МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по дисциплине «Криптографические методы защиты информации»

к практической работе на тему:

**ЭЛЕМЕНТЫ ТЕОРИИ ИНФОРМАЦИИ. ПАРАМЕТРЫ И ХАРАКТЕРИСТИКИ ДИСКРЕТНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ**

Выполнил:

студент III курса 8 группы

специальности ПОИБМС

Астровская Д.А.

Проверил:

Берников Владислав Олегович

Минск 2022

**Лабораторная работа 2**

**Элементы теории информации. Параметры и характеристики дискретных информационных систем**

**Цель работы**: приобретение практических навыков расчета и анализа параметров и информативных характеристик дискретных ИС

**Задачи:**

- Закрепить теоретические знания по основам теории информации.

- Разработать приложение для расчета и анализа параметров и информативных характеристик дискретных ИС.

- Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Практическое задание**

Создать приложение для расчета и анализа параметров и информативных характеристик дискретных ИС, с помощью которого:

- рассчитать энтропию указанных преподавателем алфавитов: один – на латинице, другой – на кириллице (по формуле (2.1) перейти от частоты появления каждого символа алфавита к соответствующей вероятности); в качестве входного может быть принят произвольный электронный текстовый документ на основе соответствующего алфавита; частоты появления символов алфавитов оформить в виде гистограмм.

*def self.shannon\_entropy(message)*

*result = 0.00*

*len = message.length*

*hash = letters\_count(message)*

*hash.each do |key, value|*

*frequency = value.to\_f / len*

*result -= frequency \* Math.log(frequency, 2)*

*end*

*result*

*end*

Листинг.1 - Функция нахождения энтропии

- для входных документов, представленных в бинарных кодах, определить энтропию бинарного алфавита;

*bin\_file = File.new("bin.bin","w+")*

*bin\_file.puts(ge\_text.unpack('b\*'))*

*bin\_file.close*

Листинг.2 - Скрипт создания бинарного файла на основе текстового файла

- используя значения энтропии алфавитов, полученных в пунктах (а) и (б), подсчитать количество информации в сообщении, состоящем из собственных фамилии, имени и отчества (на основе исходного алфавита – (а) и в кодах ASCII – (б)); объяснить полученный результат;

*def self.information\_amount(message)*

*shannon\_entropy(message).to\_f \* message.length*

*end*

*def self.information\_amount\_ascii(message)*

*message.length \* 8*

*end*

Листинг.3 - Функции для подсчета кол-ва информации в сообщении

- выполнить задание пункта (в) при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0,1; 0,5; 1,0

*def self.information\_amount\_w\_mistake(message, error)*

*shannon\_entropy(message) - (-(1 - error)) \* Math.log((1 - error), 2) - error \* Math.log(error, 2) \* message.length*

