

**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

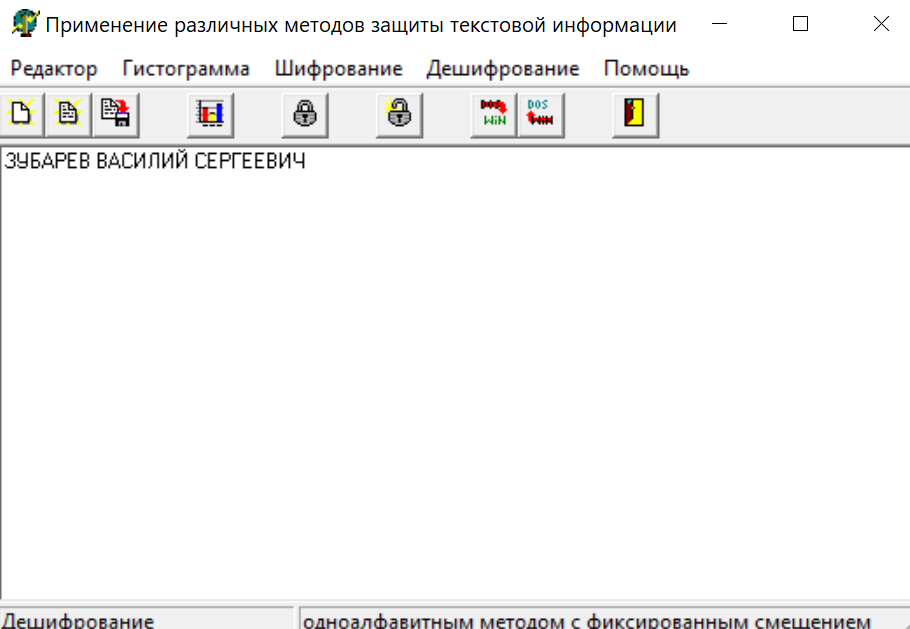
Учебной группы БИСО-02-22

Зубарев В.С.

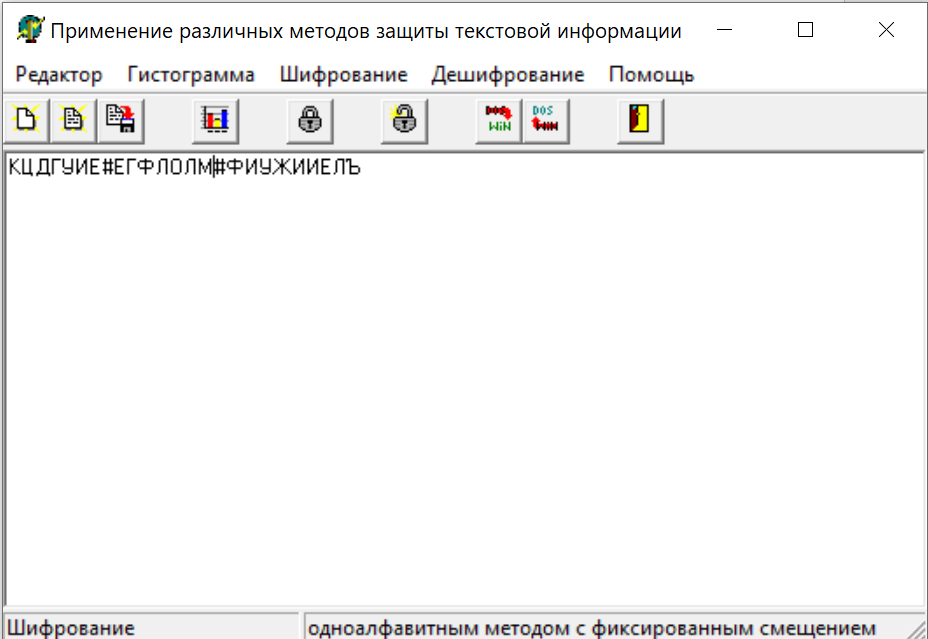
1. Ознакомиться с описанием лабораторной работы и заданием.

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

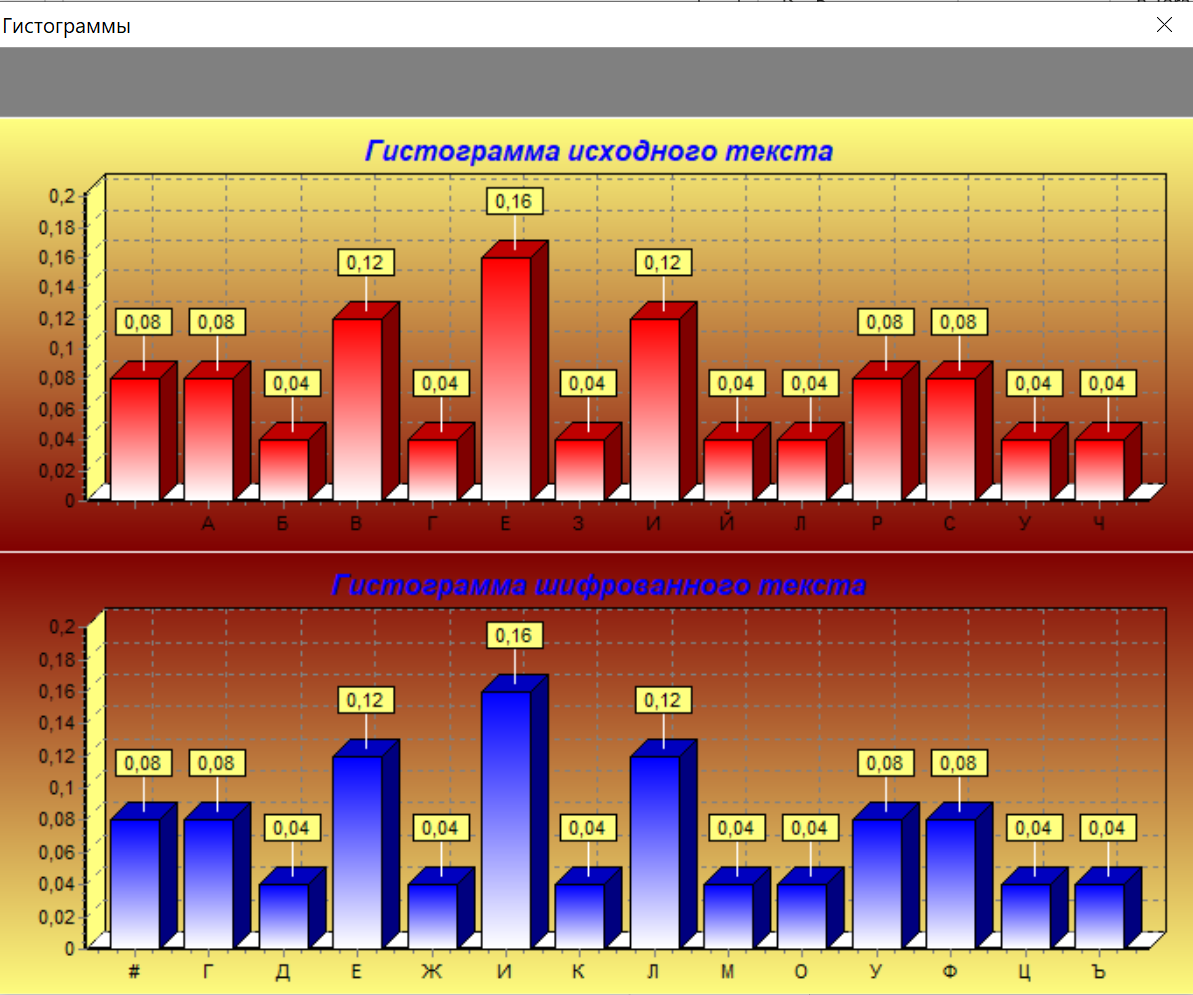
Эксперимент 1



1- исходный текст



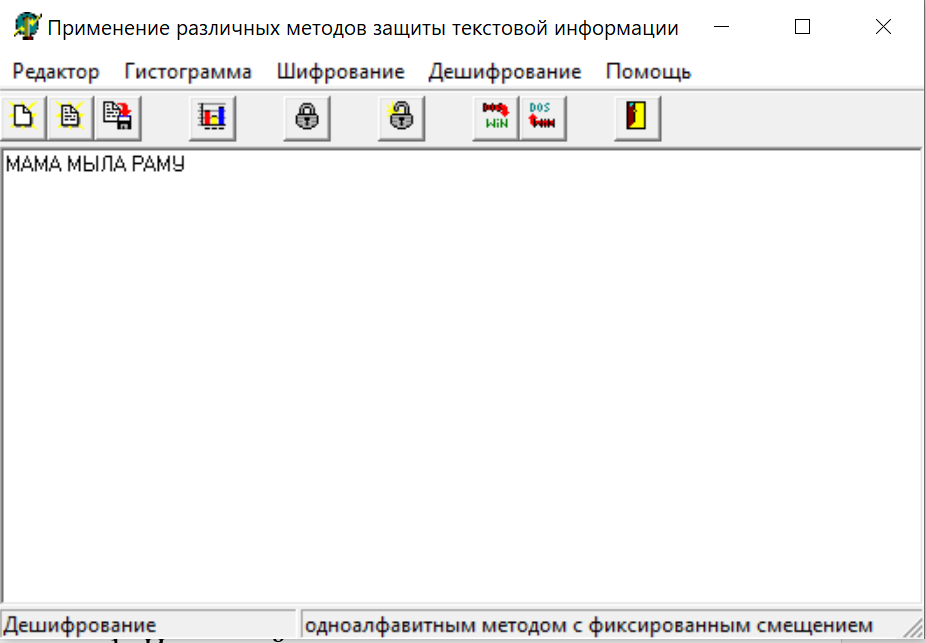
2- исходный текст



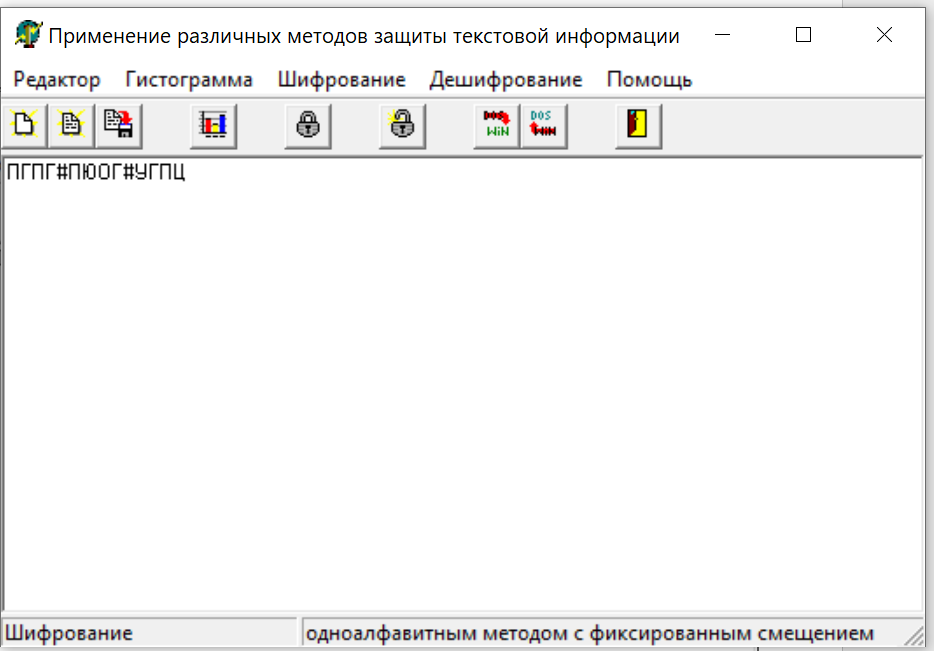
* Описать и объяснить процесс дешифрования.

