МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 05 03 Информационные системы и технологии Направление специальности 1-40 01 05 03 Программное обеспечение информационных технологий

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №2:**

по дисциплине «Криптографические методы защиты информации»

Тема «Элементы теории информации»

Студент: Вайсера Р.Л.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова

1. **Описание разработанного приложения**

Приложение написано на языке программирования C# и позволяет:

* рассчитать энтропию шотландского и чукотского алфавита; в качестве входного принята строка;
* сгенерировать гистограммы частот появления символов (MSExcel);
* определить энтропию бинарного алфавита для строки;
* подсчитать количество информации в сообщении, состоящем из ФИО;
* выполнить предыдущее задание при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0.1, 0.5, 1.0.

1. **Методика выполнения поставленных задач**

Для расчета энтропии испанского и сербского алфавитов с помощью разработанного нами приложения текст из входной строки, которая затем передается в качестве параметра при вызове функции, рассчитывающей энтропию алфавита. Описание данной функции представлено на рисунке 2.1.

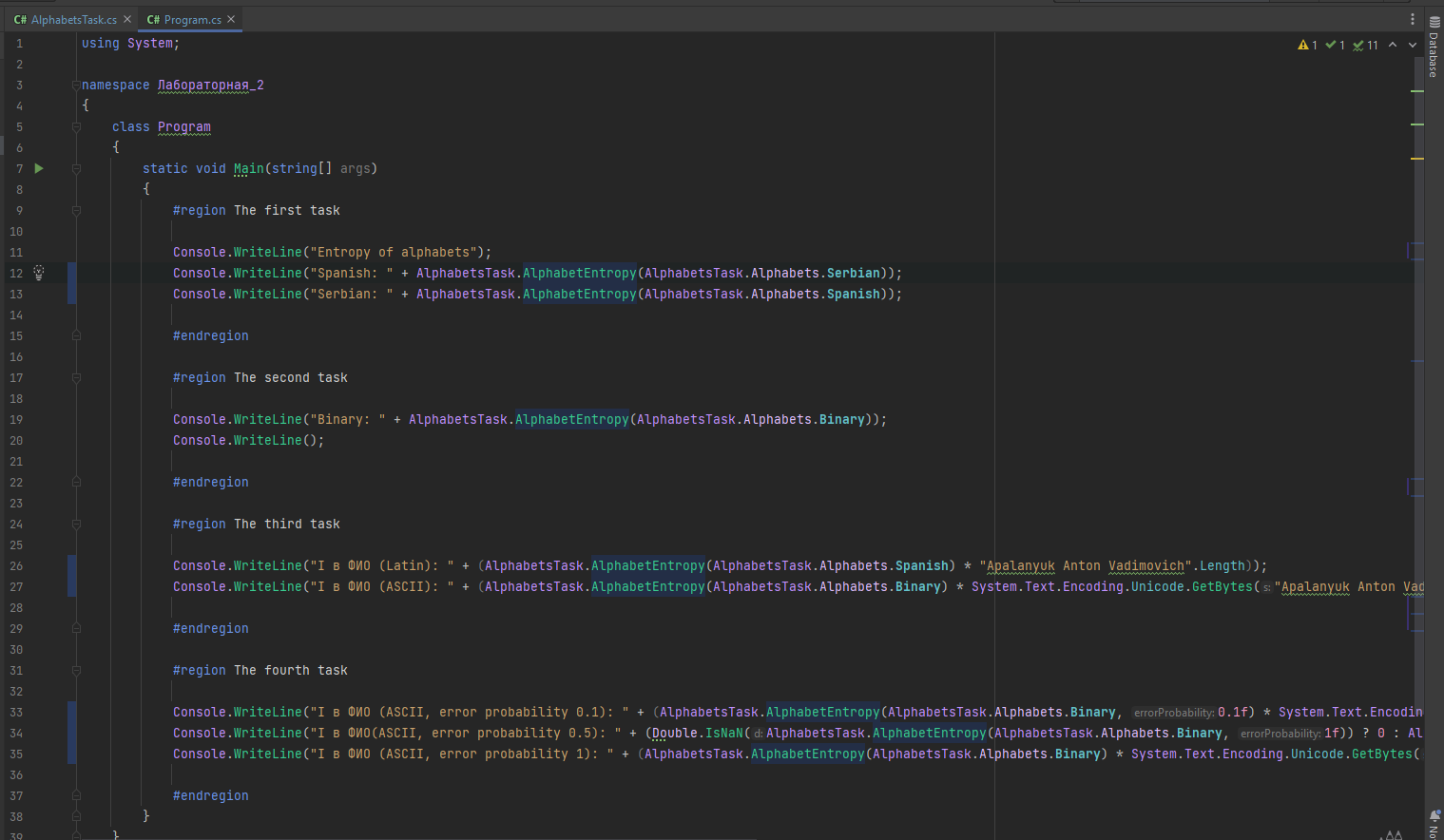


Рис. 2.1 – Функция для расчета энтропии

В результате выполнения данной функции возвращается значение энтропии, рассчитанное по формуле Шеннона: .