*end*

Листинг.4 - Функция для подсчета информации в сообщении с ошибками

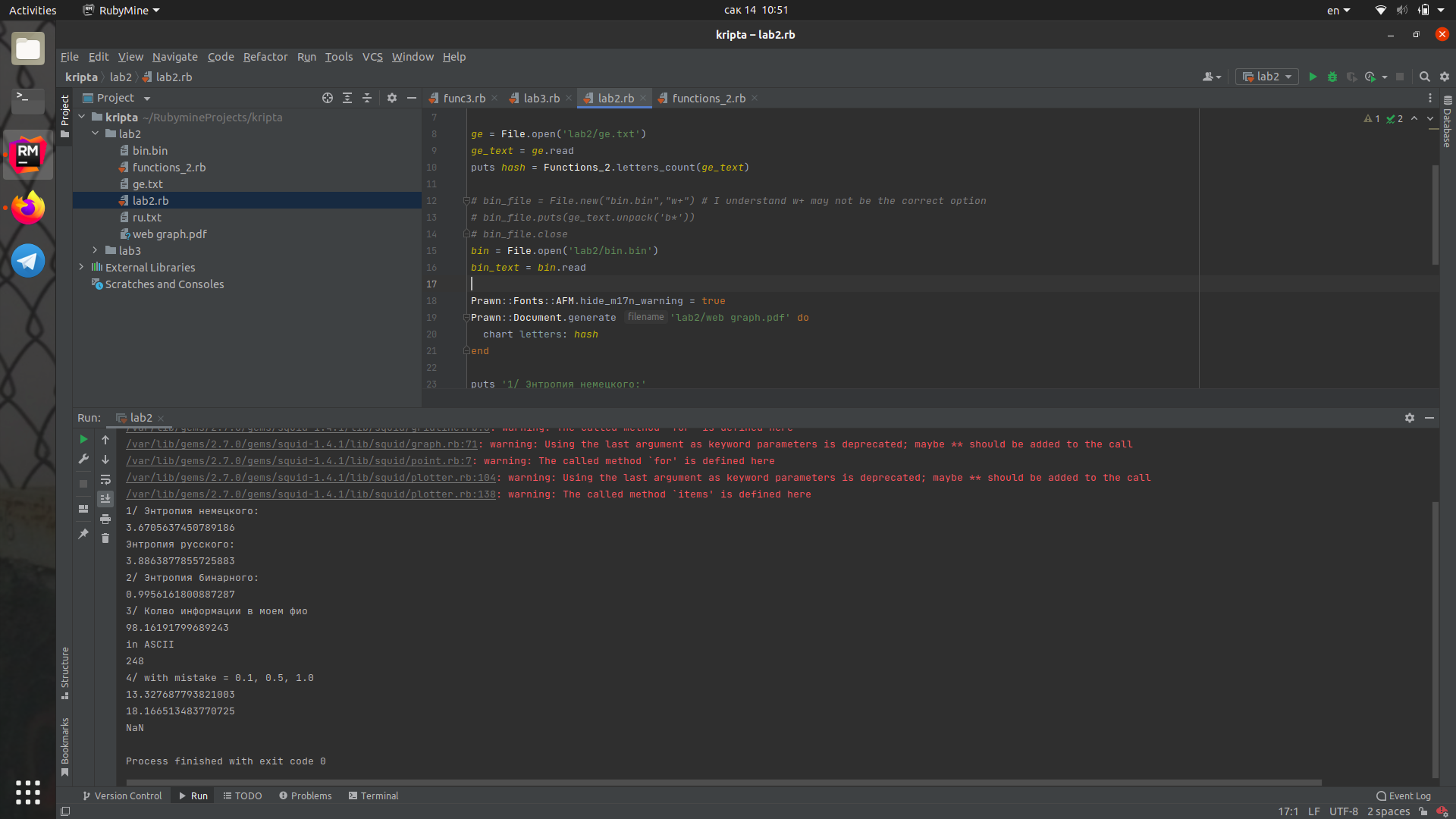


Рисунок 1 - Результат работы программы

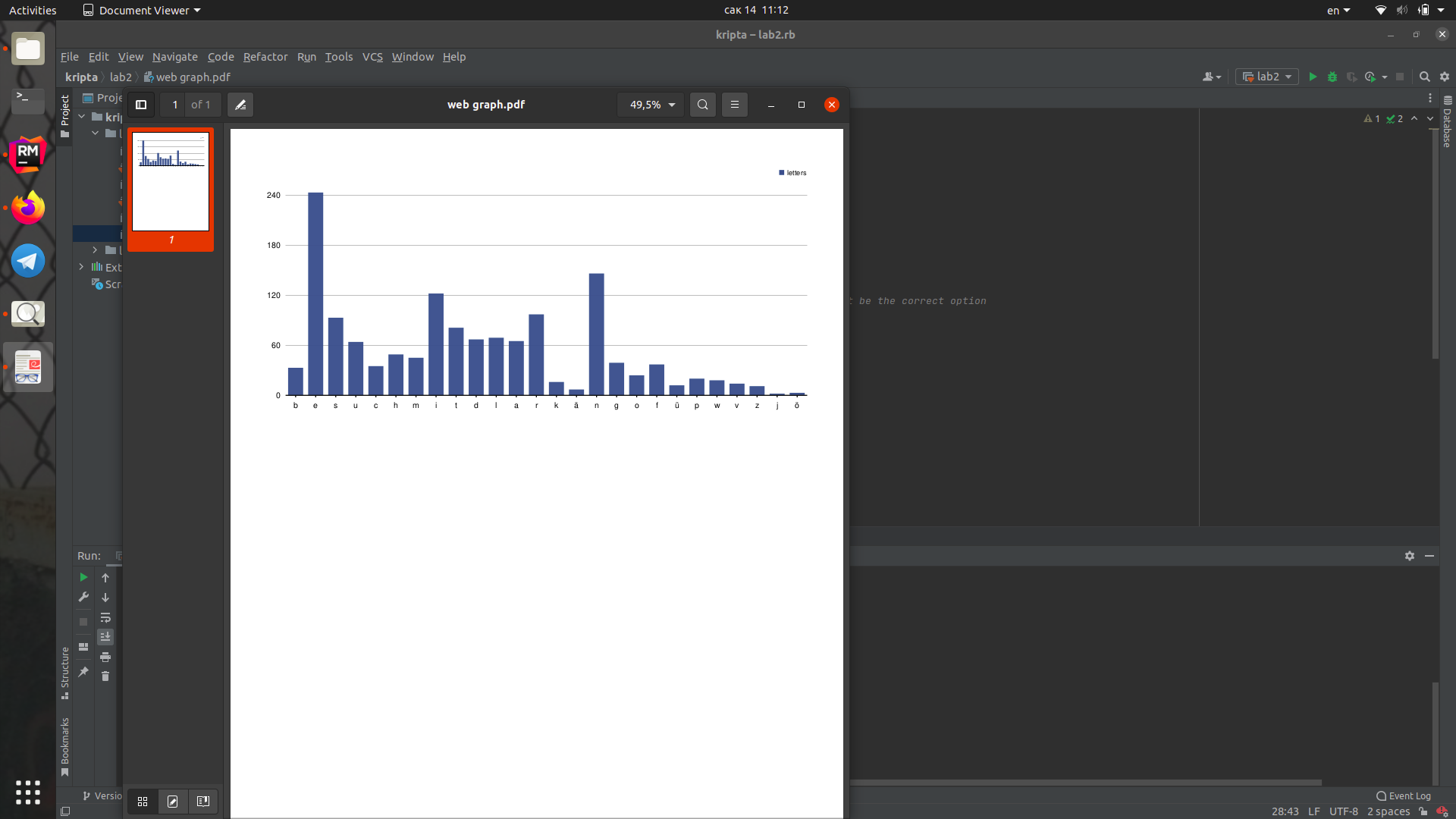


Рисунок 2 - График частоты использования букв в немецком языке

**Выводы:**

В результате выполнения лабораторной работы были приобретены практические навыки расчета и анализа параметров и информативных характеристик дискретных ИС, закреплены теоретические знания по основам теории информации, разработано приложение для расчета и анализа параметров и информативных характеристик дискретных ИС.

**Вопросы для контроля и самоконтроля**

1. Что такое алфавит источника сообщения?

2. Что такое мощность алфавита источника сообщения?

3. Какова мощность алфавита белорусского языка?

4. Какова мощность алфавита русского языка?

5. Какова мощность алфавита «компьютерного» языка?

6. Что такое энтропия алфавита?

7. Что такое энтропия сообщения?

8. От чего зависит энтропия алфавита?

9. Записать формулу для вычисления энтропии.

10. Что нужно знать для вычисления энтропии алфавита?

11. Как рассчитываются энтропия Шеннона и энтропия Хартли? В чем принципиальное различие между этими характеристиками? Дайте толкование физического смысла энтропии.

12. Пояснить назначение знака «минус» в формулах (2.1) и (2.4).

13. Что такое избыточность алфавита и избыточность сообщений, сформированных в компьютерных системах? Принцип действия каких систем основан на существовании данной избыточности?

14. Расположить в порядке возрастания энтропии известные Вам алфавиты.

15. Вычислить энтропию алфавита белорусского (русского) языка.

16. Вычислить энтропию Шеннона бинарного алфавита, если вероятность появления в произвольном документе на основе этого алфавита одного из символов составляет 0,25, другого – 0,75; либо 0 и 1,0; либо 0,5 и 0,5.

17. Чему равна энтропия алфавита по Хартли, если мощность этого алфавита равна: а) 1 символ; б) 2 символа; в) 8 символов?