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

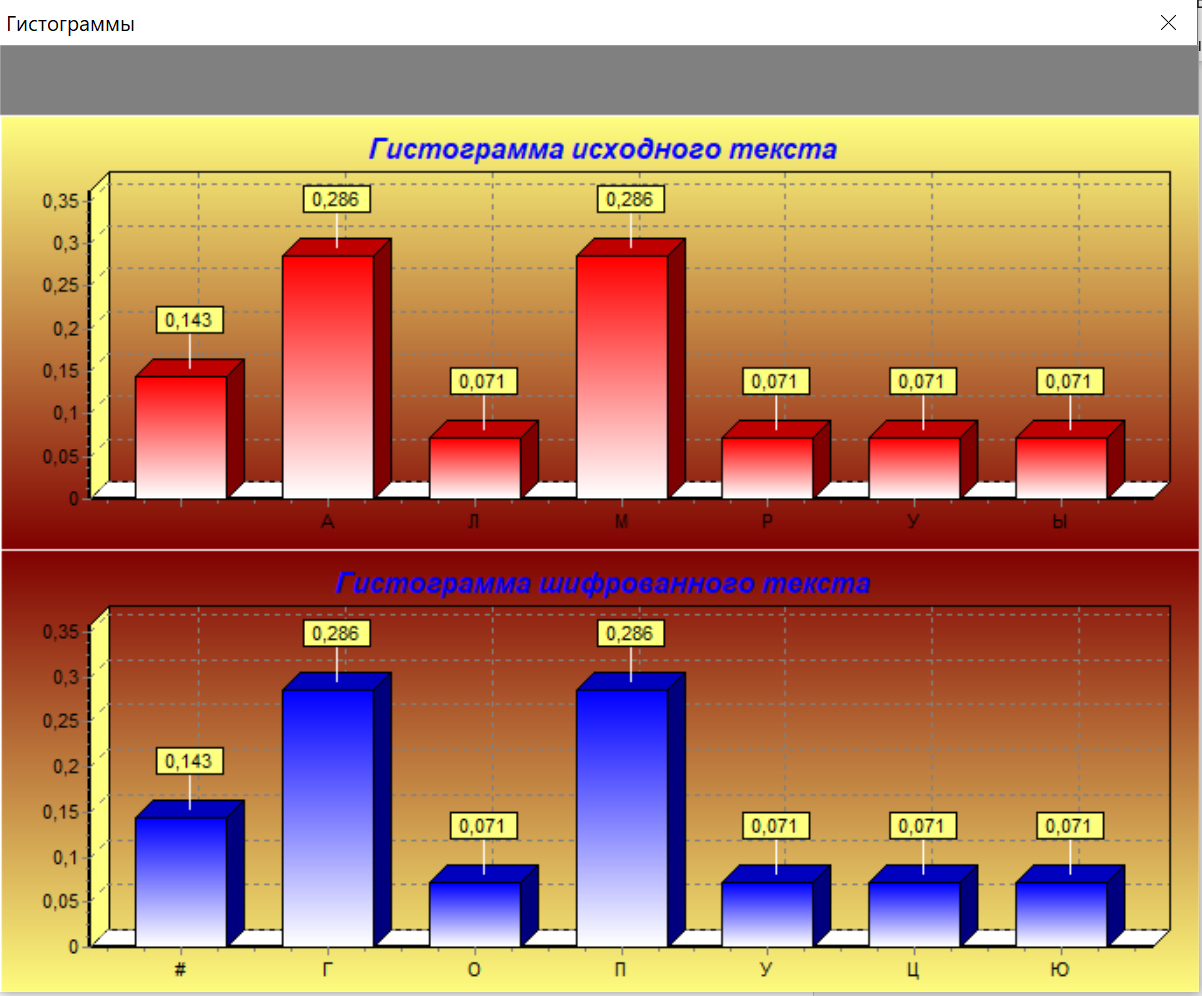
Эксперимент 2



1- Исходный текст

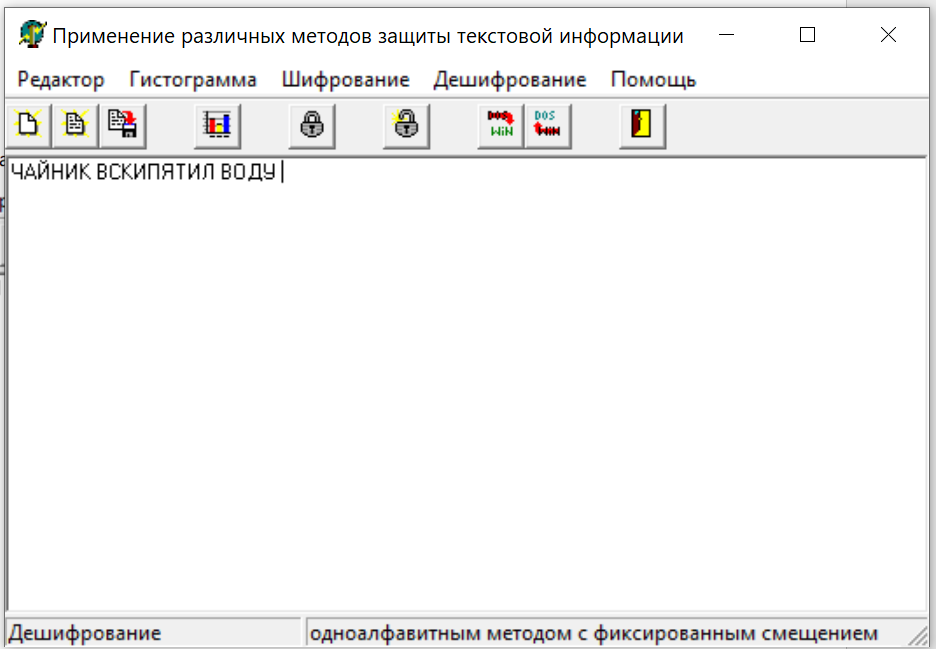


2 – Зашифрованный текст

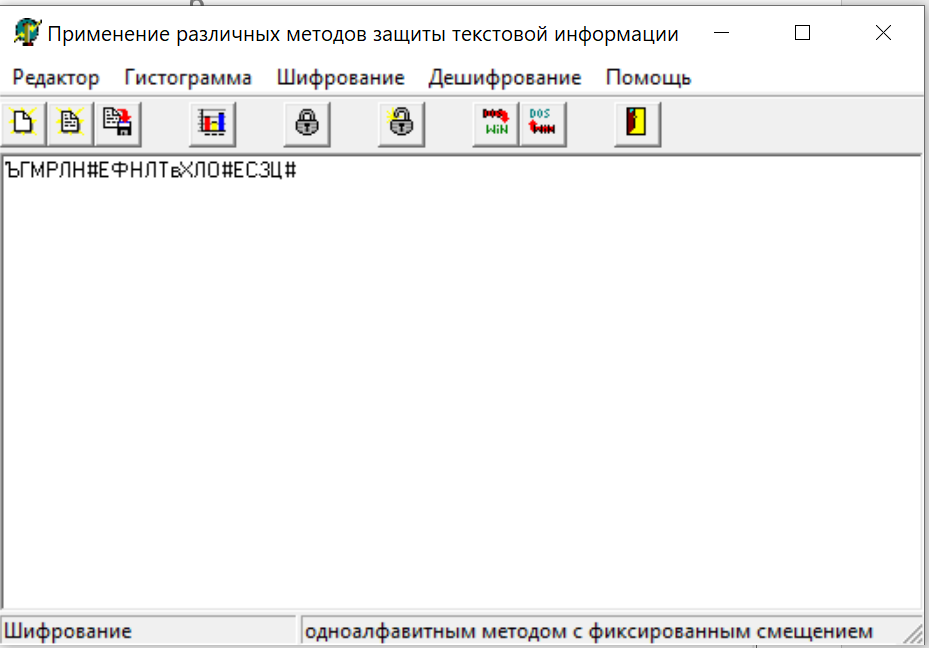


3 - Гистограммы

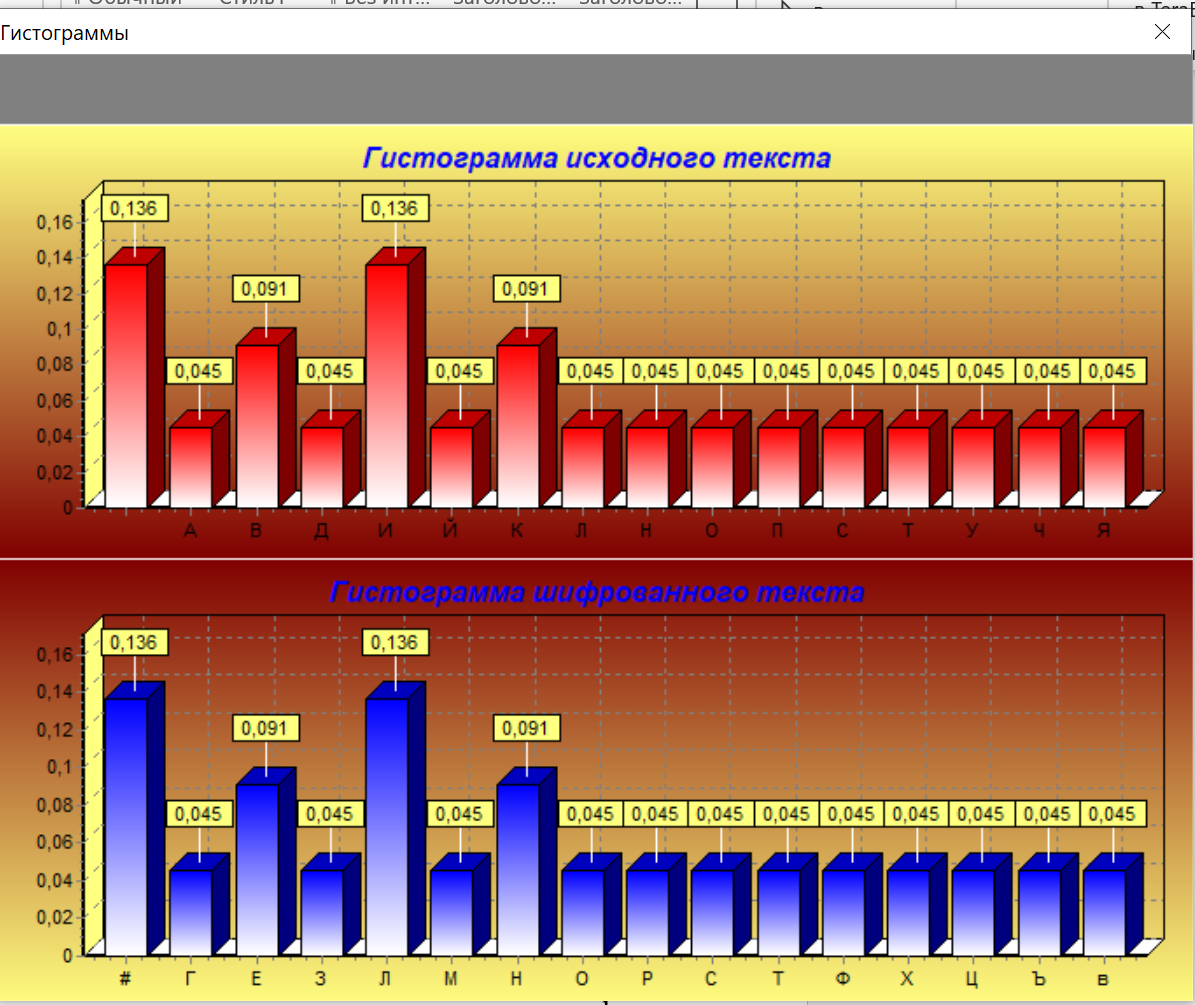
Эксперимент 3



1- Исходный текст



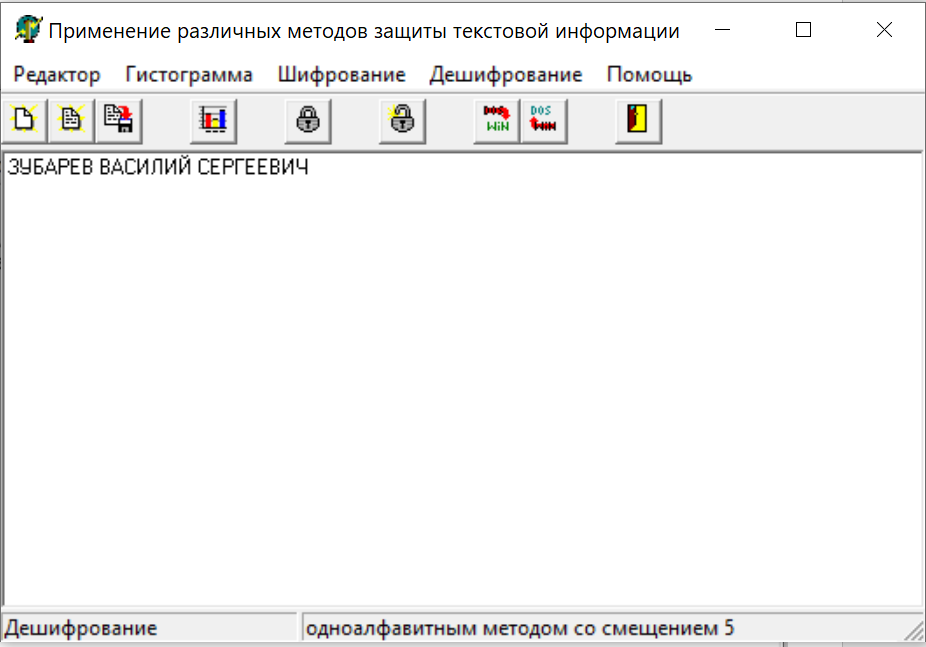
2 – зашифрованный текст



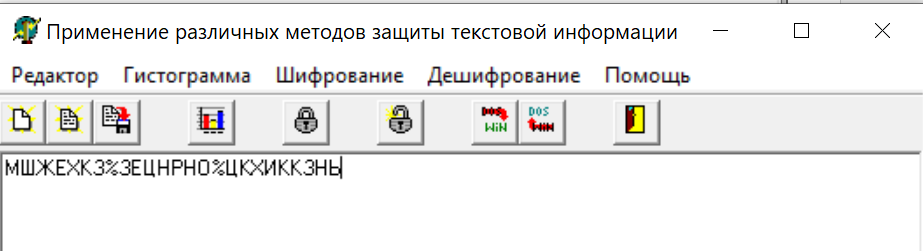
3 - Гистограммы

