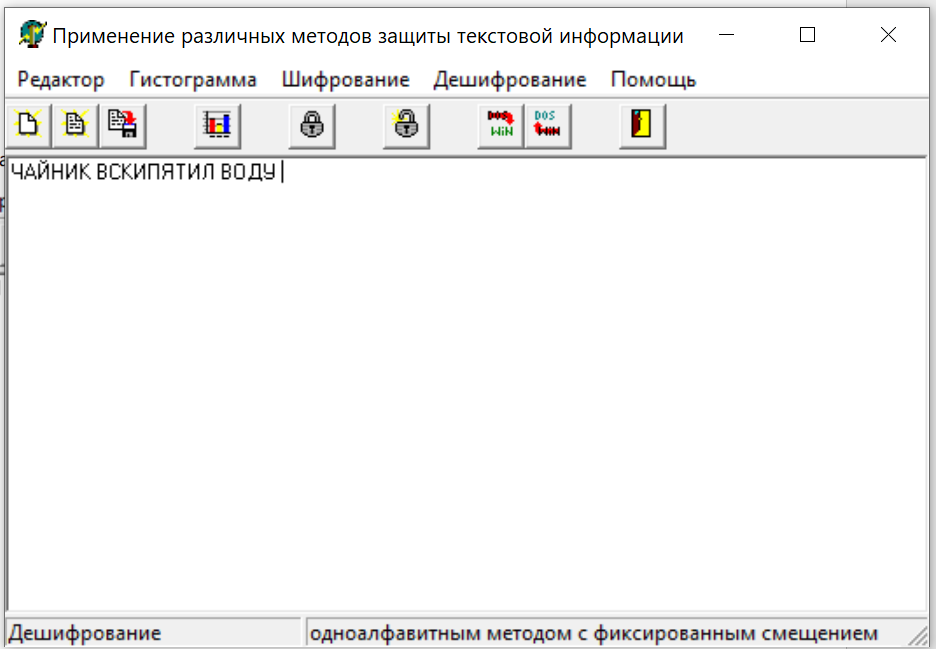


2 – Зашифрованный текст

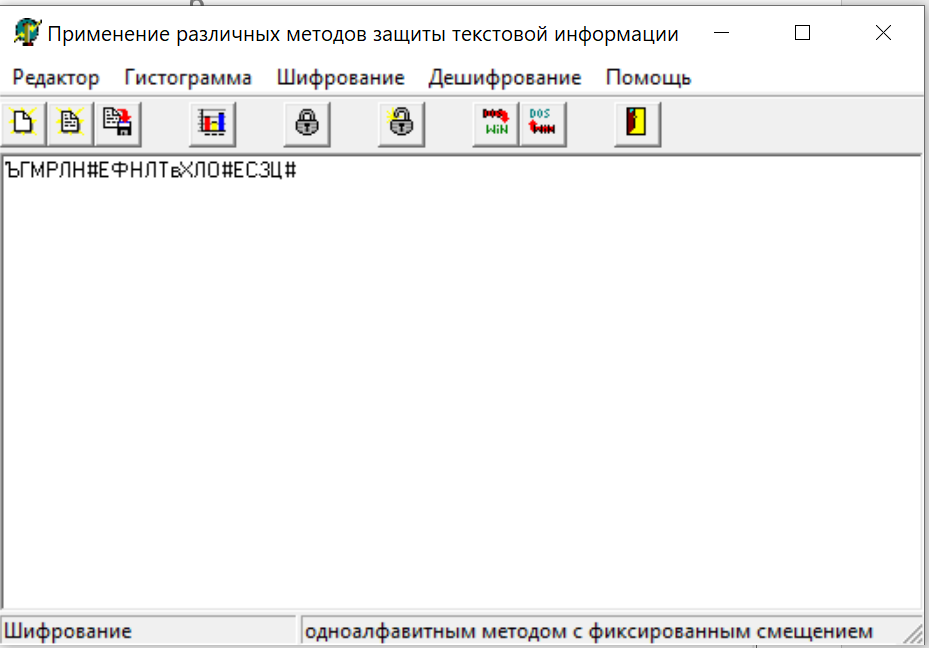


3 - Гистограммы

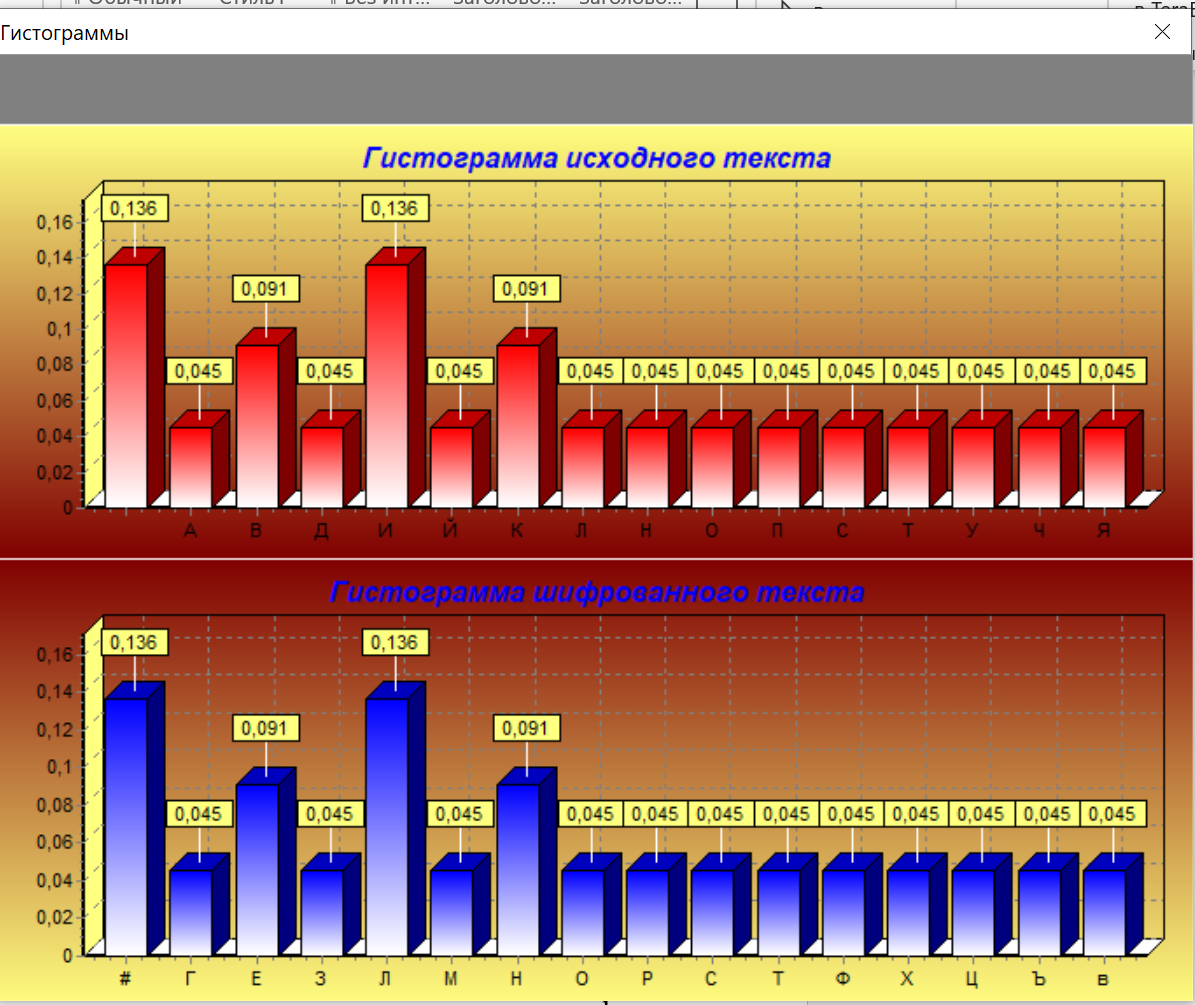
Эксперимент 3



1- Исходный текст



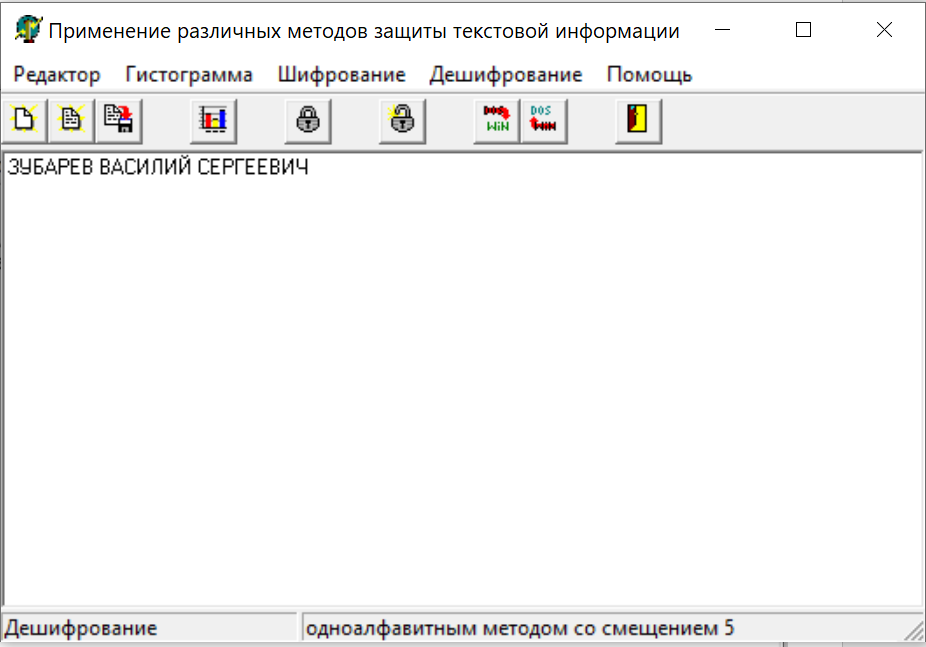
2 – зашифрованный текст



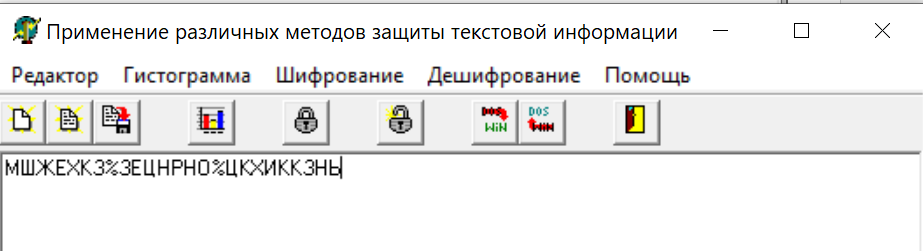
3 - Гистограммы

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

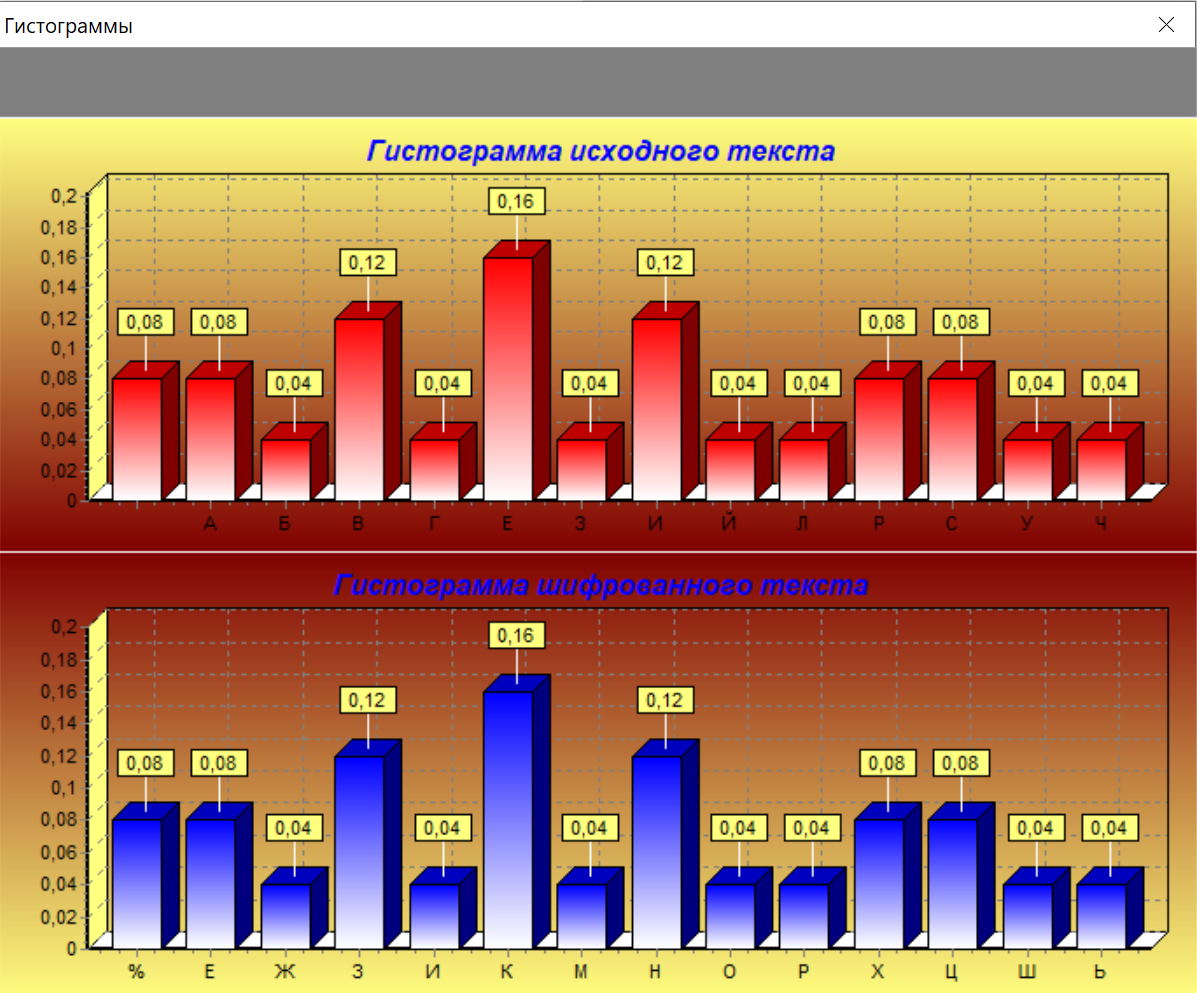
Эксперимент 1



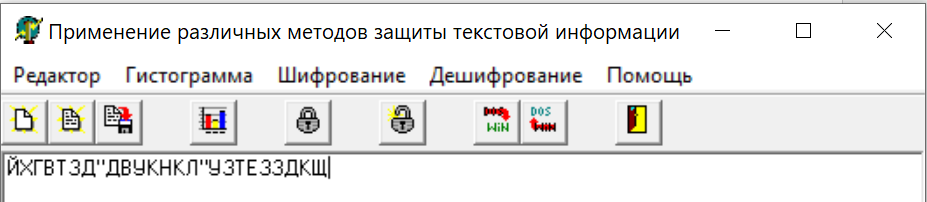
1- Исходный текст



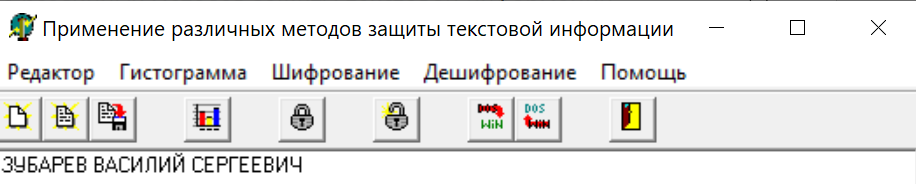
