Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Лабораторная работа №6

**ИЗУЧЕНИЕ УСТРОЙСТВА И ФУНКЦИОНАЛЬНЫХ ОСОБЕННОСТЕЙ ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**

Студент: Сосновец М.И.

ФИТ 3 курс 4 группа

Преподаватель: Нистюк О.А.

Минск 2025

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров (работа рассчитана на 4 часа аудиторных занятий).

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочно-перестановочных шифров.
2. Изучить структуру, принципы функционирования, реализацию процедур зашифрования сообщений в машинах семейства «Энигма».
3. Изучить и приобрести практические навыки выполнения криптопреобразований информации на платформе «Энигма», реализованной в виде симуляторов.
4. Получить практические навыки оценки криптостойкости подстановочных и перестановочных шифров на платформе «Энигма».
5. Результаты выполнения лабораторной работы оформить в виде отчета о проведенных исследованиях, методике выполнения практической части задания и оценке криптостойкости шифров.

**Теоретические сведения**

Машина «Энигма» – это электромеханическое устройство. Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем. Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу. Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

«Энигма» состоит из 5 основных блоков:

* панели механических клавиш 1 (дают сигнал поворота роторных дисков);
* трех (или более) роторных дисков 2, каждый имеет контакты по сторонам, по 26 на каждую, которые коммутируют в случайном порядке; по окружности нанесены буквы латинского алфавита либо числа;
* рефлектора 3 (имеет контакты с крайним слева ротором);
* коммутационной панели 4 (служит для того, чтобы дополнительно менять местами электрические соединения (контакты) двух букв);
* панели в виде электрических лампочек 5; индикационная панель с лампочками служит индикатором выходной буквы в процессе шифрования.

«Энигма» строится на основе подстановочных шифров, подобных шифру Цезаря, в котором, как известно, ключ сообщения, который должен знать получатель, – это просто смещение между двумя алфавитами. Принято считать, что в основе шифра «Энигмы» лежит динамический шифр Цезаря.

**Практическое задание**

Разработать приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Типы роторов (L – M – R) и отражателя Re следует выбрать из рис. 4.5 и 4.6 в соответствии со своим вариантом, представленным в таблице. Крайний правый столбец этой таблицы показывает, на какое число шагов (букв, i) перемещается соответствующий ротор при зашифровании одного (текущего) символа; число 0 означает перемещение соответствующего ротора на один шаг при условии, что расположенный правее ротор совершит один оборот.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вариант задания | L | M | R | Re | Li-Mi-Ri |
| 12 | III | Gamma | V | C Dunn | 1-1-2 |

С помощью разработанного приложения зашифровать сообщение в соответствии с п. 1 практического задания, применив не менее 5 вариантов начальных установок роторов. Оценить криптостойкость вашего варианта машины.

В данной лабораторной работе было разработано приложение-симулятор шифровальной машины, состоящей из клавиатуры, трех роторов и отражателя. Конфигурации роторов и отражателя представлены в листинге 1.1.

|  |
| --- |
| constructor() {      this.rotors = [        { wiring: "BDFHJLCPRTXVZNYEIWGAKMUSQO", notch: "V", position: 0 },        { wiring: "FSOKANUERHMBTIYCWLQPZXVGJD", notch: "E", position: 0 },        { wiring: "VZBRGITYUPSDNHLXAWMJQOFECK", notch: "Q", position: 0 }      ];      this.reflector = {        'A': 'R', 'B': 'D', 'C': 'O', 'E': 'J',        'F': 'N', 'G': 'T', 'H': 'K', 'I': 'V',        'L': 'M', 'P': 'W', 'Q': 'Z', 'S': 'X',        'U': 'Y', 'R': 'A', 'D': 'B', 'O': 'C',        'J': 'E', 'N': 'F', 'T': 'G', 'K': 'H',        'V': 'I', 'M': 'L', 'W': 'P', 'Z': 'Q',        'X': 'S', 'Y': 'U'      };    } |

