Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №2**

**Тема «****Элементы теории информации. Параметры и характеристики дискретных информационных систем»**

Цель: приобретение практических навыков расчета и анализа

параметров и информативных характеристик дискретных ИС.

Задачи:

1. Закрепить теоретические знания по основам теории информации.

2. Разработать приложение для расчета и анализа параметров

и информативных характеристик дискретных ИС.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Определение энтропии алфавитов**

Энтропия алфавита является мерой неопределенности, связанной с его вероятностным распределением. Она измеряется в битах и может быть рассчитана по следующей формуле:

***H* = –Σ *p*(*x*) *log*2 *p*(*x*)**

где *H* – энтропия алфавита, *p*(*x*) – вероятность появления символа x в алфавите.

В рамках практического задания была рассчитана энтропия для двух алфавитов: Датского и Македонского.

Для вычисления энтропии было разработано приложение на ЯП *C*#. Код представлен на рисунке 1.1

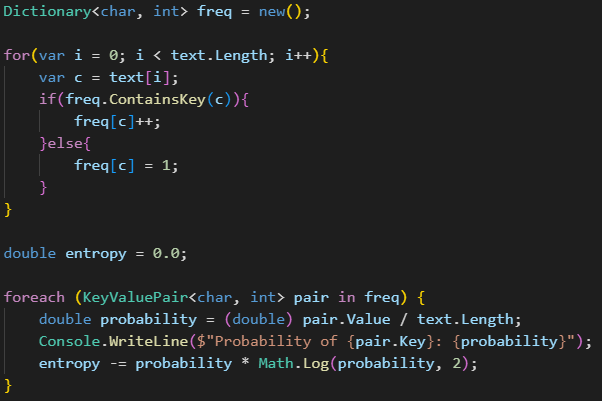


Рисунок 1.1 – Код для вычисления энтропии алфавита

Так же были созданы гистограммы, показывающие отношение символов к частоте их появления. Гистограммы представлены на рисунках 1.2 и 1.3 соответственно.

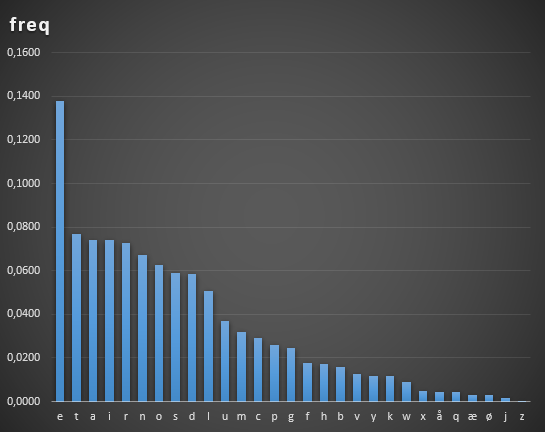


Рисунок 1.2 – Гистограмма частоты символов Датского алфавита

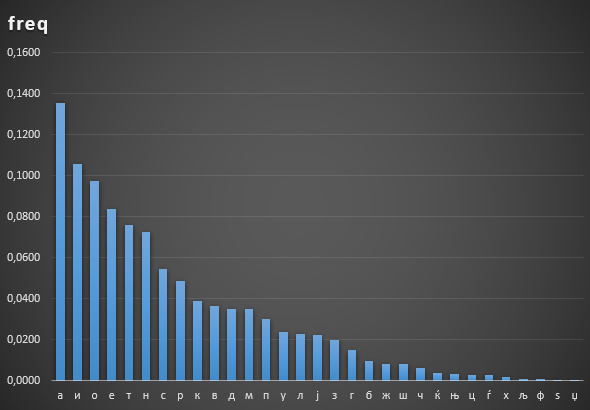


Рисунок 1.3 – Гистограмма частоты символов Македонского алфавита

В результате вычислений получилось:

Энтропия Датского алфавита: 4,24 бита

Энтропия Македонского алфавита: 4,14 бита

Энтропия бинарного алфавита: 0,99 бита

В ходе вычислений были использованы случайно сгенерированные тексты на каждом из алфавитов.

**Подсчёт количества информации**

На основе подсчитанной ранее энтропии для каждого из алфавитов необходимо рассчитать количество информации в сообщении для собственных фамилии, имени и отчества. Так же необходимо посчитать при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0,1; 0,5; 1,0.

Для вычисления использовалась следующие формулы:

Вычисление количества информации с известной энтропией:

*I* = *H* \* *L*

где *I* – количество информации, *H* – энтропия алфавита (в битах на символ), *L* – длина сообщения (в символах).

При вероятности ошибочной передачи:

*I* = –*log*2(*p*) \* *L*

где *I* – количество информации в битах, *p* – вероятность правильной передачи единичного бита сообщения, *L* – длина сообщения в битах.

Результаты вычислений предоставлены в таблице 1.1

Таблица 1.1 – Результаты по вычислению количества информации

|  |  |  |  |
| --- | --- | --- | --- |
| Условие: | Датский | Македонский | Бинарный |
| Известна энтропия | 114 | 107 | 230 |
| Вероятность ошибки: 0,1 | 14,33 | 13,80 | 123,19 |
| Вероятность ошибки: 0,5 | 0 | 0 | 0 |
| Вероятность ошибки: 1,0 | 24,81 | 0 | 0 |

Формула для вероятности ошибочной передачи не работает естественными алфавитами из-за того, что вероятность найти нужный символ вместо ошибочного слишком мала. И опять же, формула работает для бинарного алфавита из-за того, что в алфавите всего 2 символа и мы легко можем понять, что его нужно заменить на противоположный.

**Заключение**

В ходе выполнения лабораторной работы были приобретены практические навыки расчёта и анализа параметров и информативных характеристик дискретных информационных систем.