2 – Зашифрованный текст (смещение 5)



3 – Гистограммы



4 – Дешифрование подбором смещения (расшифровка со смещением 3)



5 – Дешифрование подбором смещения (расшифровка со смещением 5)

N = 256 => Tm=(T0+k)

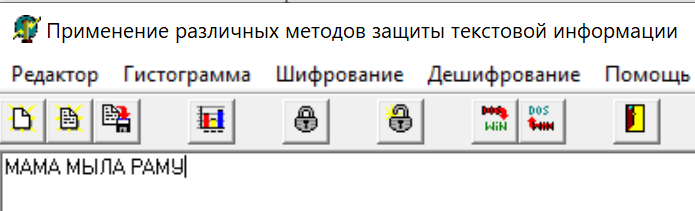
Определим k:

Tm=(T0+k)

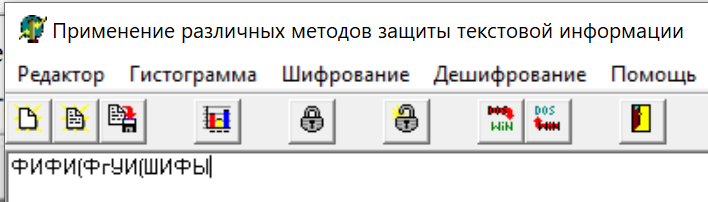
‘К’: (197 +k1) = 202 => k1 = 5

Ключ найден К = 5

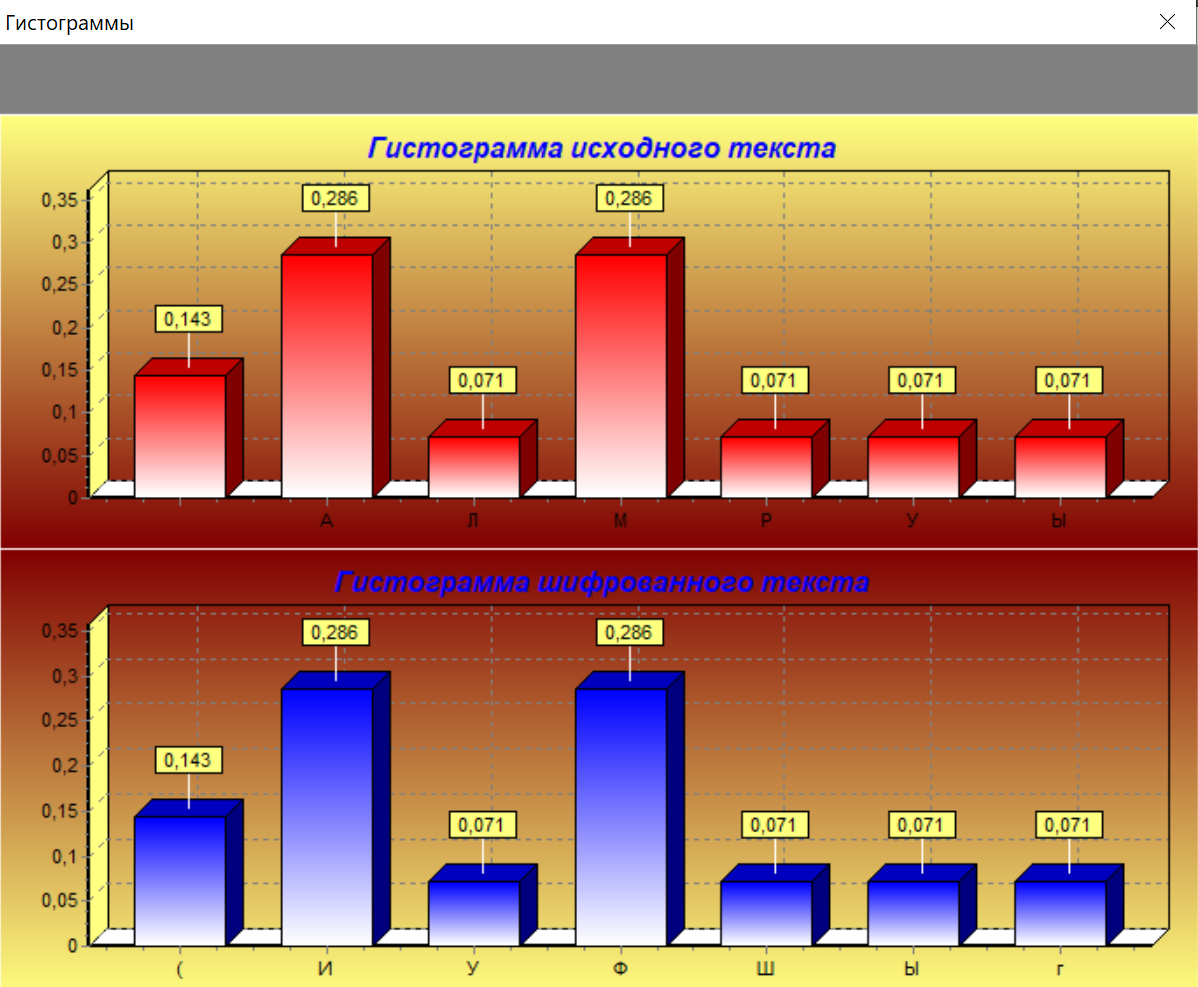
Эксперимент 2



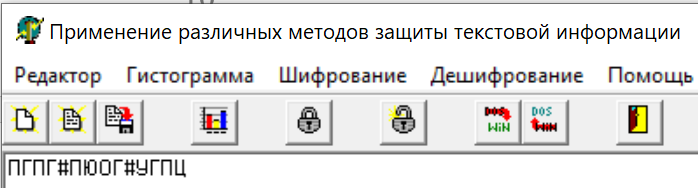
1- Исходный текст



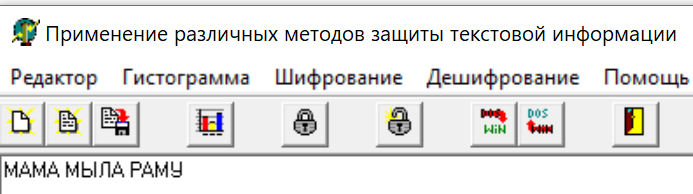
2 – Зашифрованный текст (смещение 8)



