МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №2:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

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

**Цель:** приобретение практических навыков расчета и анализа параметров и информативных характеристик дискретных ИС. Ответить на следующие вопросы:

**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.

**Теоретические сведения**

Передача информации (данных) осуществляется между двумя абонентами, называемыми источником сообщения (ИcС) и получателем сообщения (ПС). Третьим элементом информационной системы является канал (среда) передачи, связывающий ИсС и ПС.

Отметим также, что и в системах с хранением информации всегда можно выделить ИcС и ПС. В данном случае каналом передачи здесь выступает устройство хранения информации (память). Например, при записи данных в ОЗУ (оперативное запоминающее устройство) компьютера в качестве ИcС и ПС может выступать процессор (соответственно при записи и чтении данных).

Таким образом, простейшая информационная система состоит из трех элементов: источника сообщения, канала передачи сообщения и получателя сообщения.

Отображение сообщения обеспечивается изменением какой-либо физической величины, характеризующей процесс (например, амплитуда, частота, фаза). Эта величина является информационным параметром сигнала (в общем случае – информационной системы).

Сигналы, как и сообщения, могут быть непрерывными и дискретными. Информационный параметр непрерывного сигнала с течением времени может принимать любые мгновенные значения в определенных пределах. Непрерывный сигнал часто называют аналоговым, а каналы и устройства, функционирующие на основе такого типа сигналов – аналоговыми.

Дискретный сигнал (устройство или канал передачи) характеризуется конечным числом значений информационного параметра.

Дискретные сообщения состоят из последовательности дискретных знаков. Часто этот параметр принимает всего два значения (0 или 1).

Сообщение или канал его передачи на основе этих двух значений сигнала называют двоичным или бинарным.

Построение сигнала по определенным правилам, обеспечивающим соответствие между сообщением и сигналом, называют кодированием.

Кодирование в широком смысле– преобразование сообщения в сигнал.

Кодирование в узком смысле – представление исходных знаков, называемых символами, в другом алфавите с меньшим числом знаков. Оно осуществляется с целью повышения надежности и преобразования сигналов к виду, удобному для передачи по каналам связи. Последний тип кодирования относится к так называемой прикладной теории кодирования информации, занимающейся поиском и реализацией методов и средств обнаружения несоответствий (ошибок) между переданным *Xk* и принятым *Yk* сообщениями.

**Ход работы**

Приложение разработано на NodeJS.

**Задание №1, 2**

Для расчета энтропии я использовала формулу энтропии алфавита по К. Шеннону.

Функция представляет собой цикл, проходящий по каждой букве заданного сообщения. С помощью объекта RegExp мы проверяем количество вхождения буквы в заданное сообщение. Если частота вхождения буквы равно нулю, переходим к следующей букве алфавита, если же не равна нулю, рассчитываем вероятность появления этой буквы в сообщении, а затем перемножив значение вероятности на логарифм по основанию 2 от вероятности появления буквы получаем энтропию.

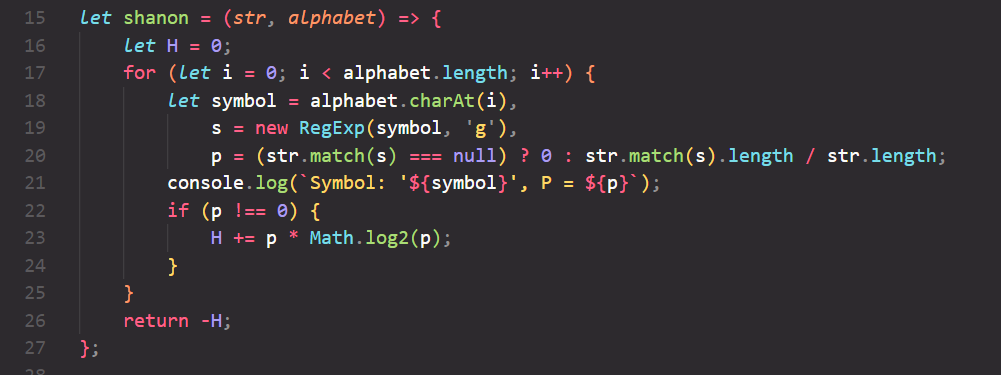


Рисунок 1 —  Функция для расчета энтропии

На данном рисунке представлена частота появления каждой буквы из чешского алфавита в заданном сообщении.