На основании частот появления символов, рассчитанных на предыдущем шаге, создана гистограммы. Данная гистограммы отображена на рисунке 2.3 и рисунке 2.4.

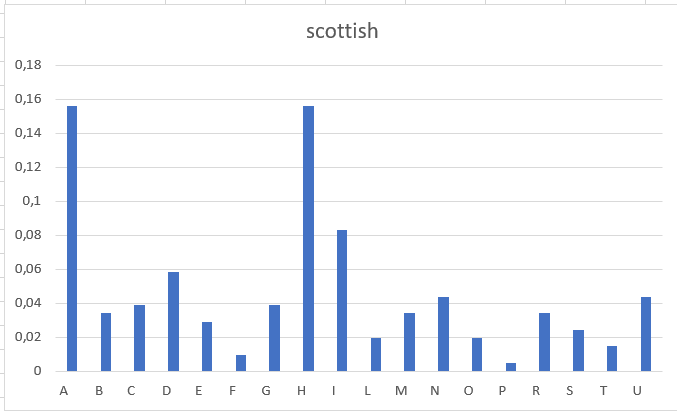


Рис. 2.3 – Гистограмма частот появления символов

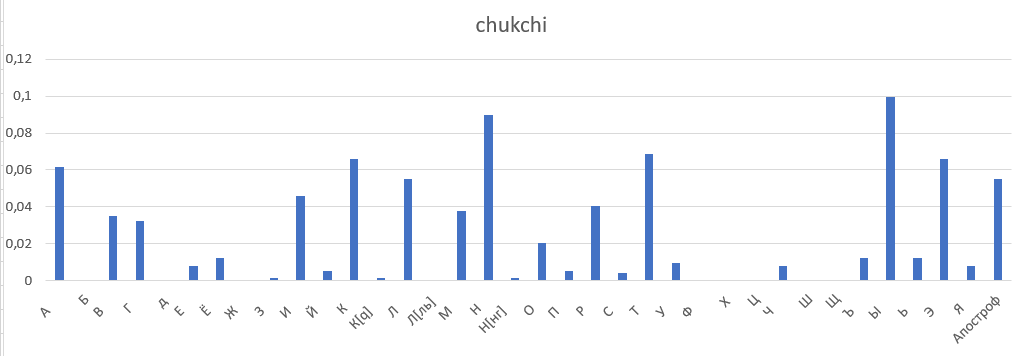


Рис. 2.4 – Гистограмма частот появления символов

Также приложение преобразует ФИО студента на шотландском языке в двоичное представление и после этого содержимое данного файла передается в функцию для расчета количества информации.

Затем приложение рассчитывает эффективную энтропию бинарного алфавита, рассчитанную по формуле , где , для различных вероятностей ошибочной передачи единичного бита (0.1, 0.5, 1.0) и выводит результат в терминал, вывод которого представлено на рисунке 2.5.



Рисунок 2.5 – Вывод терминала для бинарного алфавита

Затем приложение рассчитывает эффективную энтропию шотландского алфавита, для различных вероятностей ошибочной передачи единичного бита (0.1, 0.5, 1.0) и выводит результат в терминал, вывод которого представлено на рисунке 2.6. На рисунке видно, что количество информации шотландского алфавита при вероятности ошибки равной 1 равно 0, чего не скажешь о бинарном. Это объясняется тем, что бинарный имеет свойство инвертированности, который имеют все алфавиты, мощность которых не превышает 2, чего не скажешь о шотландским языке

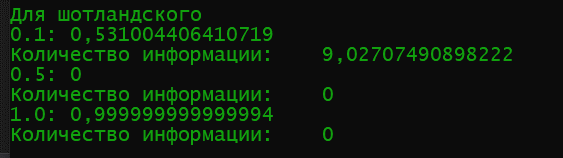


Рисунок 2.6 – Вывод терминала для шотландского алфавита

**Вывод**

В ходе лабораторной работы были закреплены теоретические знания по основам теории информации.