3 – Гистограммы

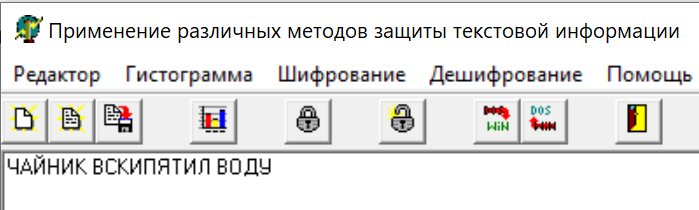


4 – Дешифрование подбором смещения (расшифровка со смещением 5)

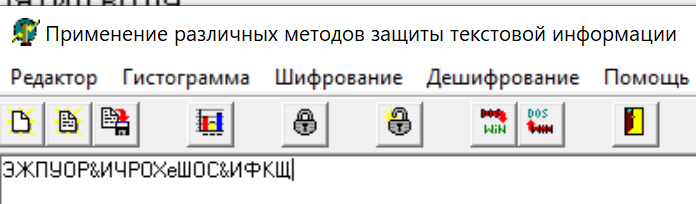


5 – Дешифрование подбором смещения (расшифровка со смещением 8)

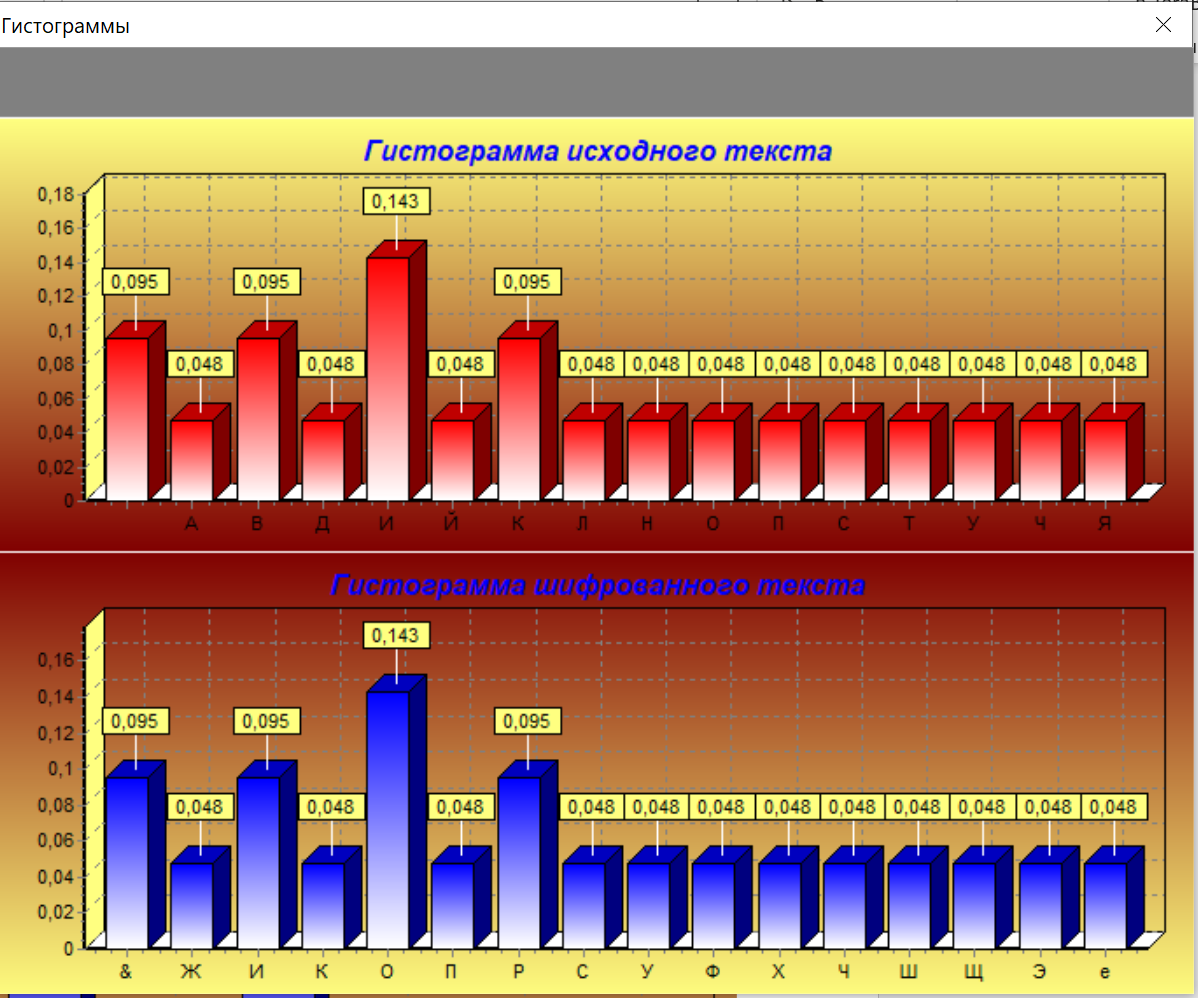
Эксперимент 3



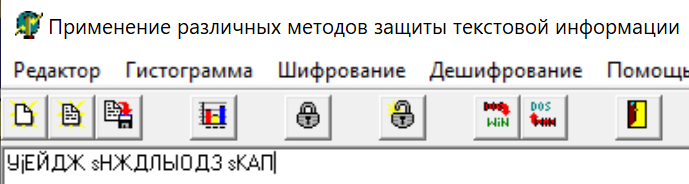
1- Исходный текст



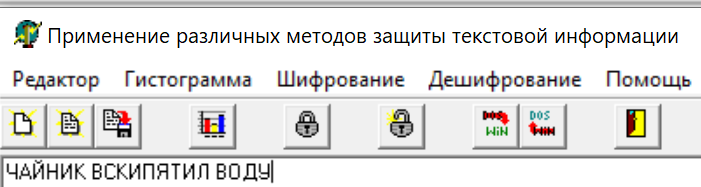
2 – Зашифрованный текст (смещение 6)



3 – Гистограммы



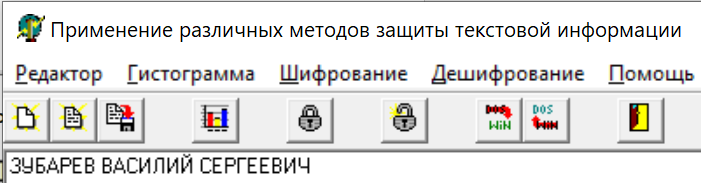
4 – Дешифрование подбором смещения (расшифровка со смещением 10)



5 – Дешифрование подбором смещения (расшифровка со смещением 6)

4. Для метода перестановки символов дешифровать зашифрованный текст.