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

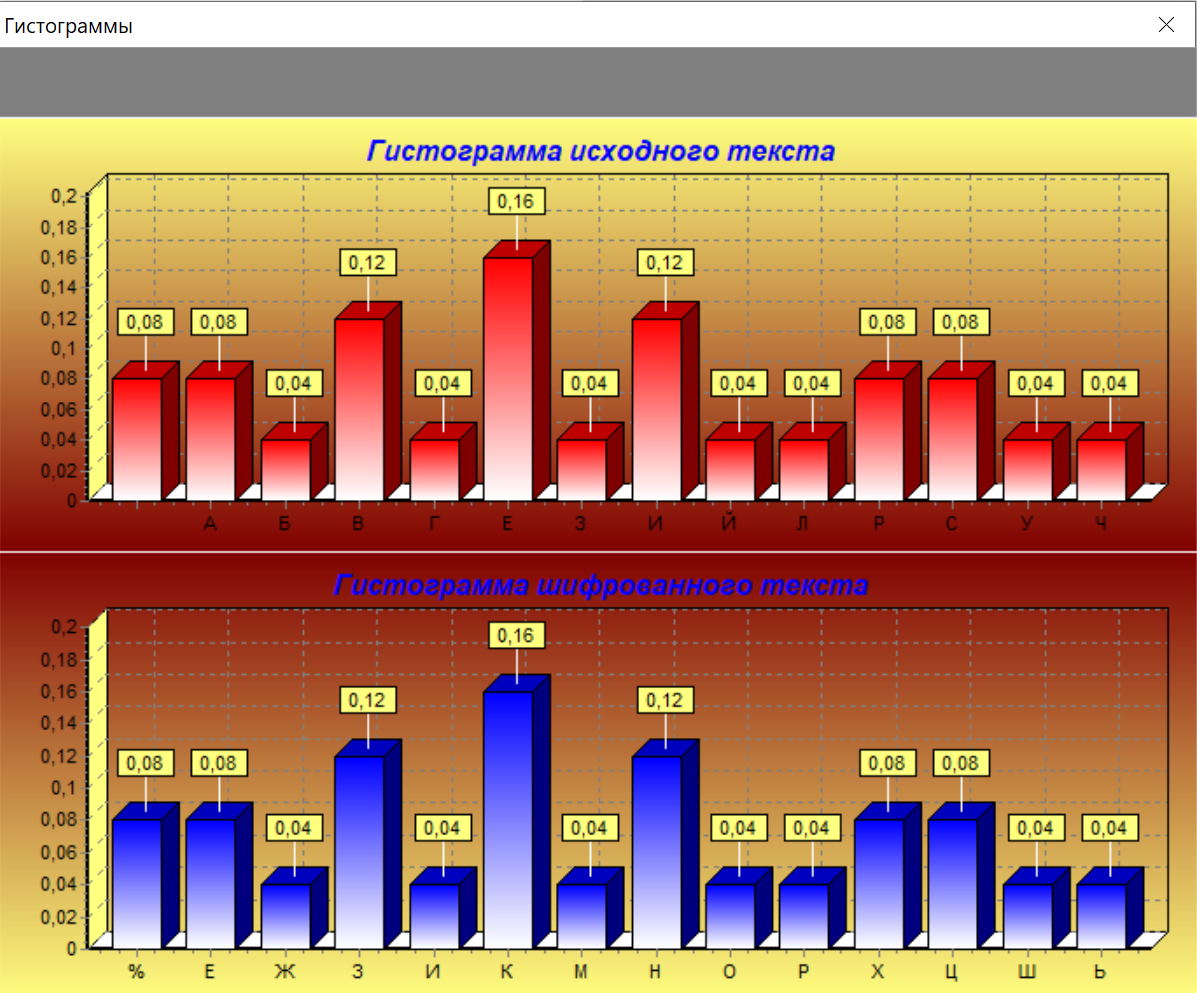
Эксперимент 1



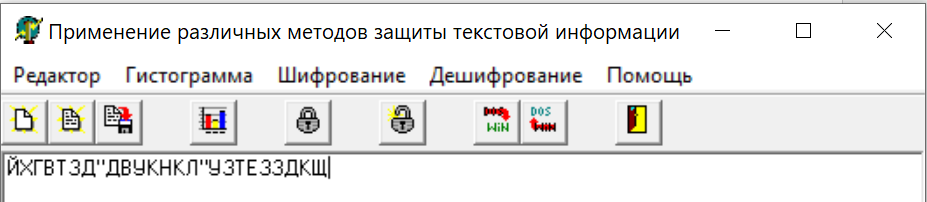
1- Исходный текст



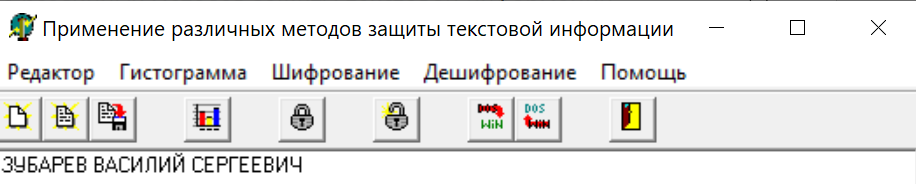
2 – Зашифрованный текст (смещение 5)



3 – Гистограммы

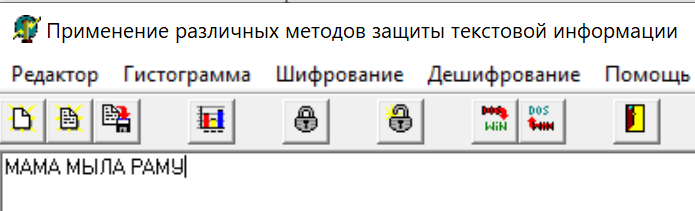


4 – Дешифрование подбором смещения (расшифровка со смещением 3)

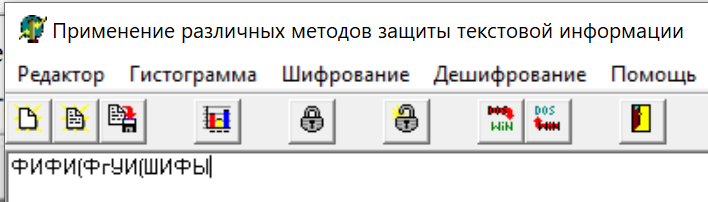


5 – Дешифрование подбором смещения (расшифровка со смещением 5)