Листинг 1.1 – Реализация конфигураций роторов и отражателя

Как можно заметить каждый ротор имеет: таблицу замен (wiring) — перестановка алфавита, позицию срабатывания (notch) — момент, когда следующий ротор сдвигается. Отражатель C Dunn реализован как объект, где каждая буква отображается в парную.

wiring - строка, определяющая перестановку алфавита:

* Для RotorIII: 4-я буква (H) заменяет D (исходная 4-я буква алфавита)
* Для GammaRotor: уникальная нелинейная перестановка
* Для RotorV: специальная перестановка с равномерным распределением

notch - контрольная точка вращения:

* RotorIII срабатывает на V (21-я буква)
* GammaRotor - на E (5-я буква)
* RotorV - на Q (16-я буква)

Логика работы состоит из:

1. Вращение роторов (реализация показана в листинге 1.2)

* Правый ротор (R) делает 2 шага.
* Средний (M) делает 1 шаг, когда правый завершает полный оборот.
* Левый (L) делает 1 шаг, когда средний завершает оборот.

|  |
| --- |
| rotateRotors() {  this.rotors[2].position = (this.rotors[2].position + 1) % 26;  if (this.rotors[2].position === "ABCDEFGHIJKLMNOPQRSTUVWXYZ".indexOf(this.rotors[2].notch)) {        this.rotors[1].position = (this.rotors[1].position + 1) % 26;          if (this.rotors[1].position === "ABCDEFGHIJKLMNOPQRSTUVWXYZ".indexOf(this.rotors[1].notch)) {          this.rotors[0].position = (this.rotors[0].position + 1) % 26;        }}} |

Листинг 1.2 – Реализация вращения роторов

1. Шифрование символов (реализация показана в листинге 1.3)

* Прямой проход (клавиатура → роторы → отражатель)
* Обратный проход (отражатель → роторы → лампочки).

|  |
| --- |
| encryptText(text) {      let result = '';      for (const c of text.toUpperCase()) {        result += this.encryptChar(c);      }return result;  } |

Листинг 1.3 – Реализация шифрования символов

Тесты проводились в пяти разных начальных положениях роторов. Тестовыми данными были фамилия имя отчество. Результат тестов представлен на рисунке 1.1.