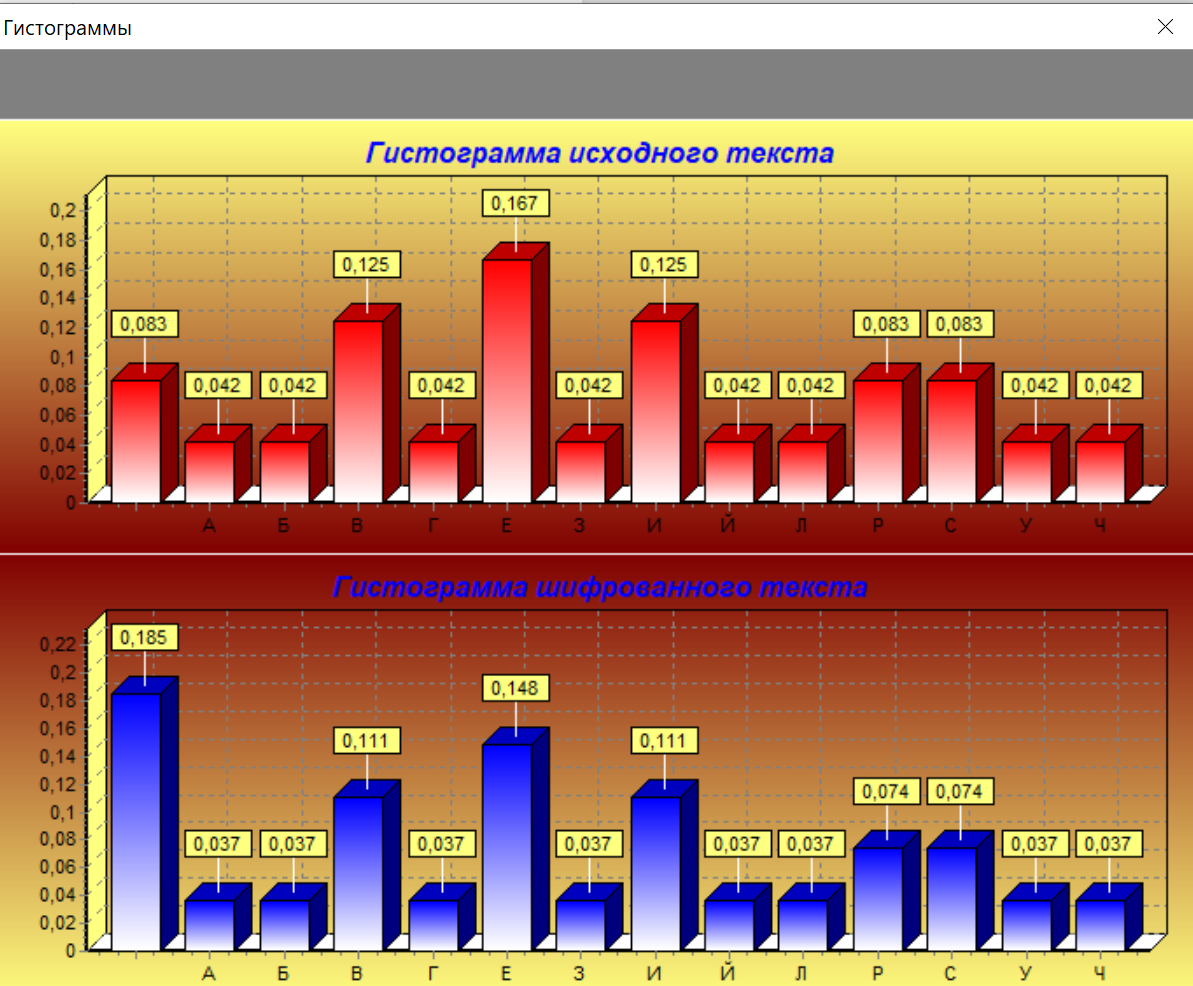
Эксперимент 1



1- Исходный текст



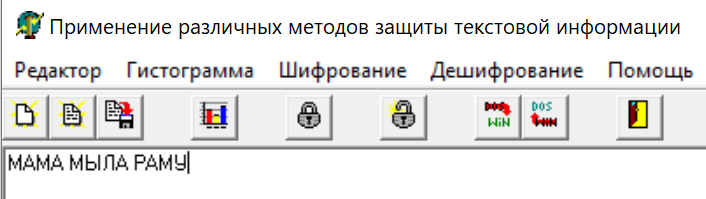
2 – Зашифрованный текст (ключ 321)



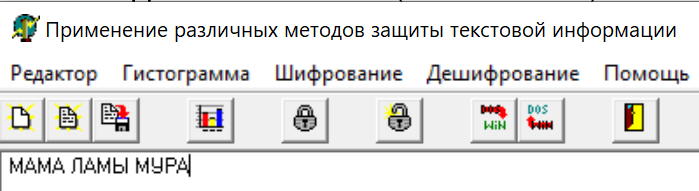
3 – Гистограммы (полезную информацию извлечь нельзя)

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)

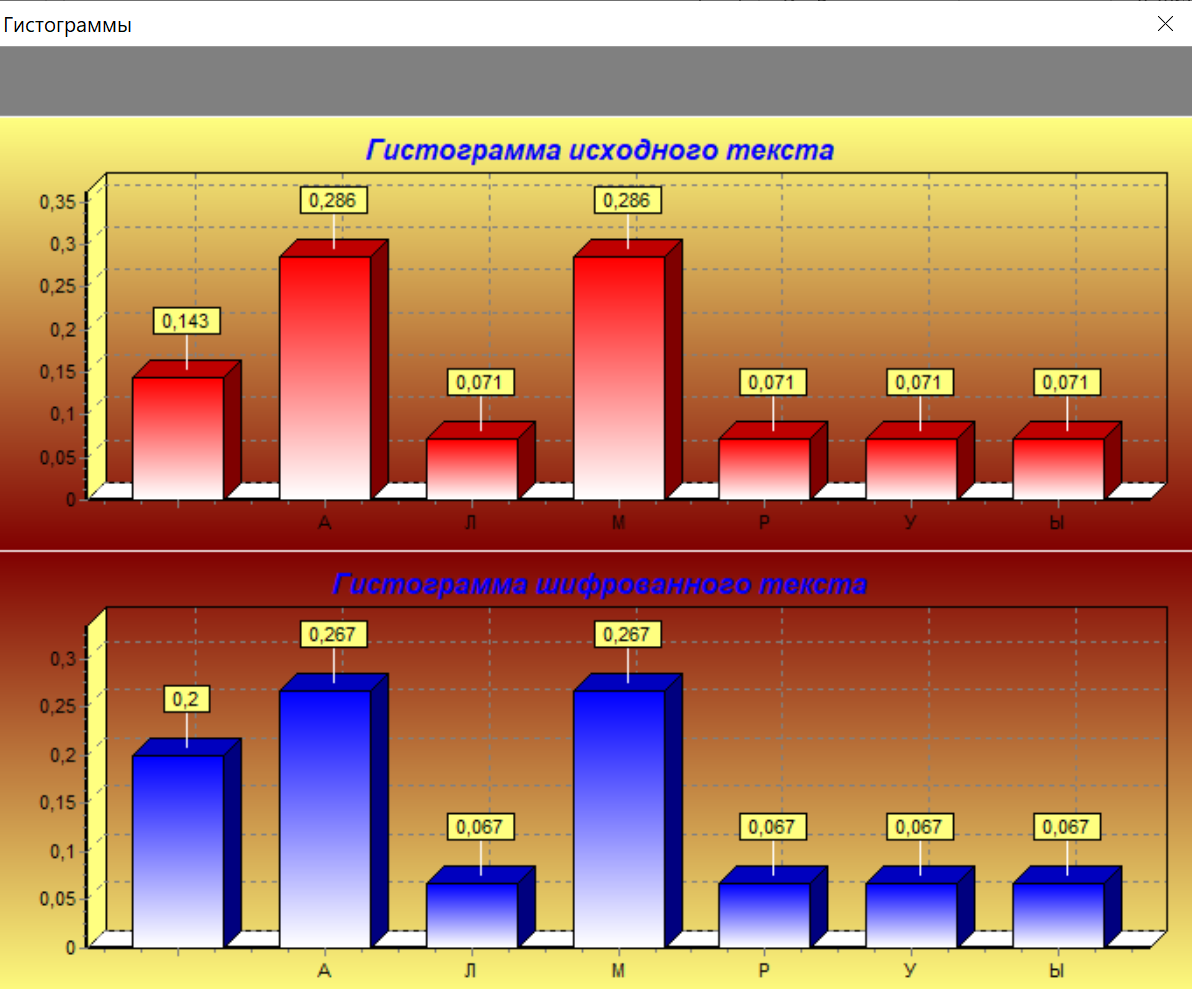
Эксперимент 2



1- Исходный текст

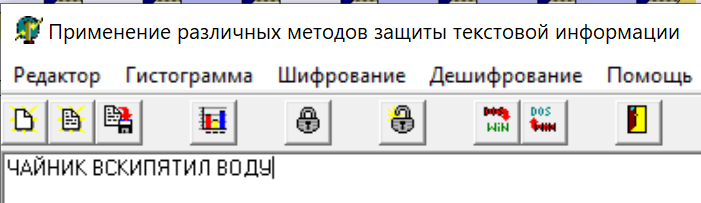


2 – Зашифрованный текст (ключ 53412)

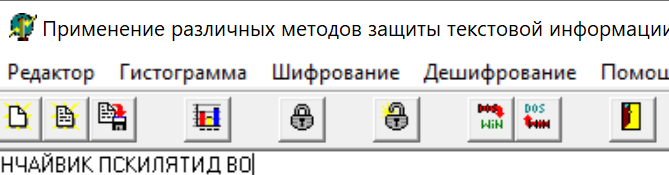


3 – Гистограммы (полезную информацию извлечь нельзя)