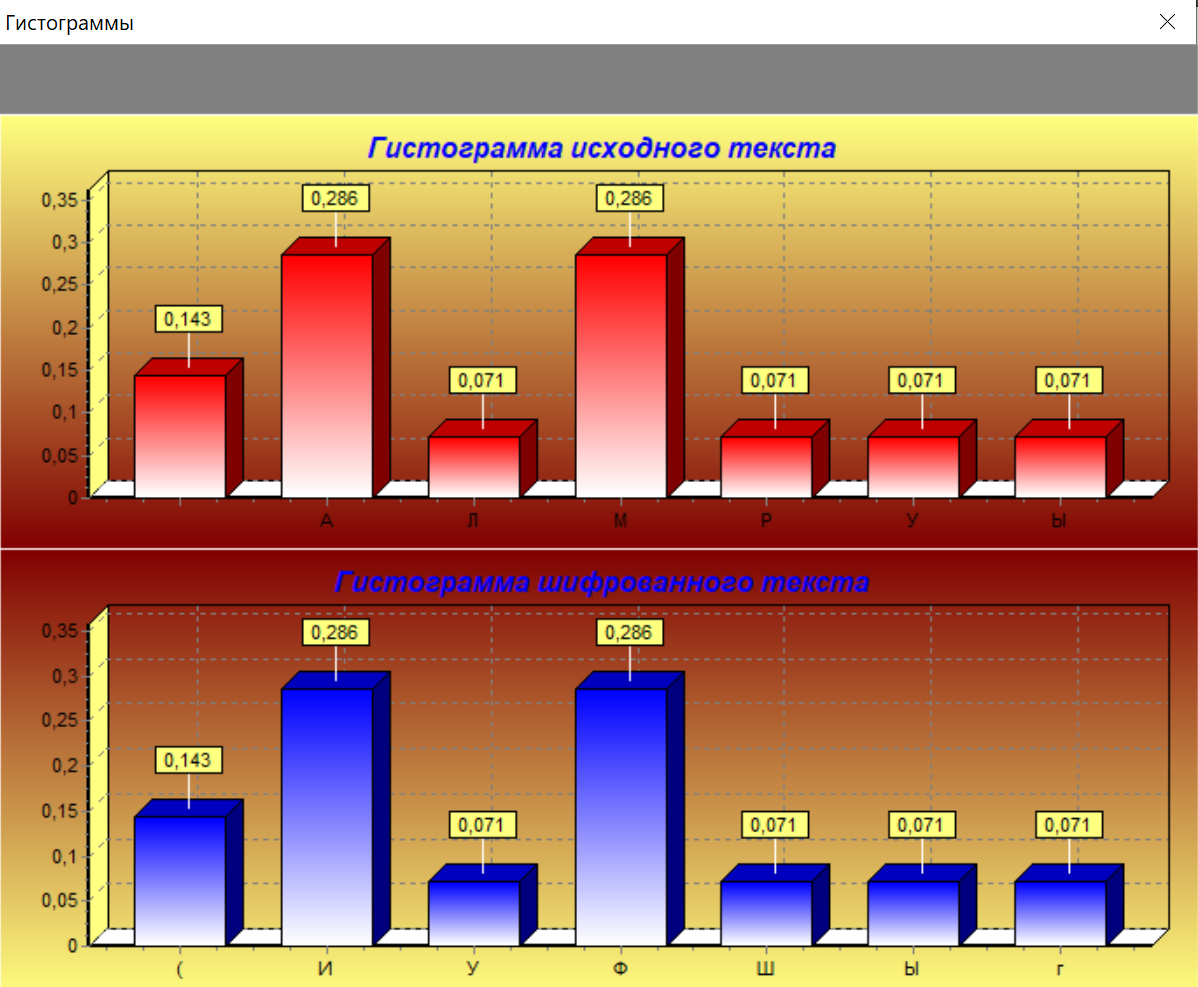
Эксперимент 2



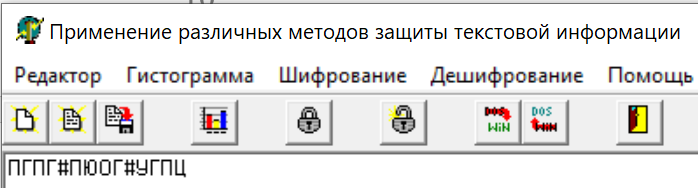
1- Исходный текст



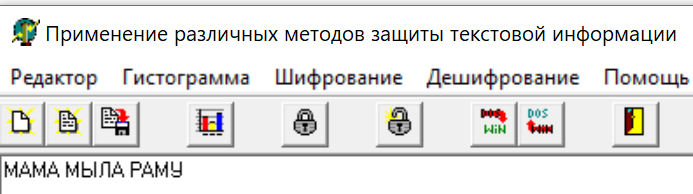
2 – Зашифрованный текст (смещение 8)



3 – Гистограммы

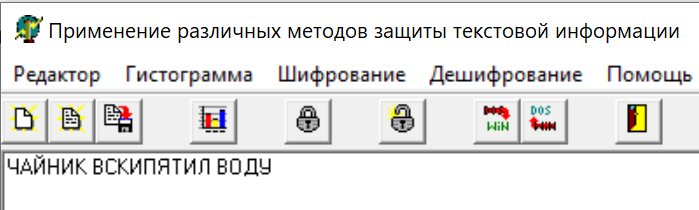


4 – Дешифрование подбором смещения (расшифровка со смещением 5)

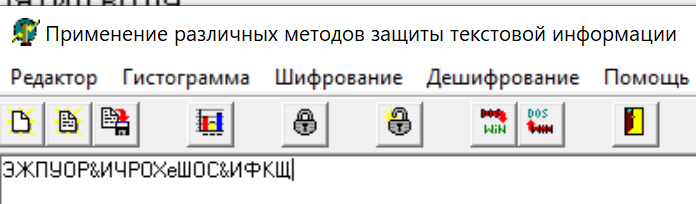


5 – Дешифрование подбором смещения (расшифровка со смещением 8)

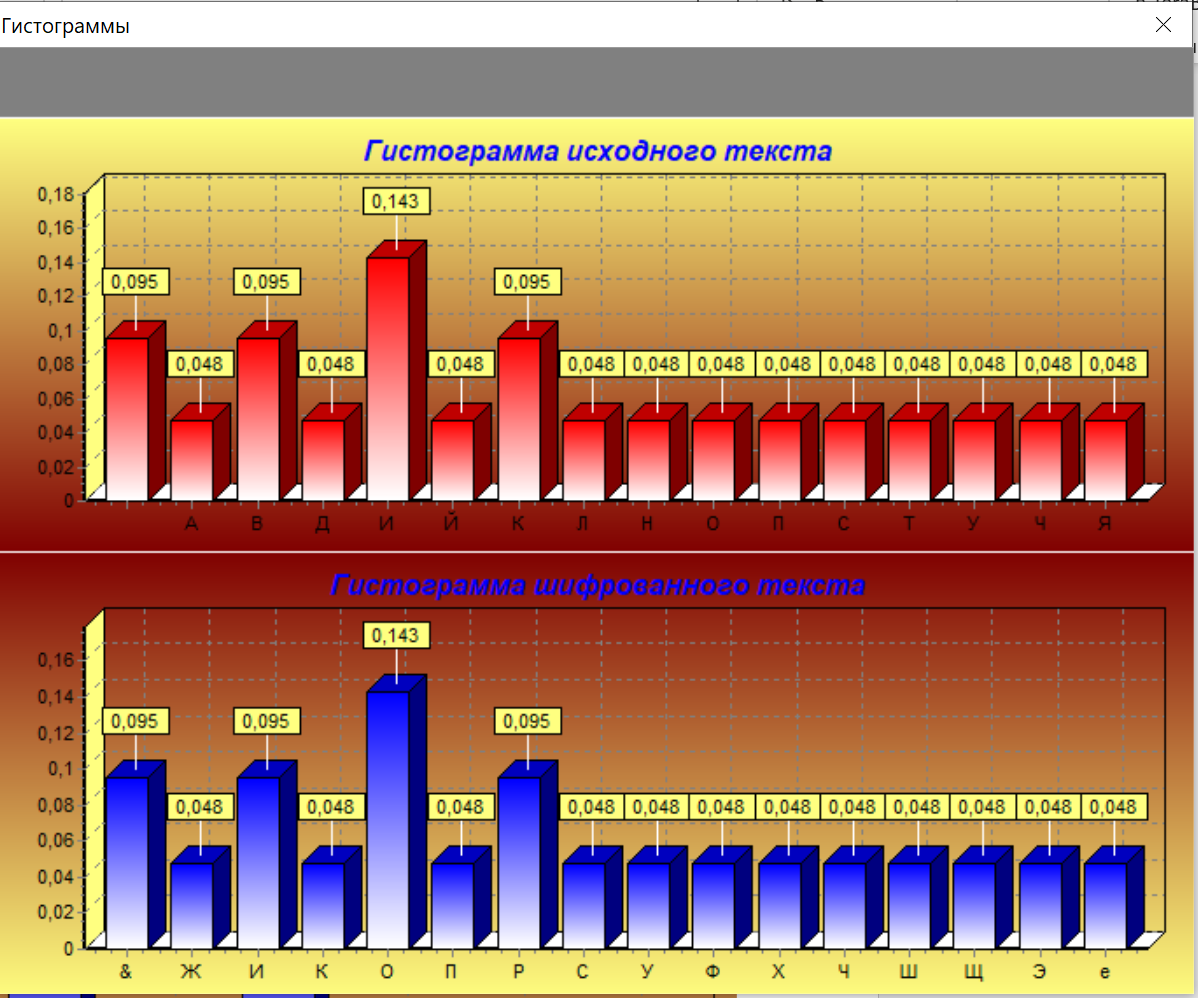
Эксперимент 3



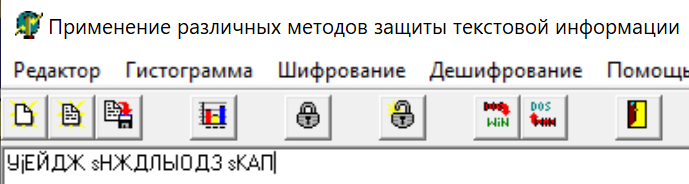
1- Исходный текст



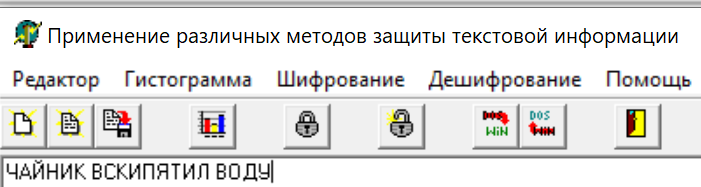
2 – Зашифрованный текст (смещение 6)



3 – Гистограммы



4 – Дешифрование подбором смещения (расшифровка со смещением 10)



5 – Дешифрование подбором смещения (расшифровка со смещением 6)

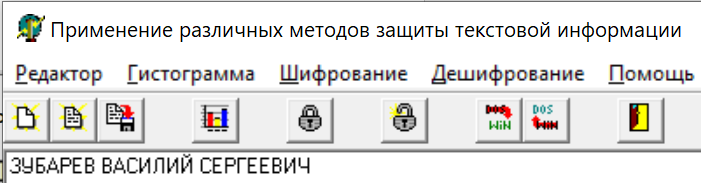
4. Для метода перестановки символов дешифровать зашифрованный файл.