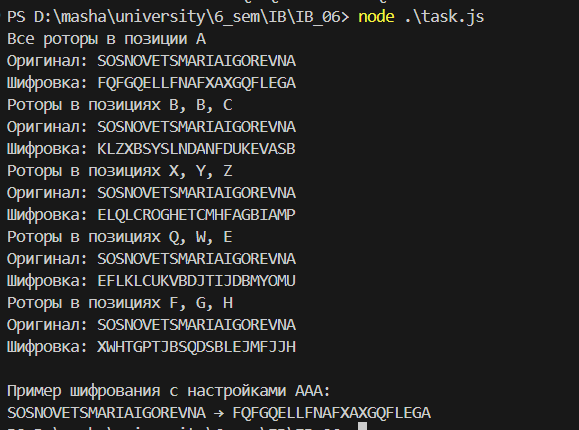
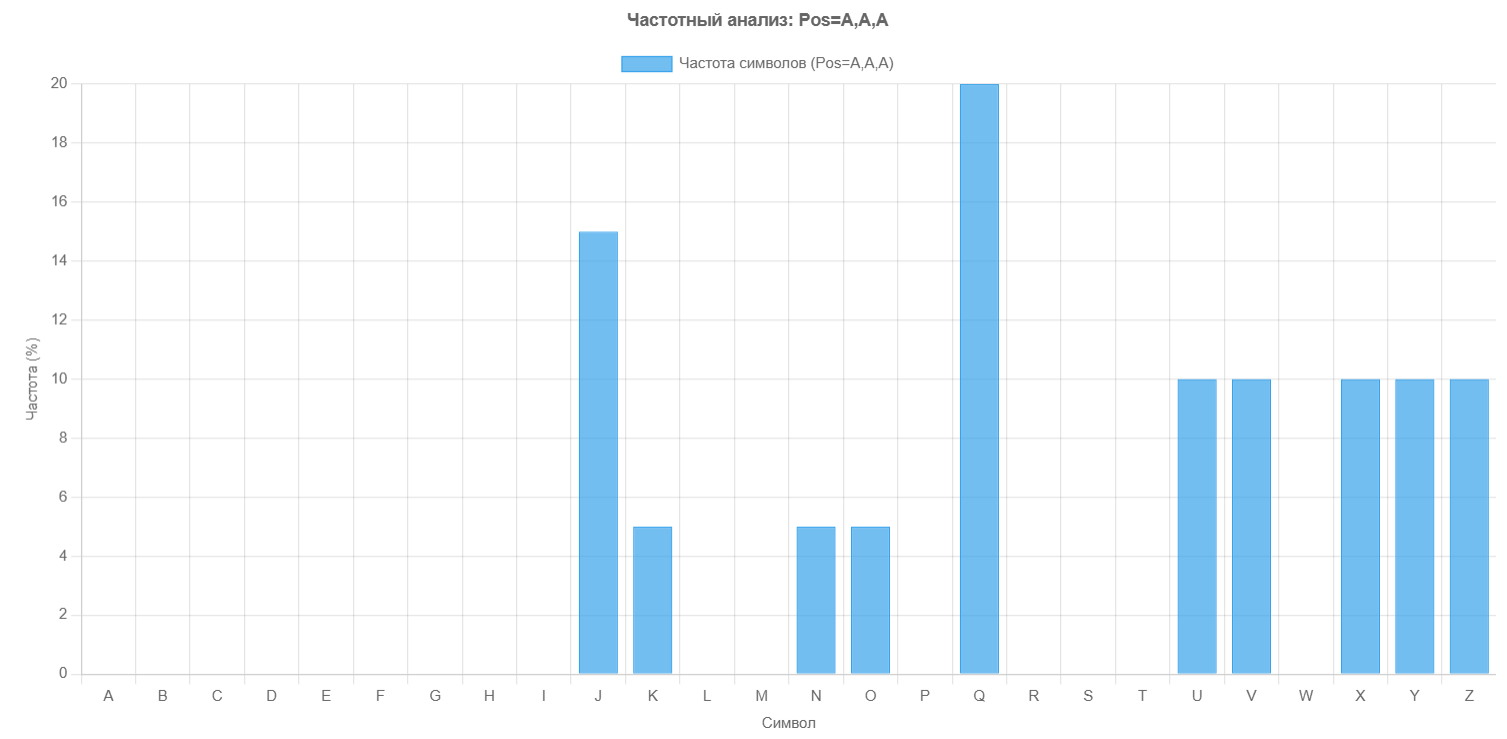
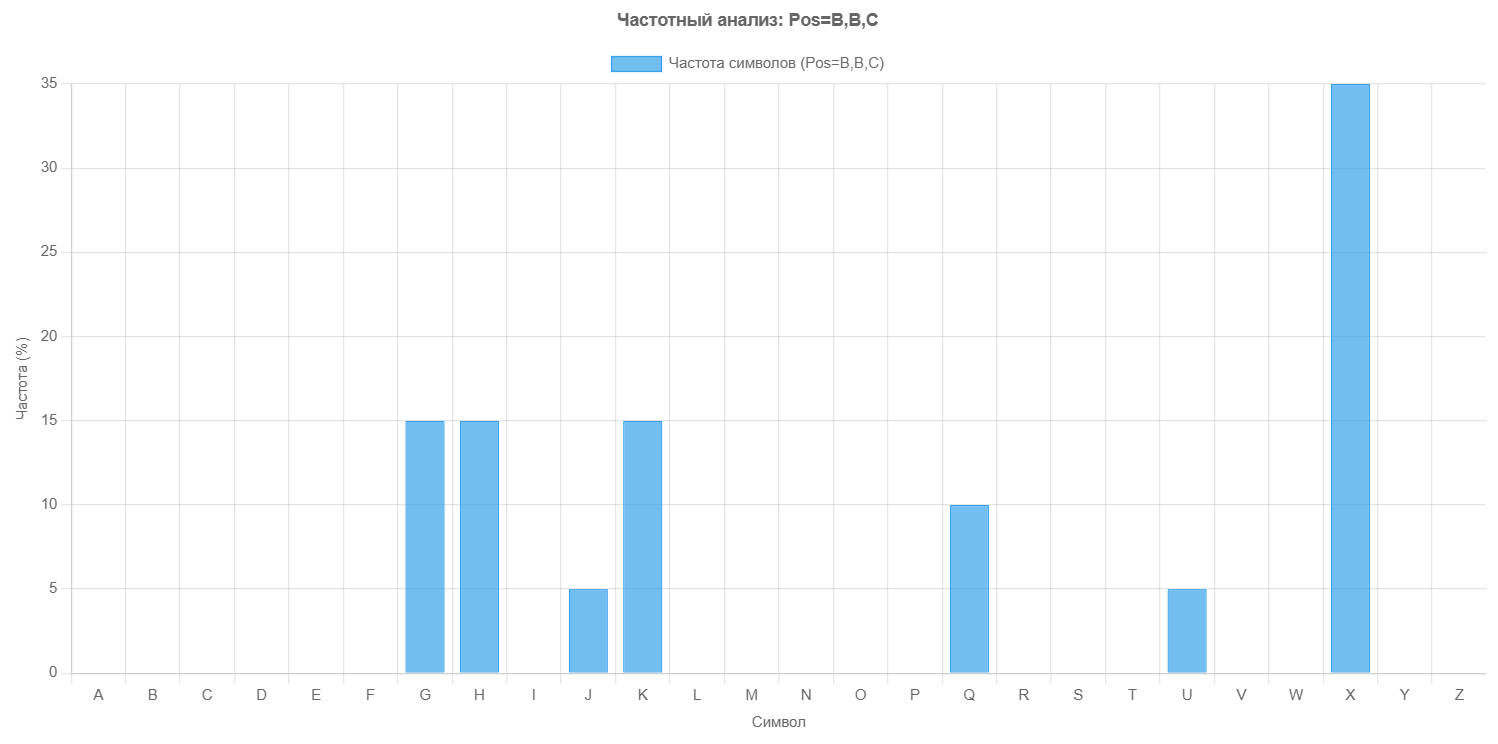