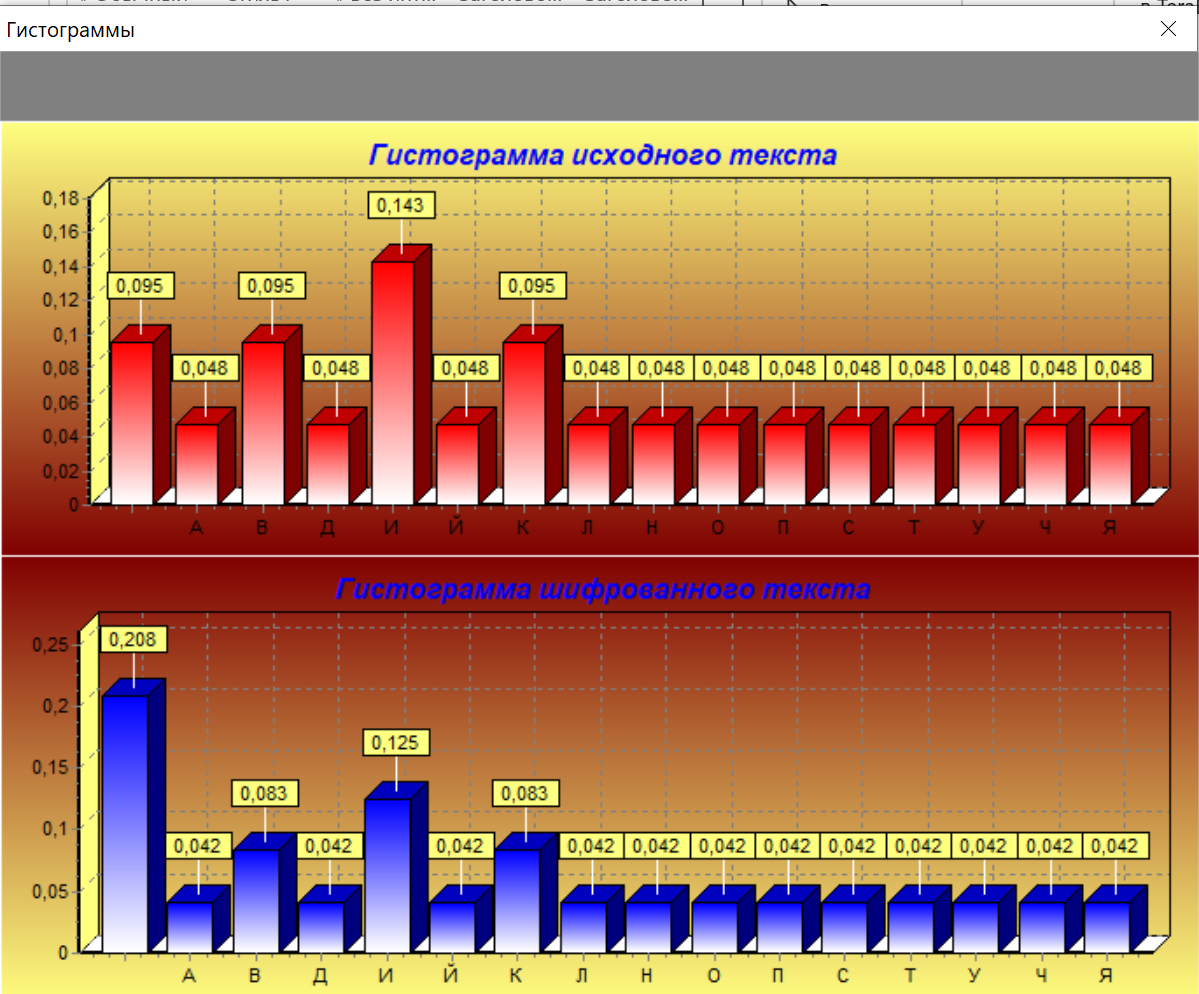
Эксперимент 3



1- Исходный текст



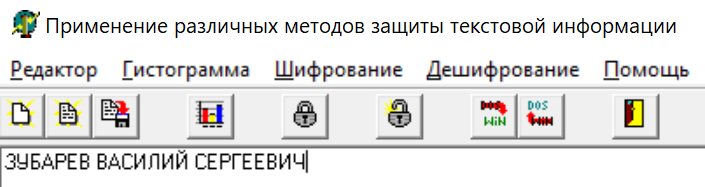
2 – Зашифрованный текст (ключ 2341)



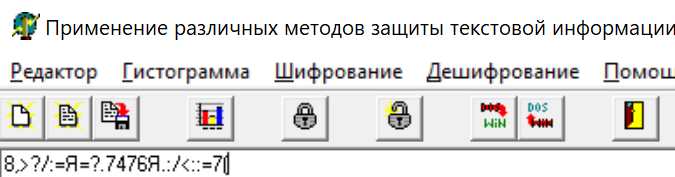
3 – Гистограммы (полезную информацию извлечь нельзя)

5. Для инверсного кодирования (по дополнению до 255)

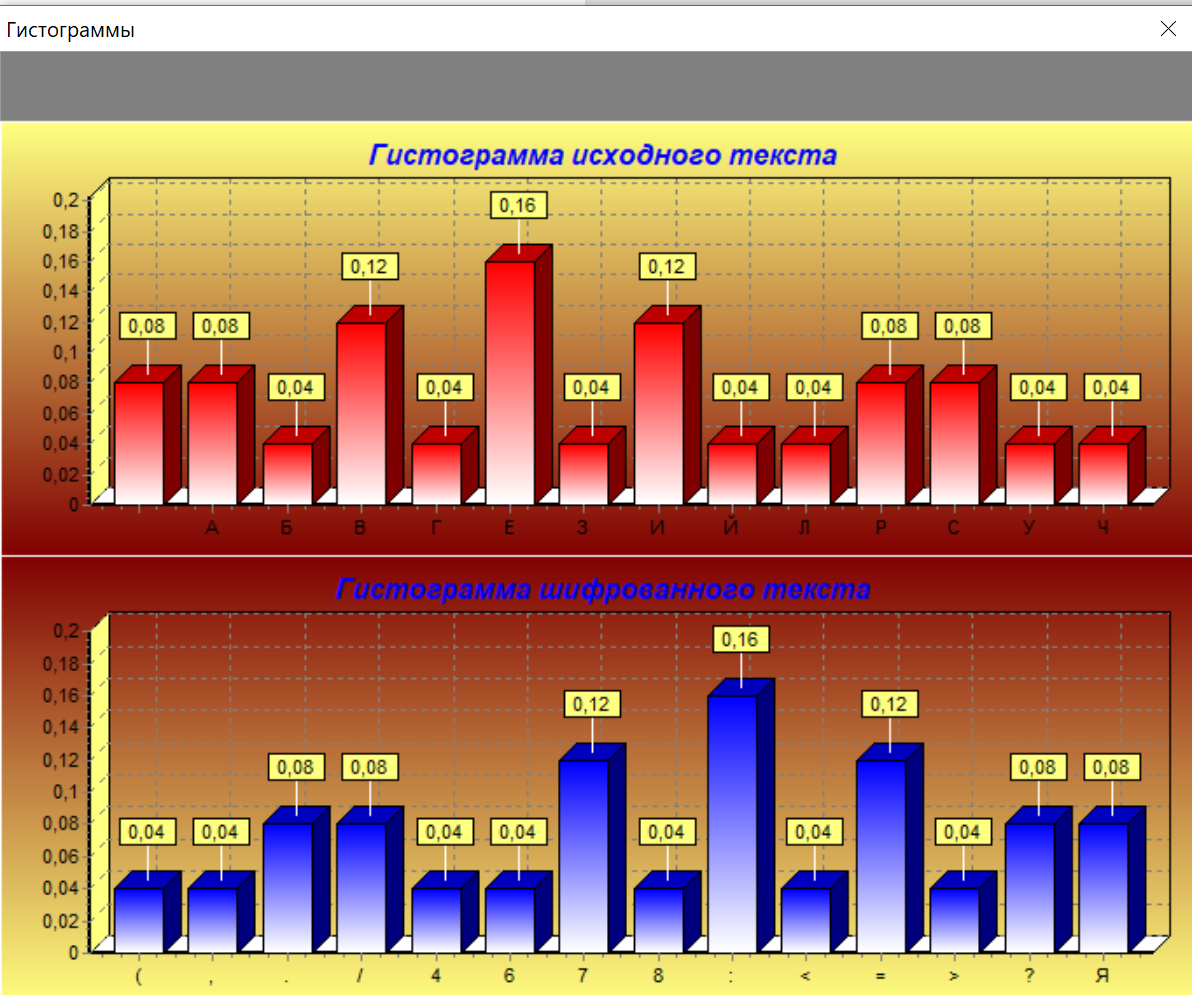
Эксперимент 1



1- Исходный текст



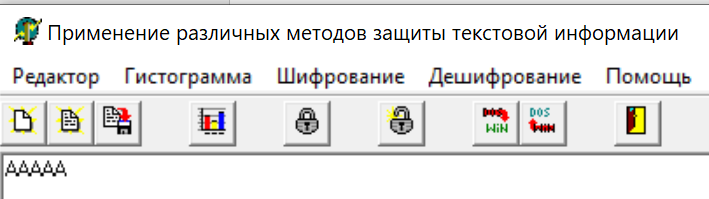
2 – Зашифрованный текст (ключ 2341)



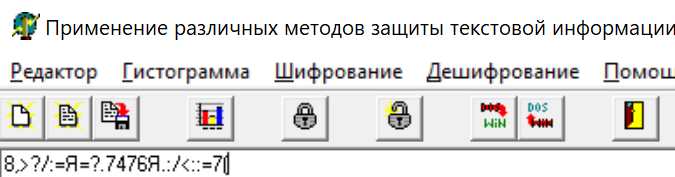
3 – Гистограммы Тш=N-T0 (на примере 58=255-197)

В данном случае N=256, так как нумерация начинается с 0, а заканчивается 255 поэтому вычитается из 255.