ЗУБАРЕВ ВАСИЛИЙ СЕРГЕЕВИЧ

БУЗЕРАВ ВИСАЙИЛЕС ЕГРИВЕ Ч

БУЗЕРАВ ВИСАЙИЛЕС ЕГРИВЕ Ч

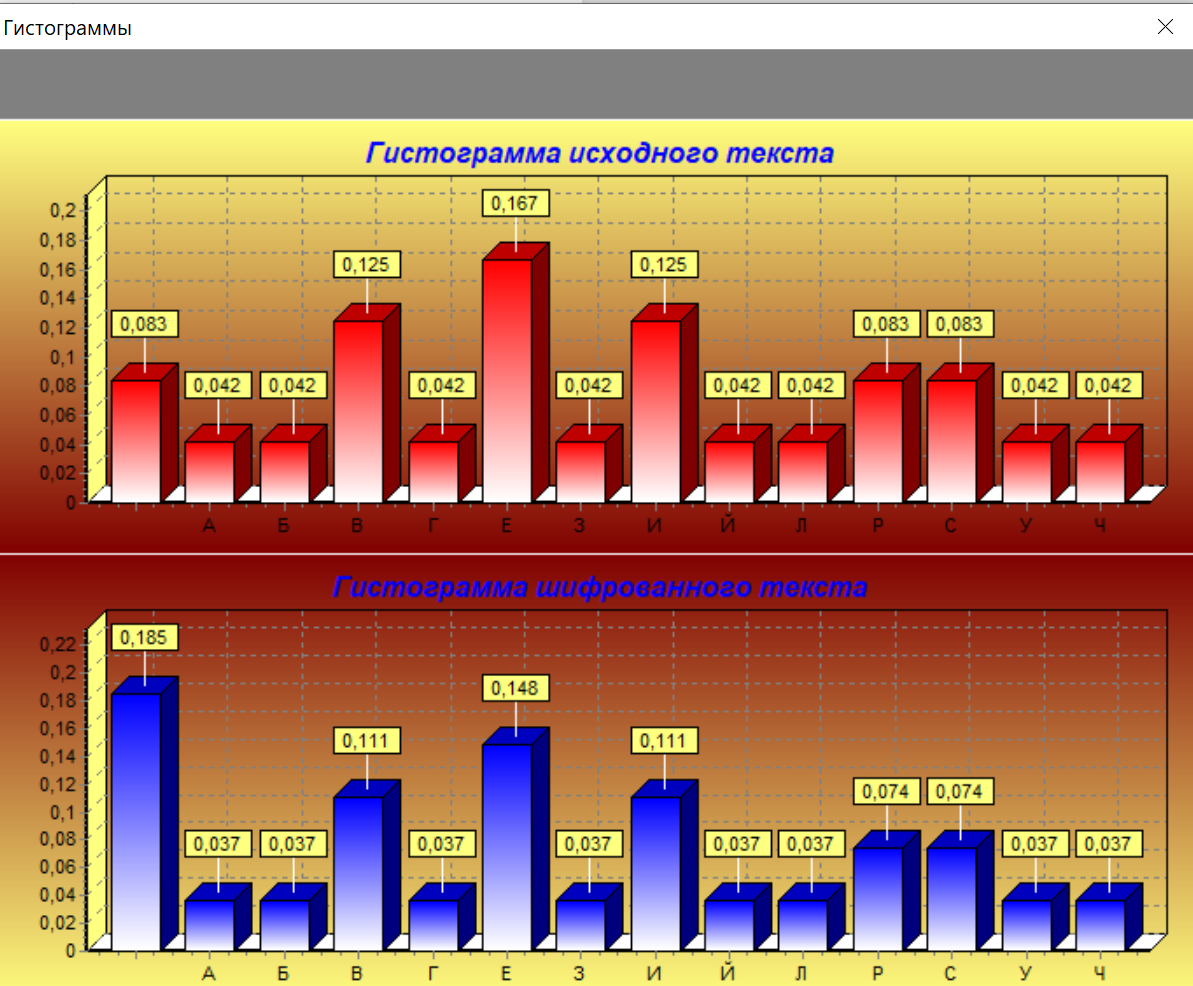
Эксперимент 1



1- Исходный текст



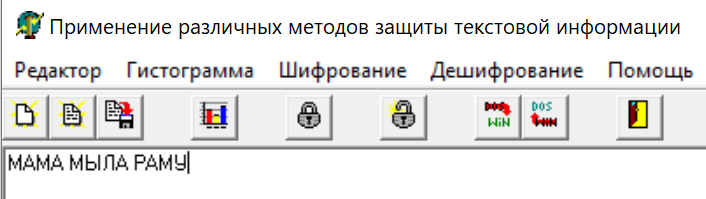
2 – Зашифрованный текст (ключ 321)



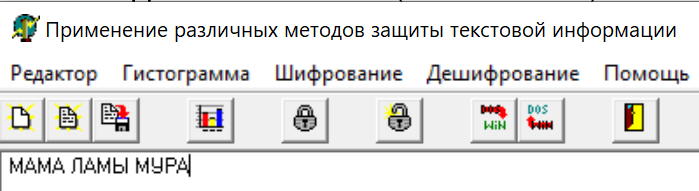
3 – Гистограммы (полезную информацию извлечь нельзя)

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)

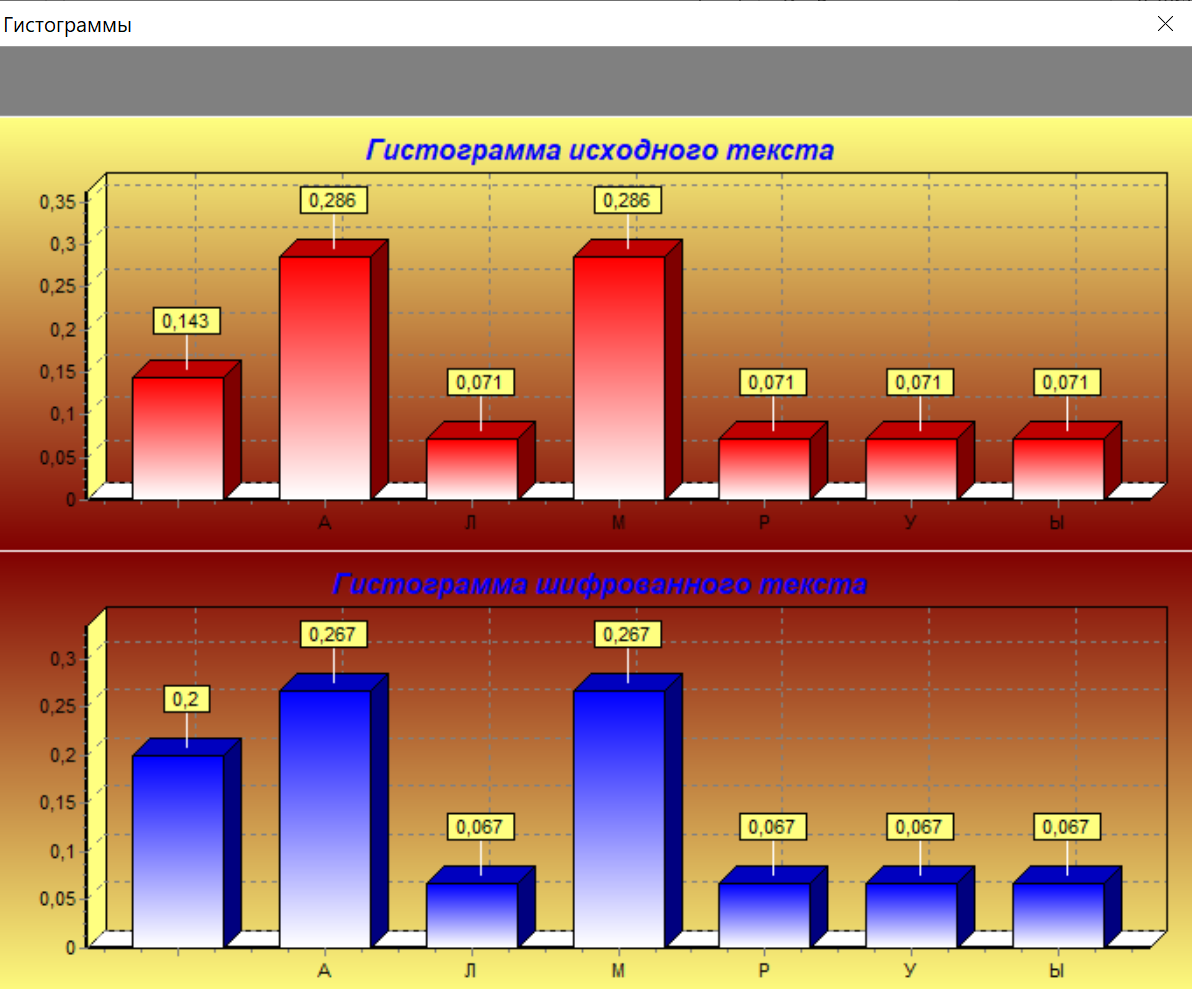
Эксперимент 2



1- Исходный текст

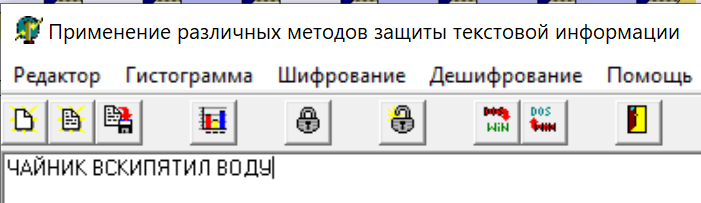


2 – Зашифрованный текст (ключ 53412)

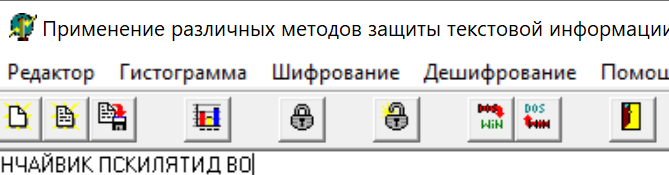


3 – Гистограммы (полезную информацию извлечь нельзя)