Также было разработано приложение для расчета и анализа параметров и информативных характеристик дискретных ИС.

Был сделан вывод, что при ошибки равной 1.0 для бинарного алфавита, количество информации будет таким же как при верной передачи, из-за того, что бинарный алфавит имеет свойство инвертированности.

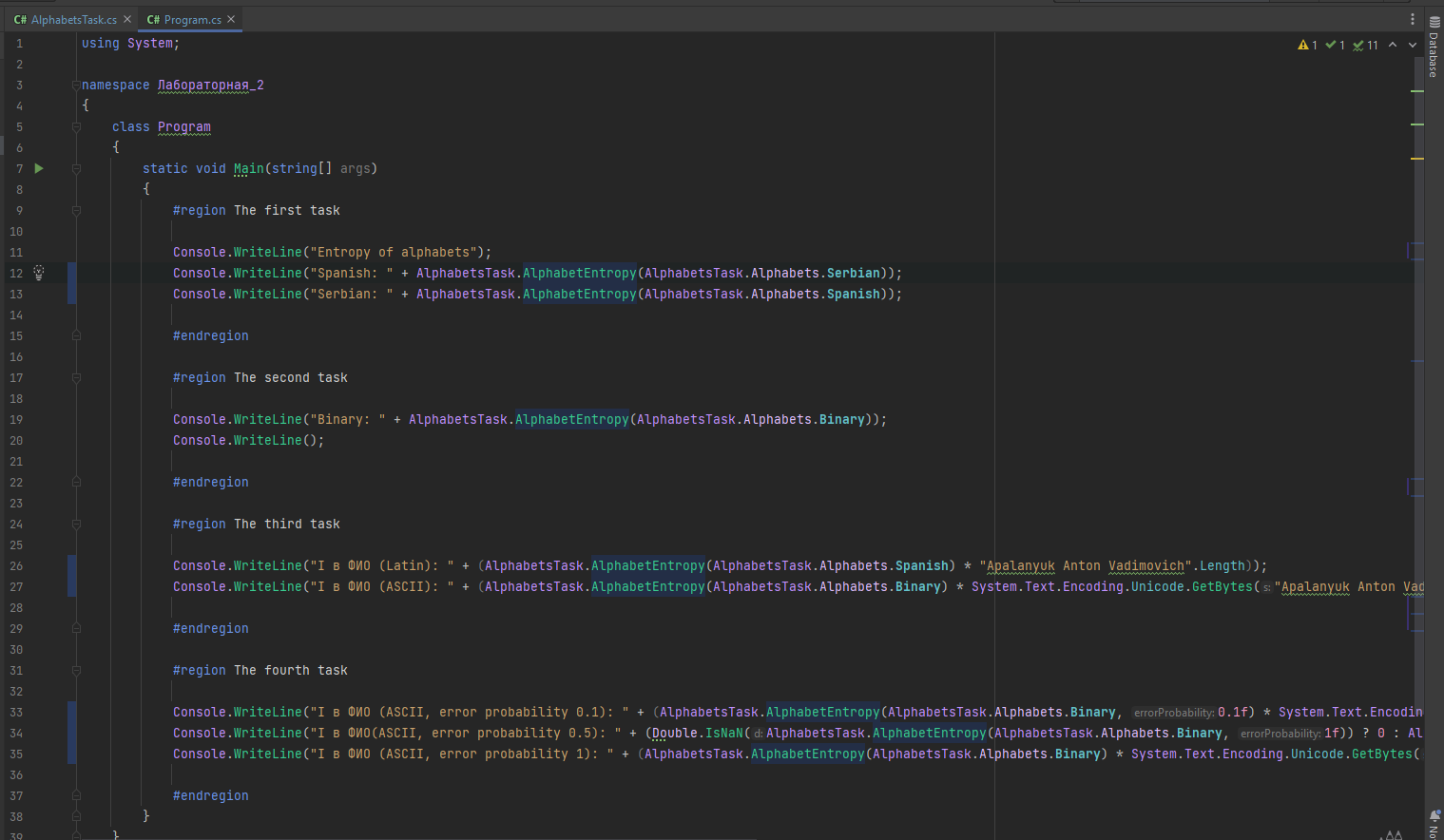


Рисунок 1 – Код программы