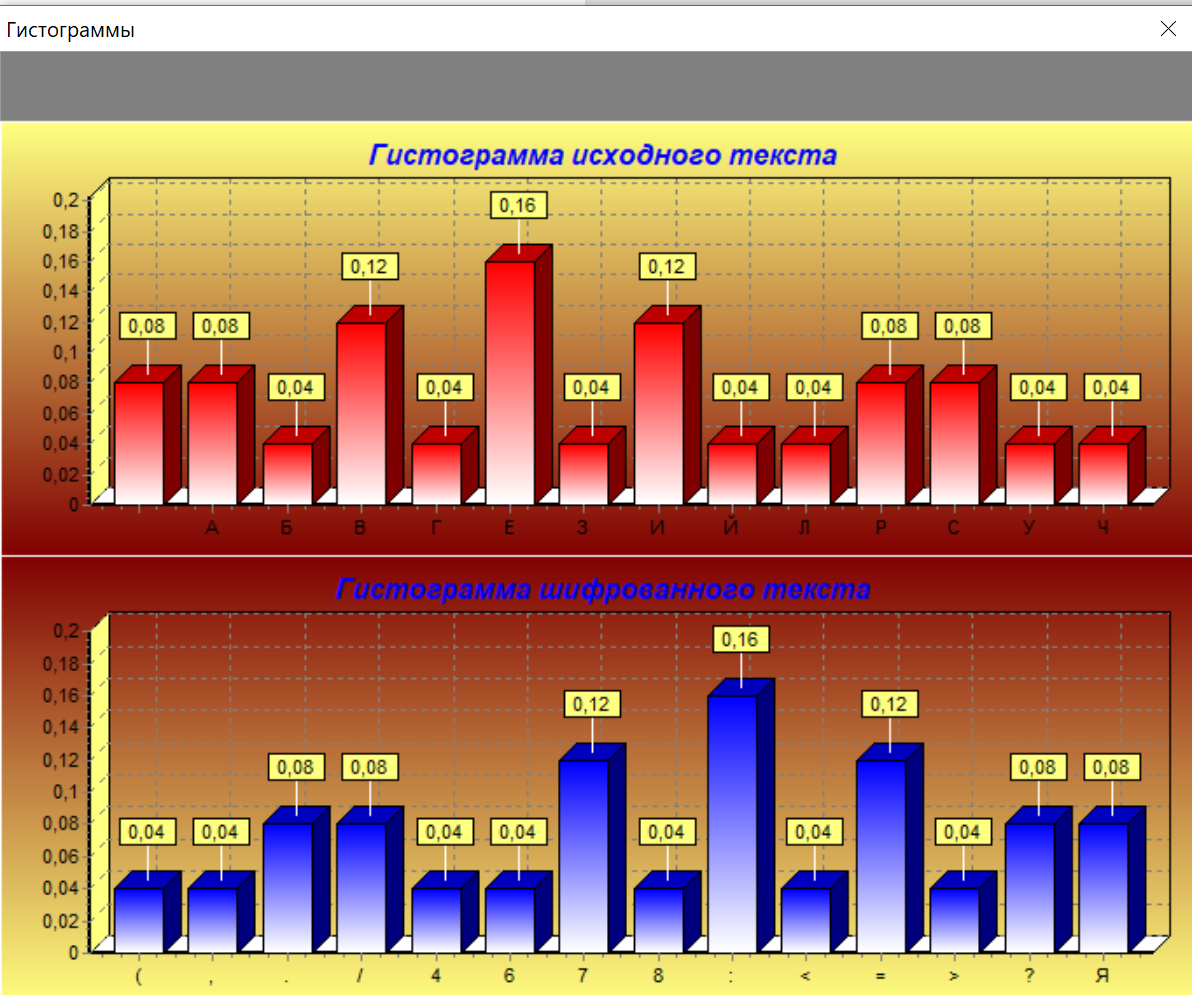
Эксперимент 2



1- Исходный текст



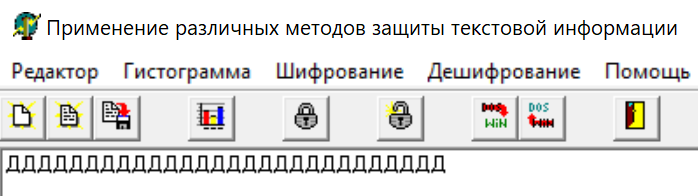
2 – Зашифрованный текст



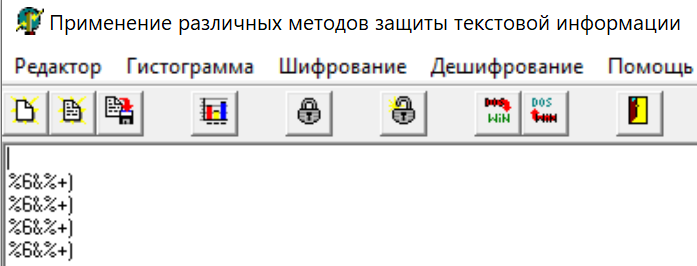
3 – Гистограммы Тш=255-T0 (на примере 58=255-197)

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

Эксперимент 1



1- Исходный текст



2 – Зашифрованный текст

Описание дешифрования текста.

В данном случае блок зашифрованного текста состоит из 7 одно алфавитных методов. Для вычисления ключа применяется Tш=(То+К) mod 255

Применяя формулу, получаем, что в многоалфавитном шифре применяется 7 одно алфавитных шифров Цезаря со следующими смещениями:

К1=74

К2=97

К3=114

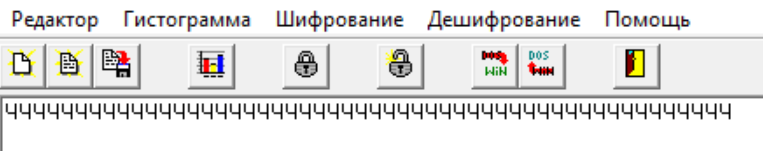
К4=98

К5=97

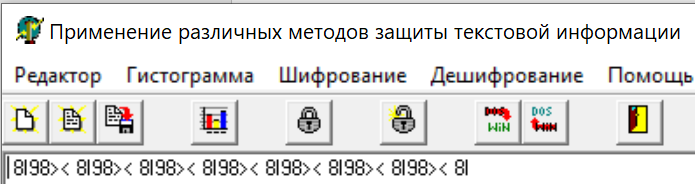
К6=103

К7=101

Эксперимент 2



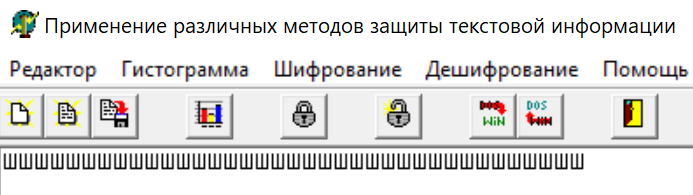
1- Исходный текст



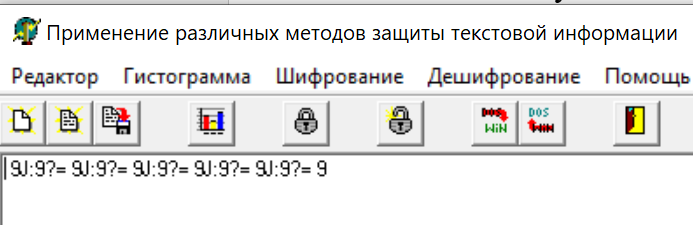
2 – Зашифрованный текст

Результаты подбора ключей аналогичны эксперименту 1

Эксперимент 3



1- Исходный текст

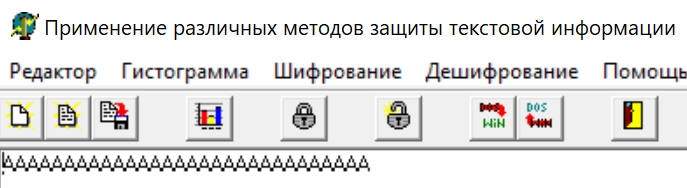


2 – Зашифрованный текст

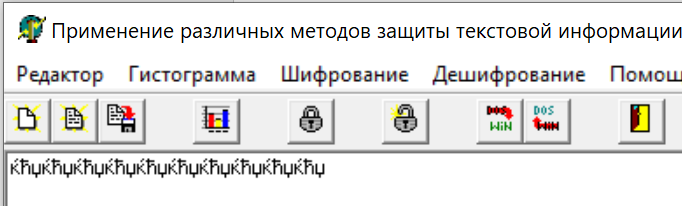
Результаты подбора ключей аналогичны эксперименту 1

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

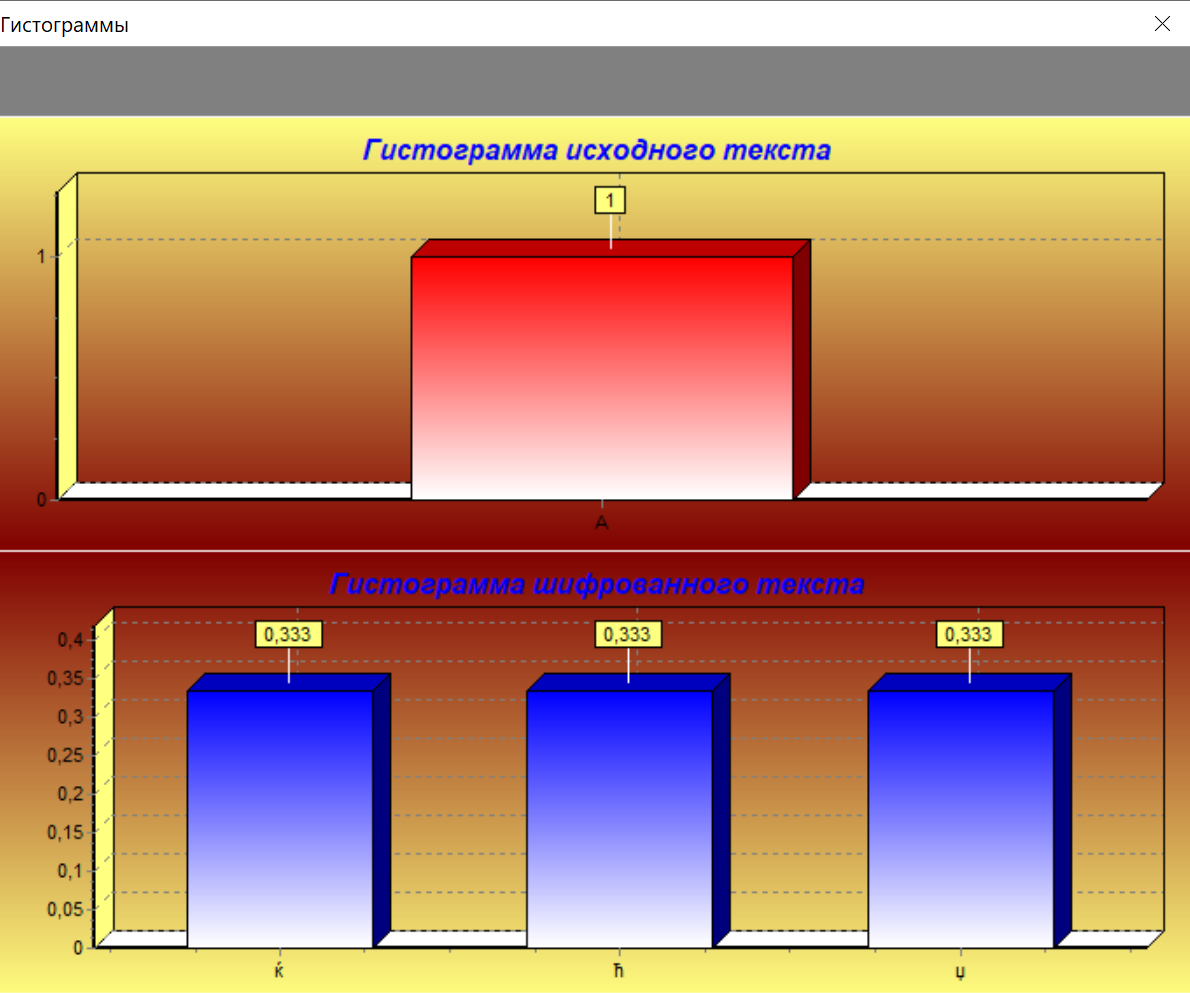
Эксперимент 1



1- Исходный текст



2 – Зашифрованный текст (ключ ЭЮЯ)



3 – Гистограмма

Из гистограммы видно, что существует 3 ключа.