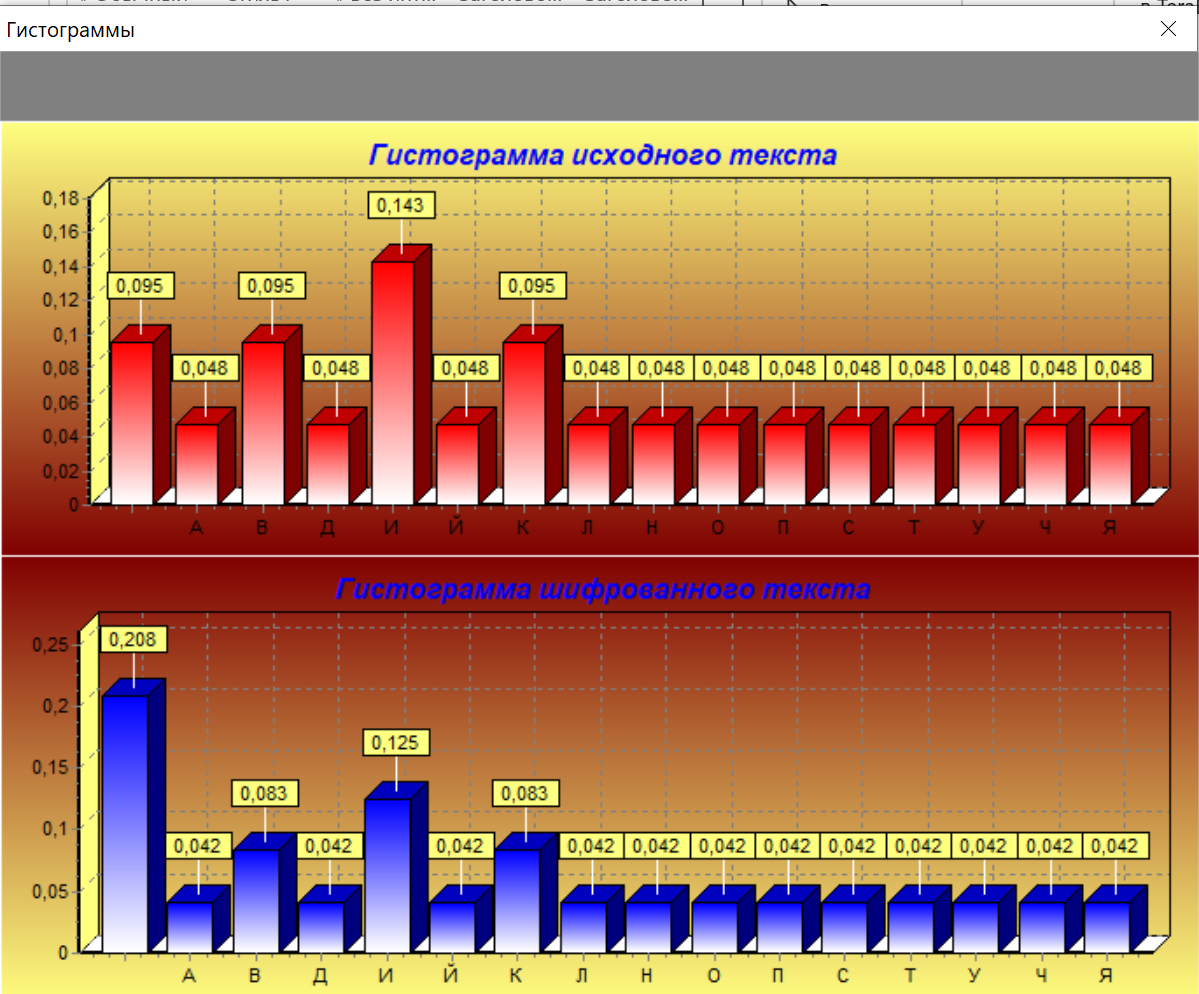
Эксперимент 3



1- Исходный текст



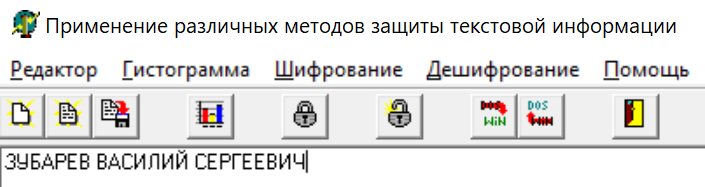
2 – Зашифрованный текст (ключ 2341)



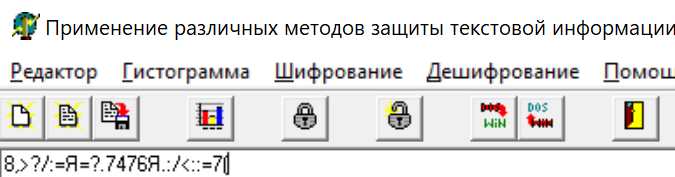
3 – Гистограммы (полезную информацию извлечь нельзя)

5. Для инверсного кодирования (по дополнению до 255)

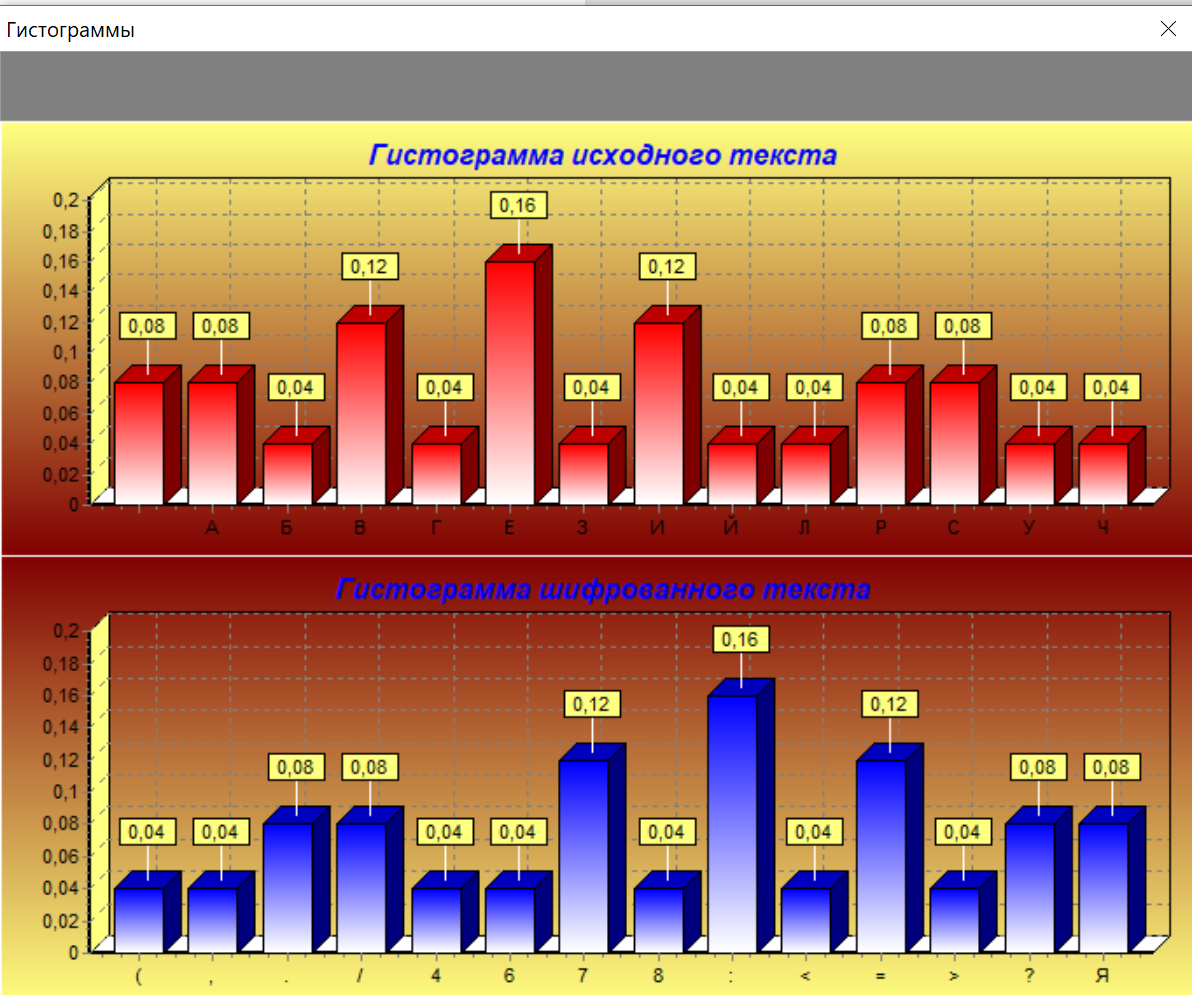
Эксперимент 1



1- Исходный текст



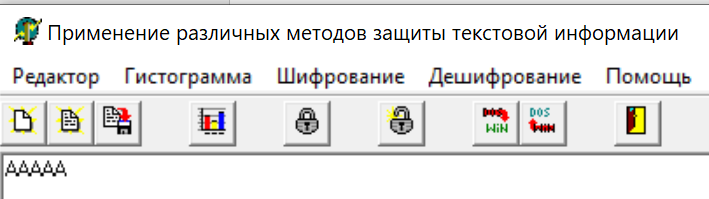
2 – Зашифрованный текст (ключ 2341)



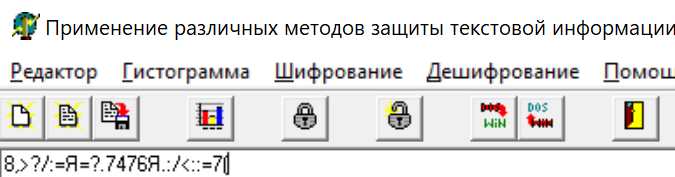
3 – Гистограммы Тш=N-T0 (на примере 58=255-197)

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

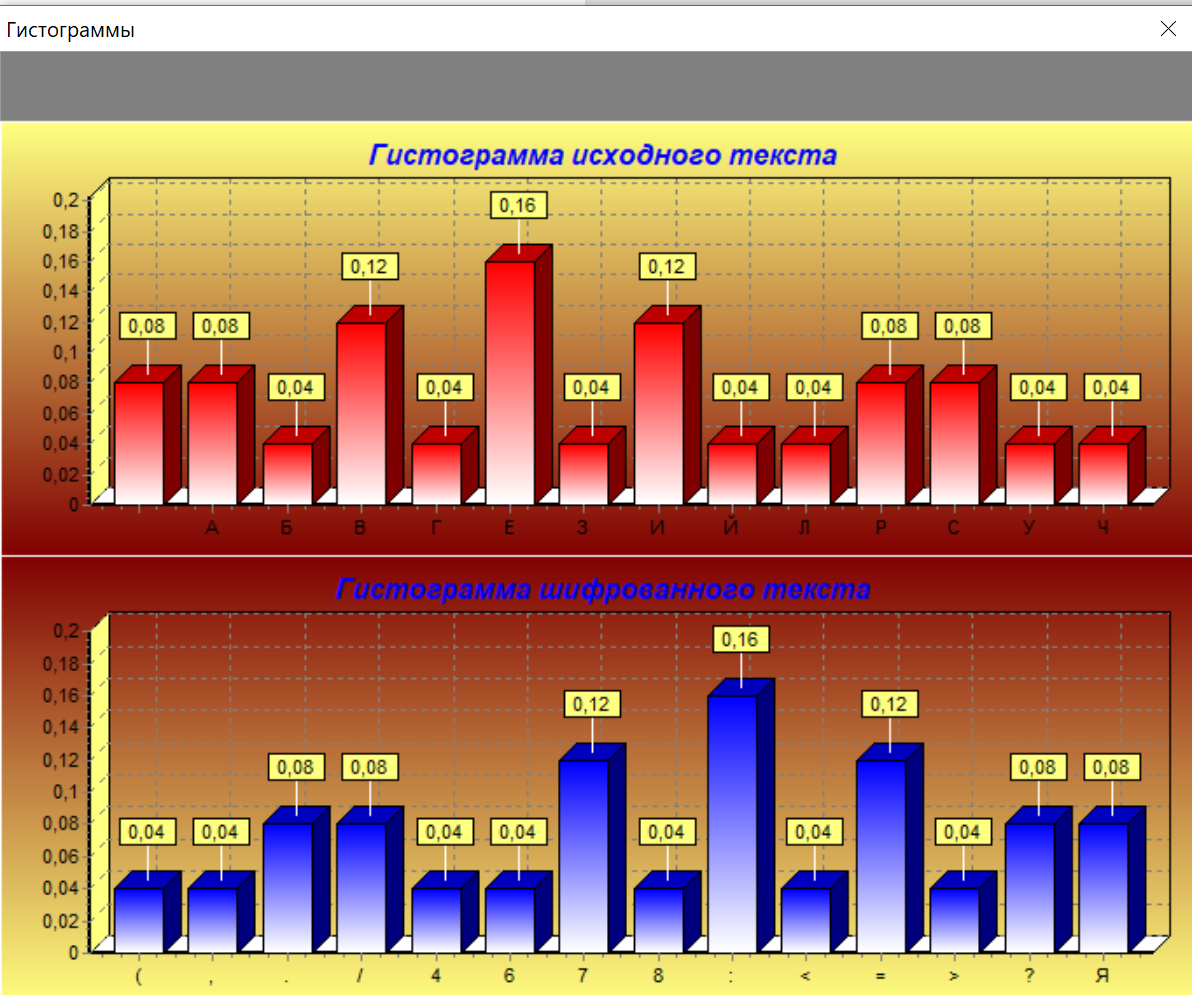
Эксперимент 2



1- Исходный текст



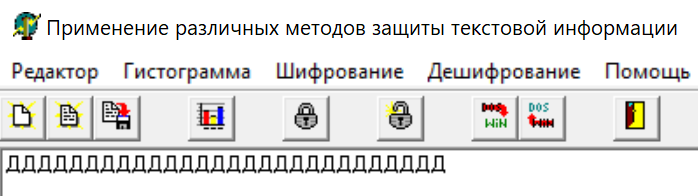
2 – Зашифрованный текст (ключ 2341)