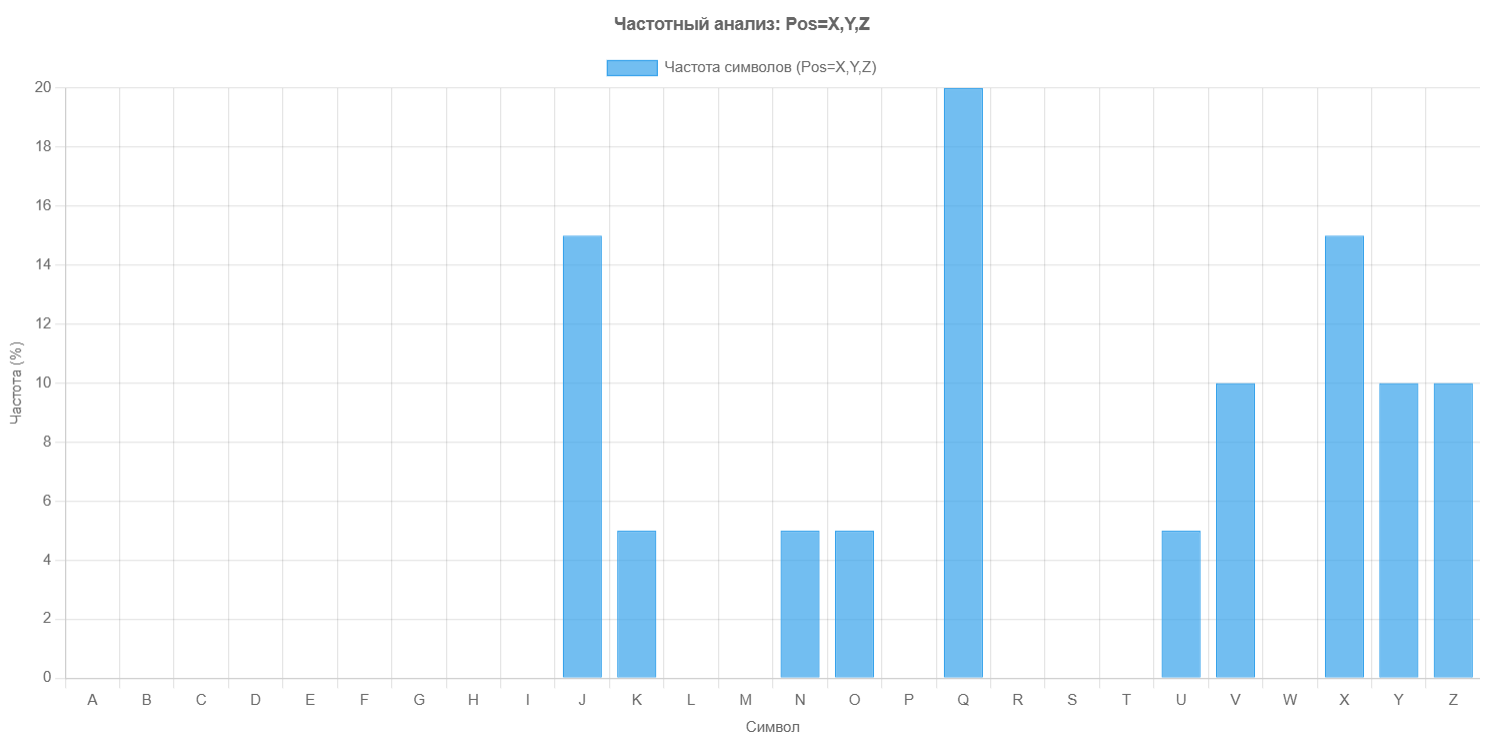