N = 256 => Tm=(T0+k) mod 256

Определим k:

Tm=(T0+k)modN

‘Ѕ’: (192 +k1) mod 256 = 189 => k1 = 253 ‘э’

‘ѕ’: (192 +k2) mod 256 = 190=> k2 = 254 ‘ю’

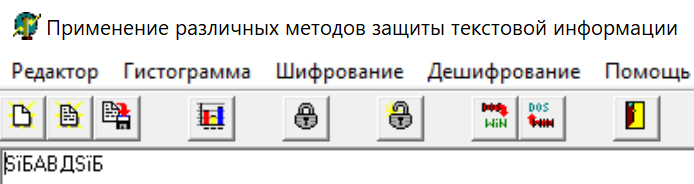
‘ї’: (192 +k3) mod 256 = 191 => k3 = 255 ‘я’

Ключ: ‘эюя’

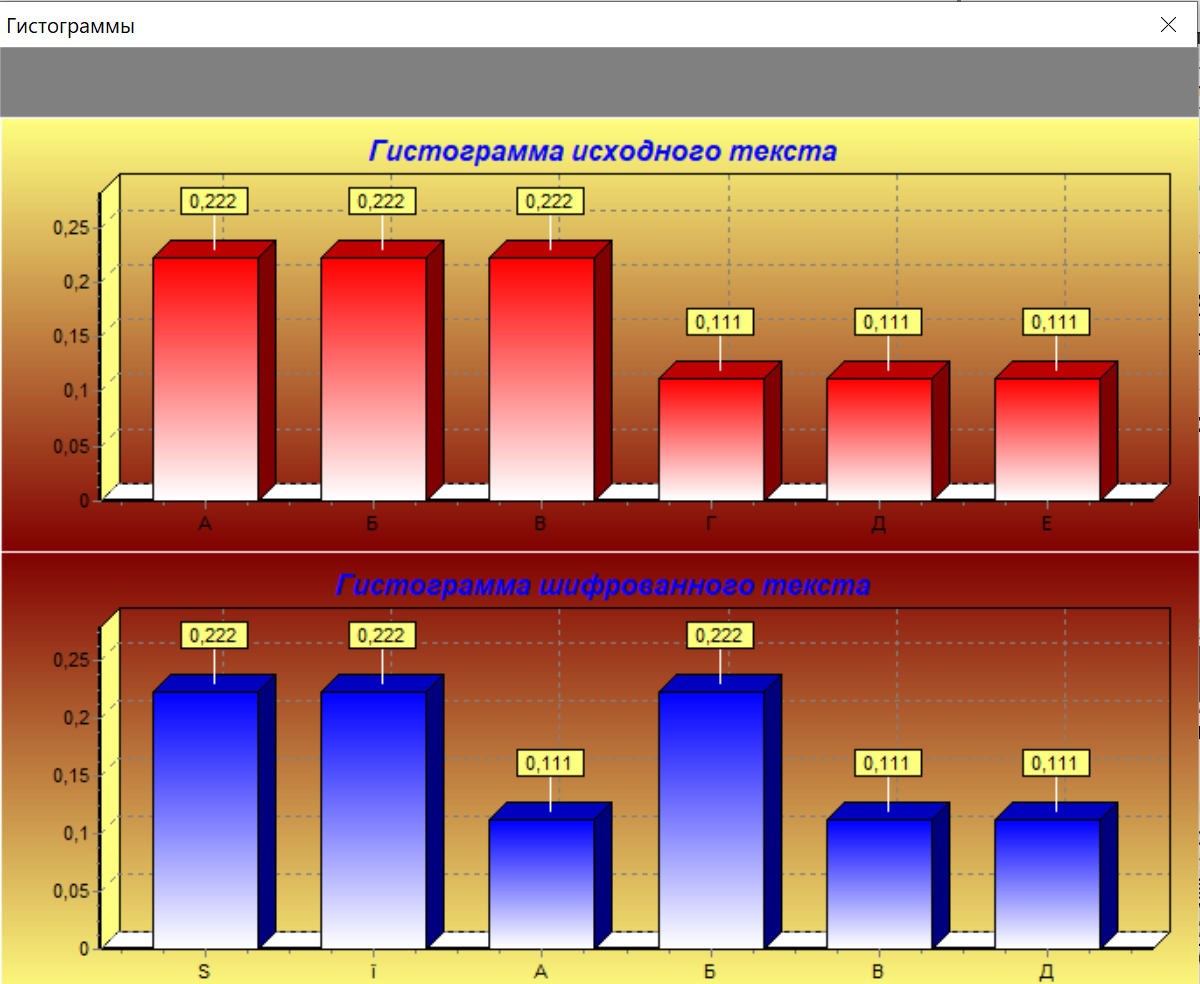
Эксперимент 2



1- Исходный текст



2 – Зашифрованный текст (ключ эюя)



3 – Гистограмма (длинна ключа эюя)

N = 256 => Tm=(T0+k) mod 256

Определим k:

Tm=(T0+k)modN

‘Ѕ’: (192 +k1) mod 256 = 189 => k1 = 253 ‘э’

‘ї’: (193 +k2) mod 256 = 190 => k2 = 254 ‘ю’

‘Б’: (194 +k3) mod 256 = 191 => k3 = 255 ‘я’

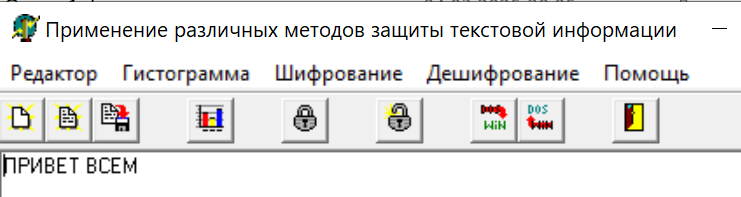
‘А’: (195 +k1) mod 256 = 192 => k1 = 253 ‘э’

‘В’: (196 +k2) mod 256 = 194 => k2 = 254 ‘ю’

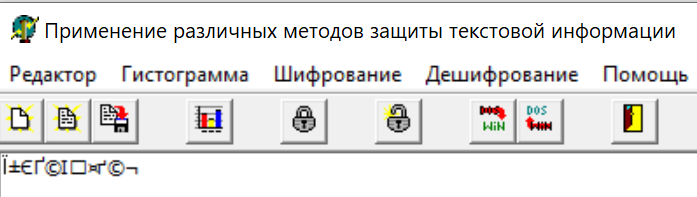
‘Д’: (197 +k3) mod 256 = 195 => k3 = 255 ‘я’

Ключ: ‘эюя’

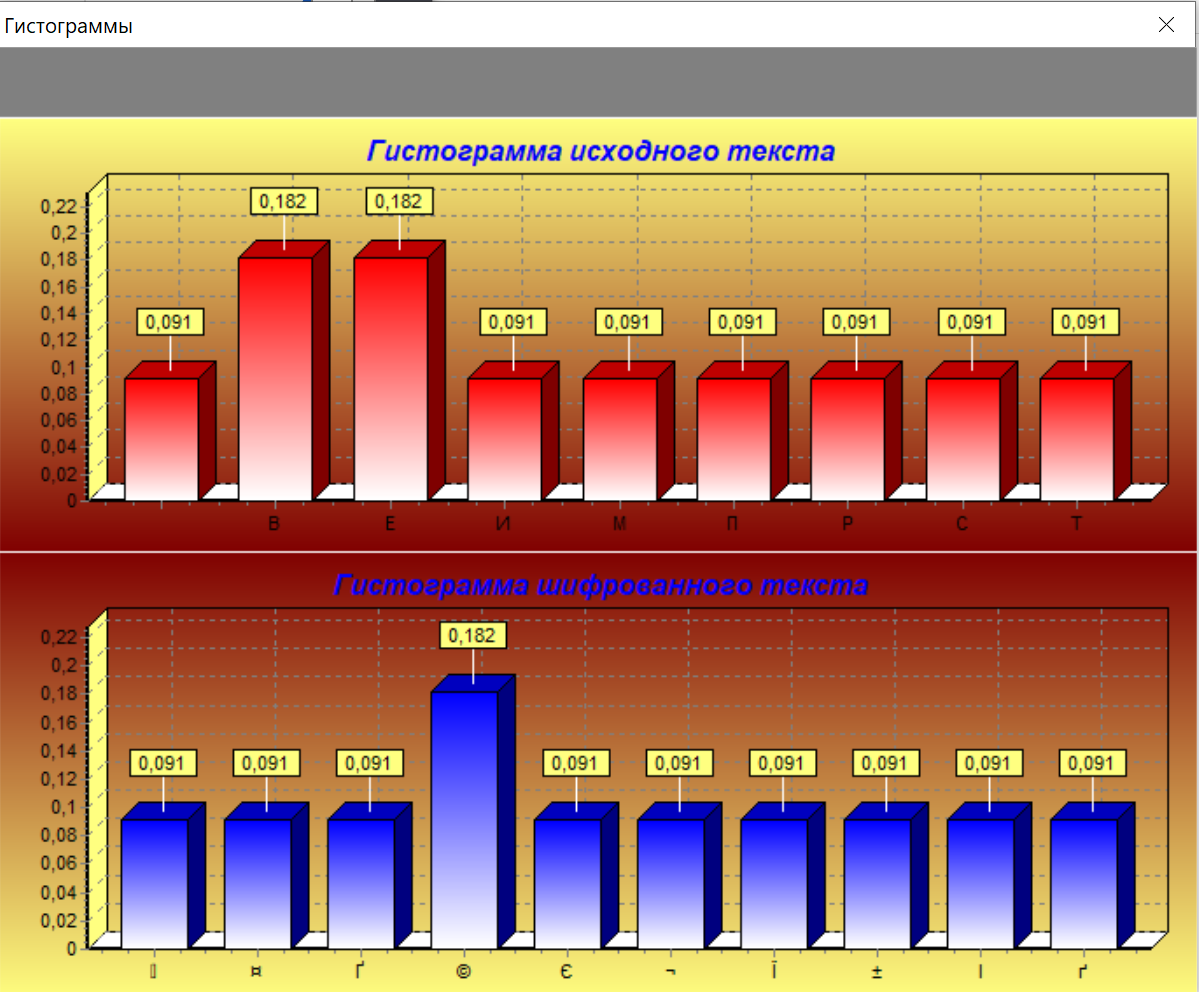
Эксперимент 3



1- Исходный текст



2 – Зашифрованный текст (ключ абвгд)



3 – Гистограмма (ключ абвгд)

Tm=(T0+k)modN

‘Ї’: (207 +k1) mod 256 = 175=> k1 = 224 ‘а’

‘±’: (208 +k2) mod 256 =176 => k2 = 225 ‘б’

‘Є’: (200 +k3) mod 256 = 170 => k3 = 226‘в’

‘Ґ’: (194 +k1) mod 256 = 165 => k1 = 227 ‘г’

‘©’: (197 +k2) mod 256 = 169 => k2 = 228 ‘д’

‘І’: (197 +k3) mod 256 = 178 => k3 = 224 ‘а’

‘\_’: (32 +k1) mod 256 = 1 => k1 = 225 ‘б’

‘¤’: (196 +k2) mod 256 = 164 => k2 = 226 ‘в’

‘ґ’: (209 +k3) mod 256 = 180 => k3 = 227 ‘г’