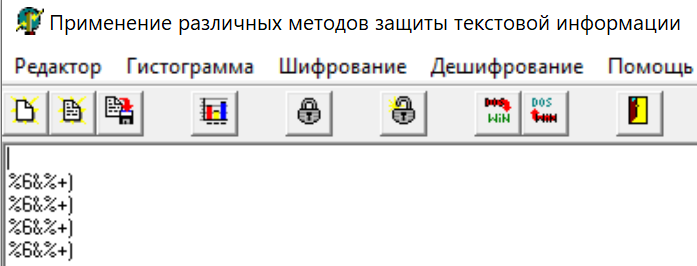
3 – Гистограммы Тш=N-T0 (на примере 58=255-197)

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

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 6 одно алфавитных шифров Цезаря со следующими смещениями:

К1=74

К2=97

К3=114

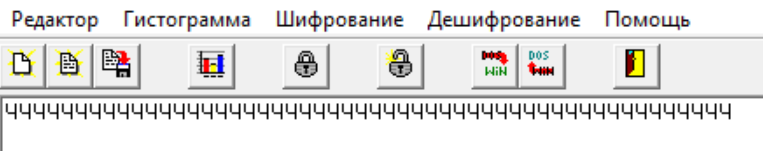
К4=98

К5=97

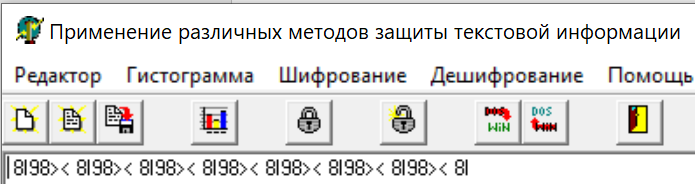
К6=103

К7=101

Эксперимент 2



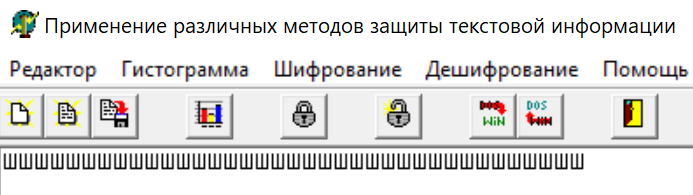
1- Исходный текст



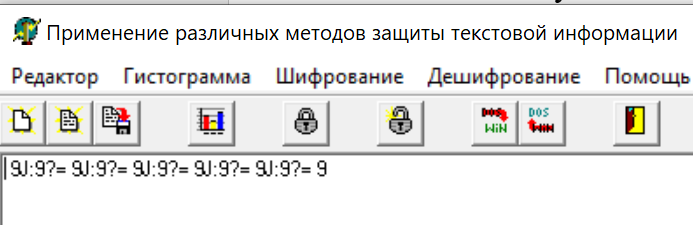
2 – Зашифрованный текст

Результаты подбора ключей аналогичны эксперименту 1

Эксперимент 3



1- Исходный текст

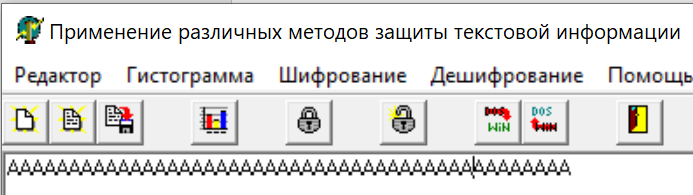


2 – Зашифрованный текст

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 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.

Эксперимент 1



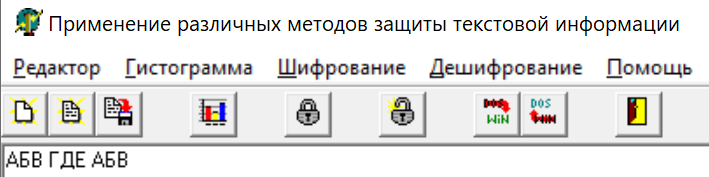
1- Исходный текст



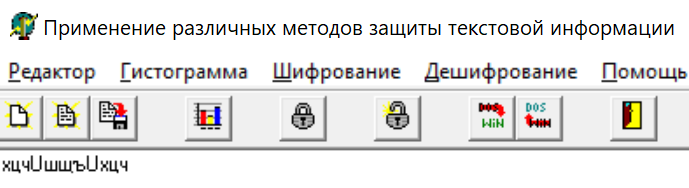
2 – Зашифрованный текст (длинна ключа 5)

К=31

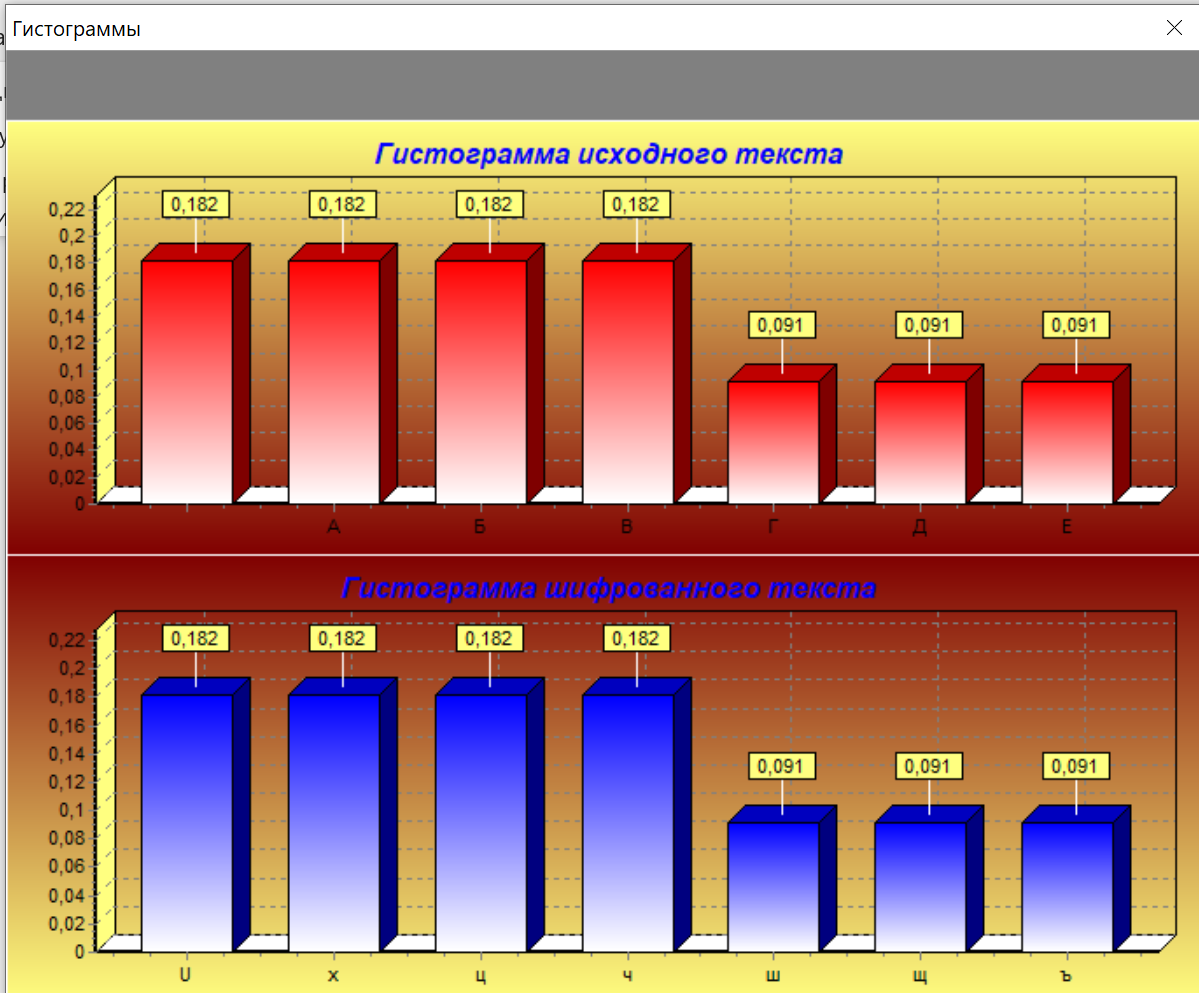
Эксперимент 2



1- Исходный текст



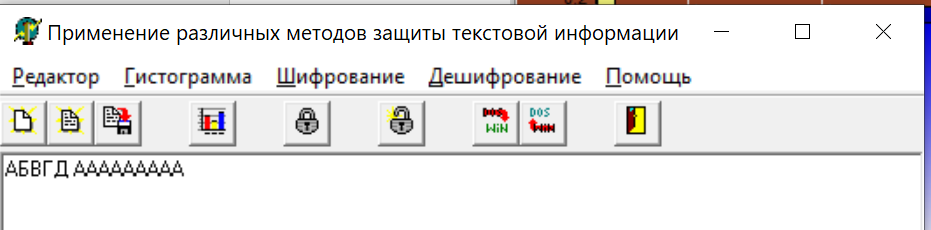
2 – Зашифрованный текст (длинна ключа 5)



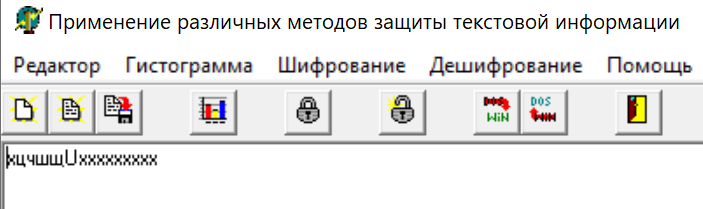
3 – Гистограмма (длинна ключа 5)

Заметим, что гистограмма открытого и шифро текста схожи по структуре, что свидетельствует о фиксированном сдвиге ключа. По таблице ASCII(1251) и исходя из гистограмм сдвиг равен 21

Эксперимент 3



1- Исходный текст



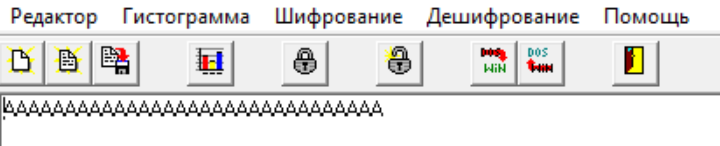
2 – Зашифрованный текст (длинна ключа 5)