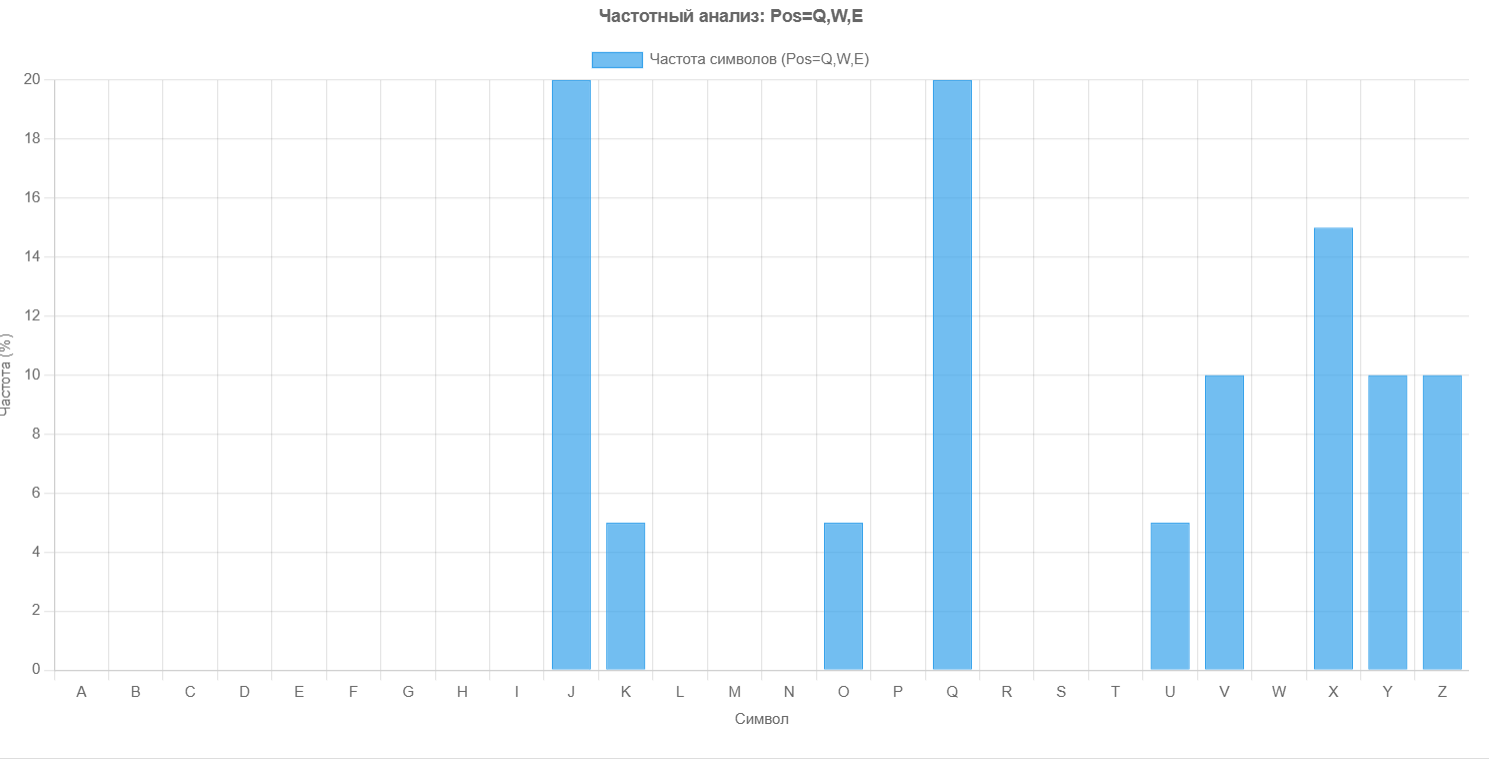
Рисунок 1.1 – Результат тестов

Оценка частотных свойств символов в шифртекстах и сравнить этот параметр с частотными свойствами символов для исходного текста.