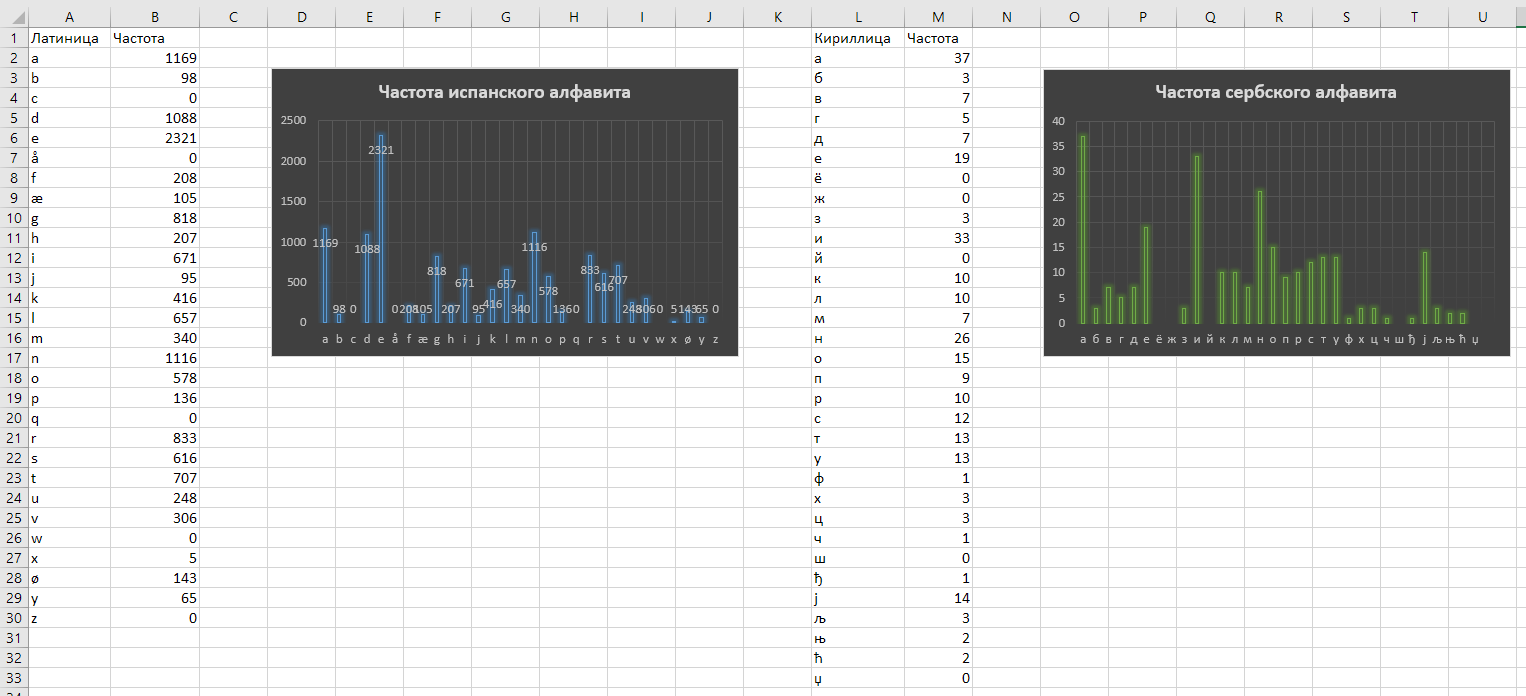


Рисунок 2 – Гистограмма частоты появления символов в алфавите



Рисунок 3 – Результат выполнения программы

**Вывод:** бинарное представление сообщения обладает избыточной информативностью. Для передачи информации выгодно использовать алфавит с меньшей избыточностью. Данный способ будет минимизировать потерю данных, а также уменьшит объем данных.