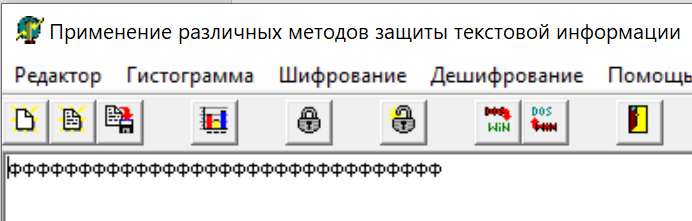
3 – Гистограмма (длинна ключа 5)

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

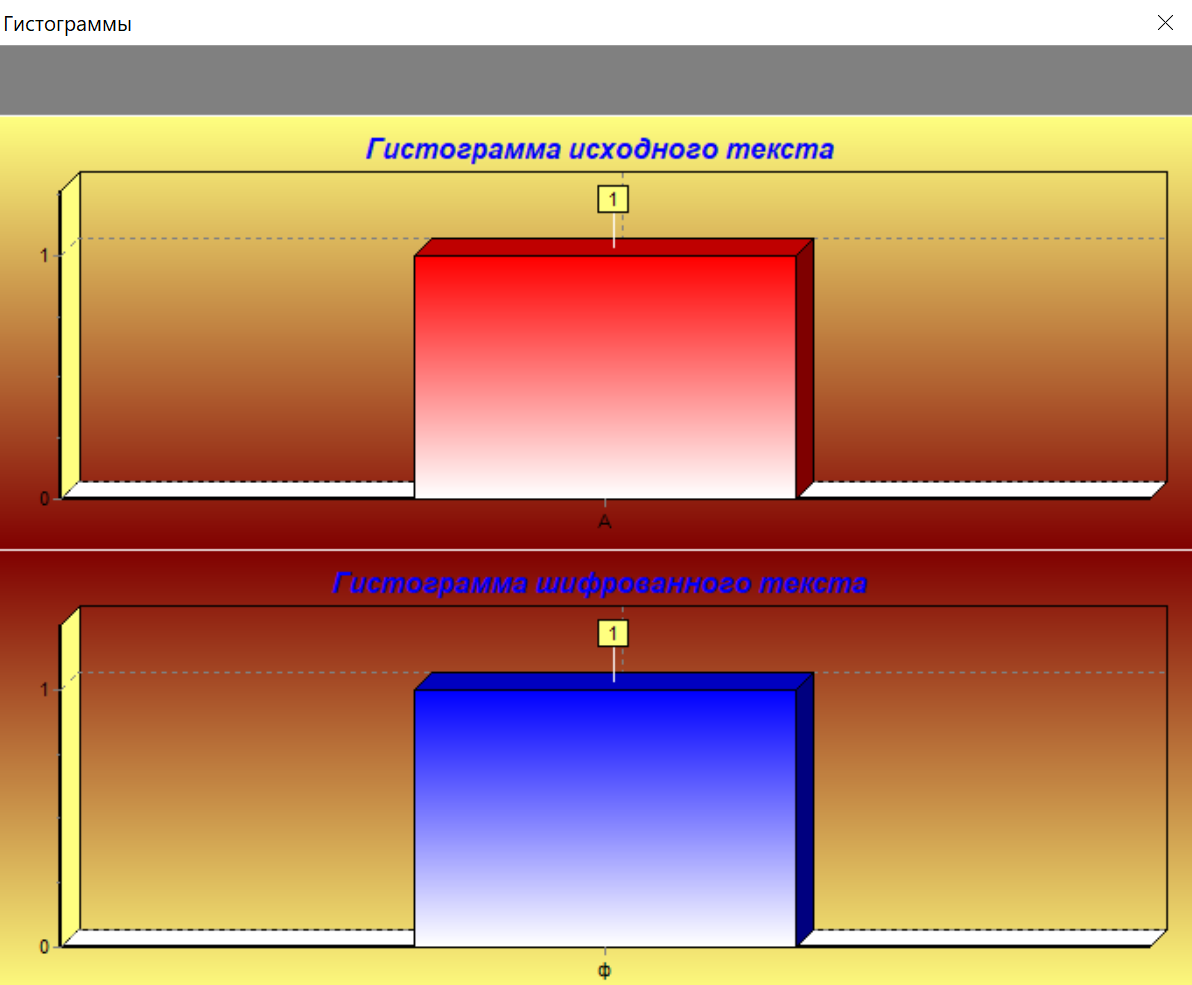
Эксперимент 1



1- Исходный текст



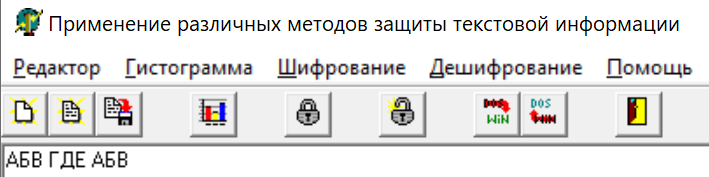
2 – Зашифрованный текст (длинна ключа 4)



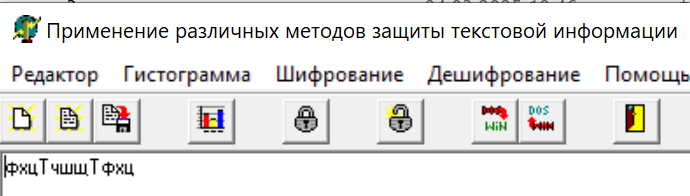
3 – Гистограмма (длинна ключа 4)

Из гистограммы видно, что сдвиг равен 20.

Эксперимент 2



1- Исходный текст



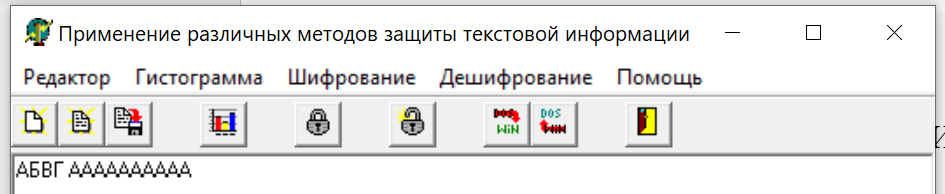
2 – Зашифрованный текст (длинна ключа 4)



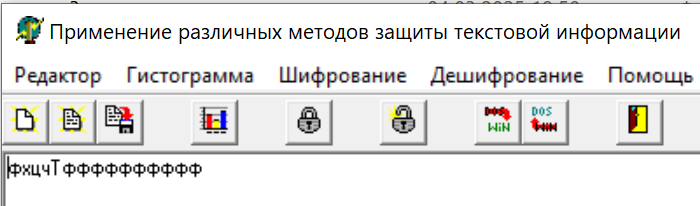
3 – Гистограмма (длинна ключа 4)

Заметим, что гистограмма открытого и шифро текста схожи по структуре, что свидетельствует о фиксированном сдвиге ключа. По таблице ASCII(1251) и исходя из гистограмм сдвиг равен 21

Эксперимент 3



1- Исходный текст



2 – Зашифрованный текст (длинна ключа 4)



3 – Гистограмма (длинна ключа 4)

Задание 9

Привести пример, когда рассматриваемые алгоритмы могут назваться абсолютно стойкими шифрами

Абсолютная стойкость шифра (в понимании К. Шеннона) означает, что **расшифровать сообщение невозможно, даже имея бесконечное количество зашифрованных текстов**. Такое возможно только если шифр удовлетворяет следующим условиям:

1. **Ключ абсолютно случаен**, то есть не имеет предсказуемых закономерностей.
2. **Ключ имеет такую же длину, как и сообщение** (одноразовый блокнот, **One-Time Pad, OTP**).
3. **Ключ используется только один раз**.

Рассмотрим каждый из перечисленных шифров с точки зрения возможности абсолютной стойкости.

**1. Алгоритм с фиксированным смещением**

**Суть**: Каждый символ заменяется на другой с фиксированным сдвигом.

**Нельзя сделать абсолютно стойким**

* Фиксированный сдвиг приводит к **циклическому распределению символов**.
* Если известен **хотя бы один фрагмент открытого текста**, легко найти сдвиг и расшифровать весь текст.
* Частотный анализ полностью ломает шифр.

**Вывод**: Не является абсолютно стойким, даже если использовать случайный фиксированный сдвиг.

**2. Алгоритм с задаваемым смещением**

**Суть**: Сдвиг может быть **разным**, но определяется по некоторому правилу (например, зависит от позиции символа или другого параметра).

**Нельзя сделать абсолютно стойким**

* Если **сдвиги предсказуемы**, можно восстановить их и дешифровать текст.
* Если используются ограниченные варианты сдвига, статистический анализ может вскрыть закономерность.

**Вывод**: Может усложнить анализ, но не дает абсолютной стойкости.

**3. Алгоритм перестановки**

**Суть**: Меняются **местами символы** в тексте, но сами символы остаются неизменными.

**Нельзя сделать абсолютно стойким**

* Восстановление текста возможно при анализе структуры (например, биграмм, триграмм).
* Если известна даже небольшая часть исходного текста, можно вычислить перестановку и расшифровать сообщение.
* Перестановка **не скрывает статистику символов** (частотный анализ эффективен).

**Вывод**: Не является абсолютно стойким.

**4. Алгоритм по дополнению до 255 (инверсный метод)**

**Суть**: Каждый символ заменяется на 255 - P\_i (инверсия кодов символов).

**Нельзя сделать абсолютно стойким**

* Преобразование **обратимо** и **однозначно предсказуемо**.
* Если известна хотя бы одна пара **открытый текст — шифротекст**, легко вычислить все остальные символы.

**Вывод**: совершенно не является стойким шифром.

**5. Многоалфавитный шифр с фиксированным ключом**

**Суть**: используется **фиксированный ключ** для сдвигов в многоалфавитном шифровании.

**Нельзя сделать абсолютно стойким**

* Если ключ **повторяется**, можно анализировать частоту символов и восстановить открытый текст.
* Можно использовать **методы взлома шифра Виженера** (индекс совпадений, анализ повторов).
* Даже если ключ длинный, он **конечный**, значит, текст можно анализировать по блокам.

**Вывод**: не является абсолютно стойким.

**6. Многоалфавитный шифр с ключом фиксированной длины**

**Суть**: Ключ имеет фиксированную длину, но может быть любым (например, Виженер с ключом длины 10).

**Нельзя сделать абсолютно стойким**

* Как и в предыдущем случае, если **ключ короче текста**, он **повторяется**, что открывает уязвимости.
* При длинных текстах можно обнаружить **структурные закономерности**.
* Можно применять **методы анализа периодичности ключа**.

**Вывод**: Длина ключа улучшает стойкость, но не делает шифр абсолютно стойким.

**7. Многоалфавитный шифр с ключом задаваемой длины**

**Суть**: Ключ может быть любой длины, включая длину всего сообщения.

**Можно сделать абсолютно стойким, если:**

* Ключ **случаен**.
* Ключ **такой же длины, как и текст**.
* Ключ **используется только один раз**.

**Вывод**:  
**Единственный абсолютно стойкий шифр — это одноразовый блокнот (OTP), где ключ равен по длине сообщению и используется только один раз.** Все остальные шифры имеют уязвимости.