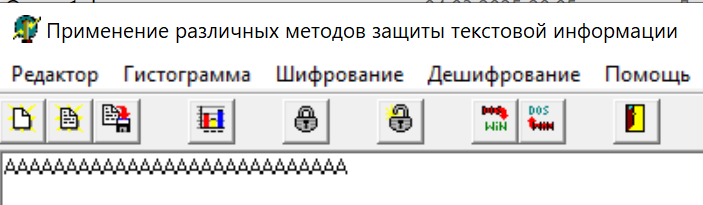
‘©’: (197 +k2) mod 256 = 169 => k2 = 228 ‘д’

‘¬’: (204 +k3) mod 256 = 172 => k3 = 224 ‘а’

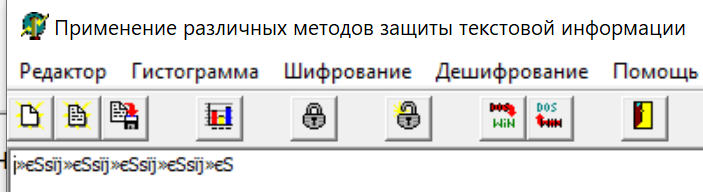
Ключ: абвгд

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

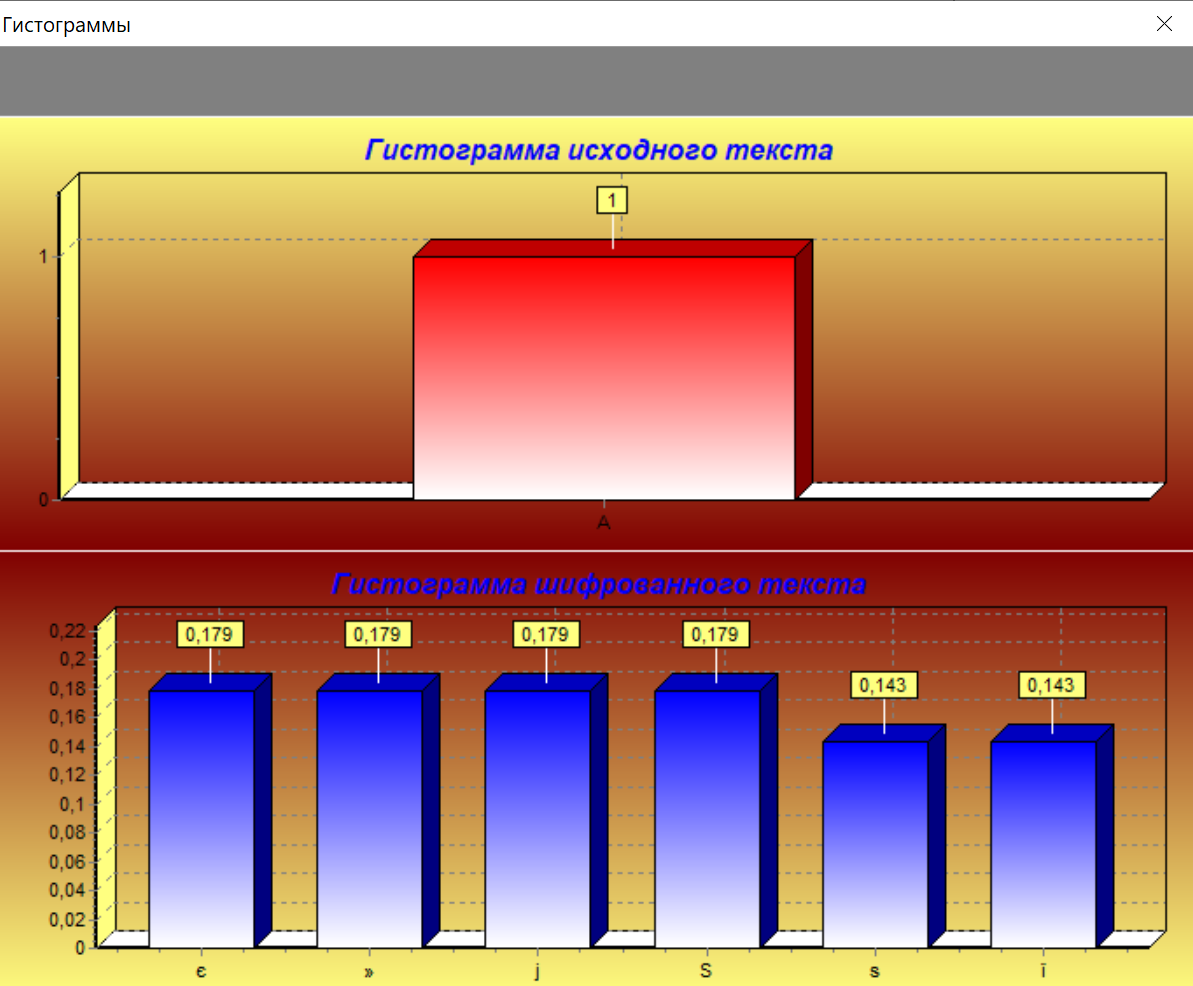
Эксперимент 1



1- Исходный текст



2 – Зашифрованный текст (ключ ьыъэюя)



3 – Гистограмма (ьыъэюя)

N = 256 => Tm=(T0+k) mod 256

ј»єЅѕїј»єЅѕїј»єЅѕїј»єЅѕїј»єЅ

Определим k:

Tm=(T0+k)modN

‘ј’: (192 +k1) mod 256 = 188 => k1 = 252 ‘ь’

‘»’: (192 +k2) mod 256 = 187 => k2 = 251 ‘ы’

‘є’: (192 +k3) mod 256 = 186 => k3 = 250 ‘ъ’

‘Ѕ’: (192 +k1) mod 256 = 189 => k1 = 253 ‘э’

‘ѕ’: (192 +k2) mod 256 = 190 => k2 = 254 ‘ю’

‘ї’: (192 +k3) mod 256 = 191 => k3 = 255 ‘я’

Ключ ‘ьыъэюя’

Задание 9

Привести пример, когда рассматриваемые алгоритмы могут назваться абсолютно стойкими шифрами

Для создания абсолютно стойкого шифра необходим ключ, отвечающий следующим условиям:

* все символы ключа равновероятны;
* длина ключа равна либо больше длинны исходного текста.

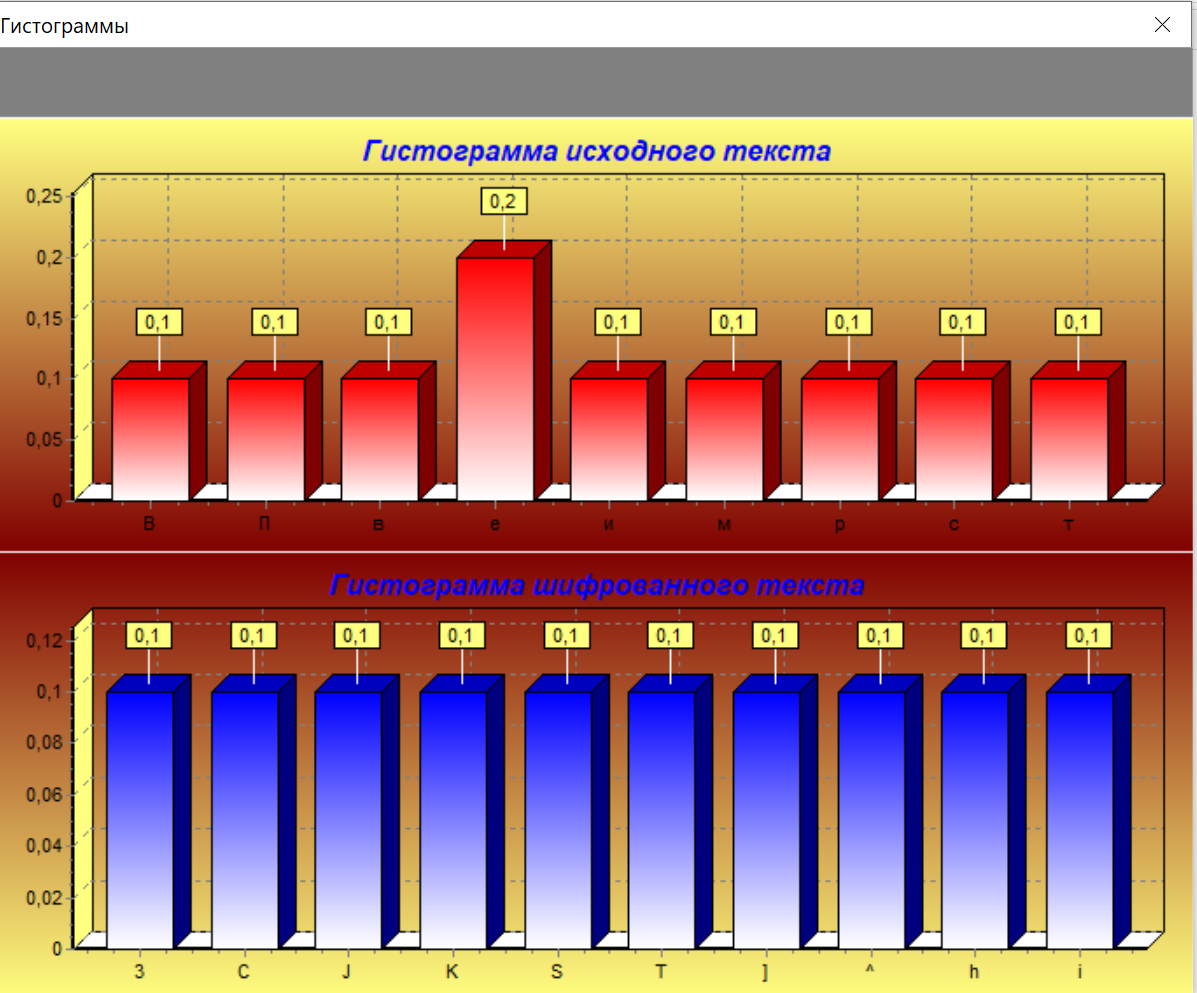
**Многоалфавитный шифр с ключом задаваемой длины**

Пример



1- Исходный текст

Ключ ‘qwertyuiopa’



2- Гистограмма

Вывод:

Из гистограммы видно, что все появление всех символов зашифрованного сообщения равновероятны, что исключает взлом шифра за счет метода частотного анализа.