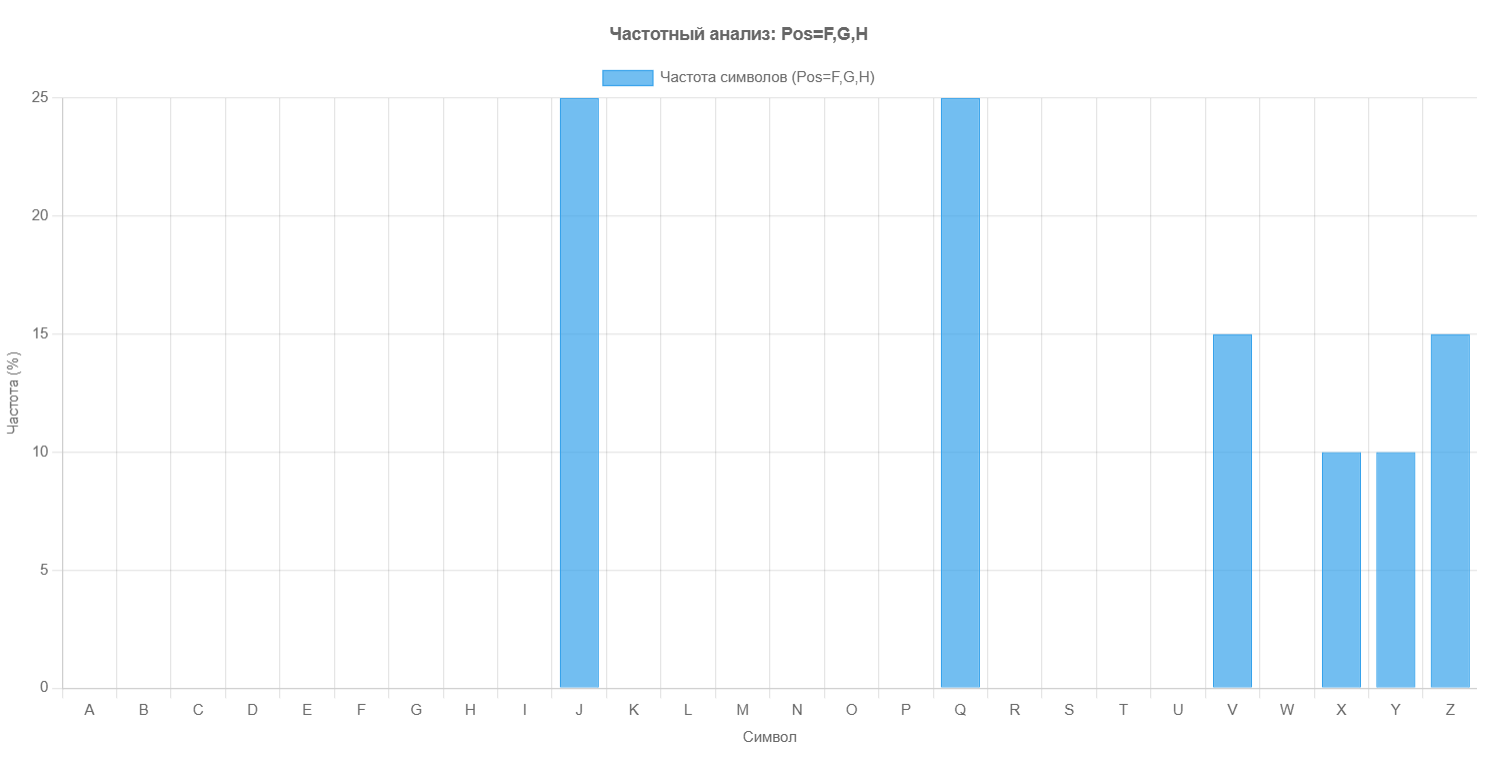


Рисунок 1.2 – Результат оценки

Оценка криптостойкости машины.

1. Расчет количества возможных ключей

Для симулятора с тремя роторами (III, Gamma, V) и отражателем C Dunn пространство ключей определяется следующими параметрами:

* Каждый из 3 роторов может находиться в одной из 26 стартовых позиций (A-Z)
* Роторы можно переставлять местами в 3! = 6 различных комбинациях

Таким образом, общее количество возможных ключей вычисляется по формуле:  
Ek = 26³ × 3! = 17,576 × 6 = 105,456 вариантов

1. Оценка времени взлома перебором

При различных методах атаки время взлома будет существенно отличаться:

Ручной перебор:

* Скорость: 1 вариант в минуту
* Общее время: 105,456 минут = 1,758 часов ≈ 73 дня

При 105,456 возможных комбинациях начальных настроек (26³ позиций × 6 перестановок роторов) симулятор обладает недостаточной стойкостью для практического применения.

26 \* 26 \* 26 =17576 комбинаций

5 \* 4 \* 3 = 60 кол-во перестановок

26 \* 26 = 676 нач. положение роторов

17576\*60\*676\*13! = 4439134529077248000

**Вывод:**

В данной лабораторной работе мной были изучены и приобретены практических навыков разработки и использования симулятора шифровальной машинки «Энигма». В рамках были разработаны три компонента для симулятора. Был проведён анализ криптостойкости симулятора.