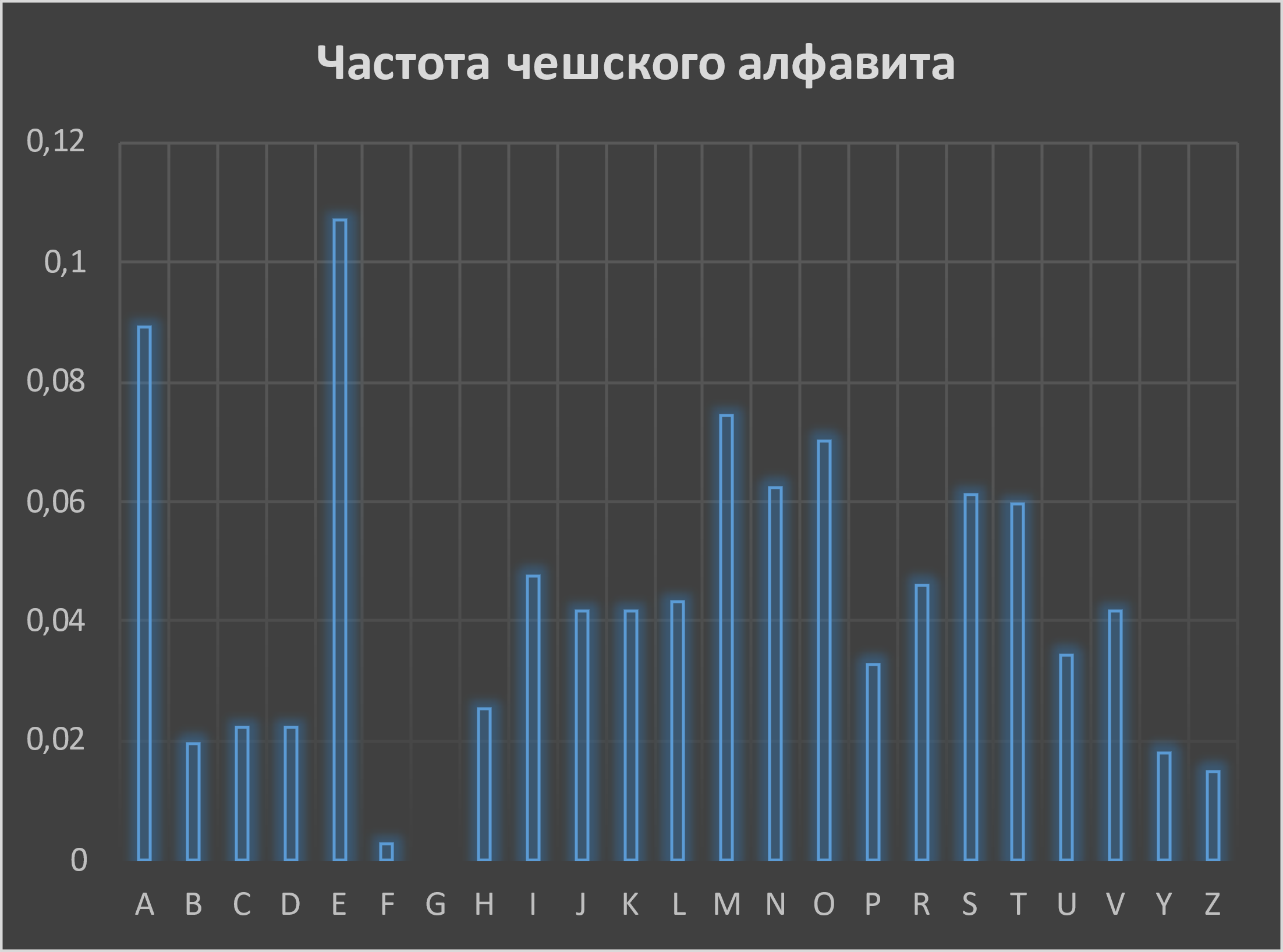


Рисунок 2 —  Частота чешского алфавита

На данном рисунке представлена частота появления каждой буквы из таджикского алфавита в заданном сообщении.



Рисунок 3 —  Частота чешского алфавита

**Задание №3**

В данном задании нам надо было посчитать количество информации в заданном сообщении. Сообщение представляло собой ФИО учащегося. Для расчета количества информации в сообщении нам надо перемножить энтропию используемого алфавита на количество символов в сообщении.

В качестве параметров функция принимает заданное сообщение и энтропию алфавита.

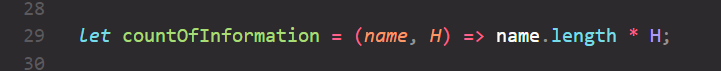


Рисунок 4 —  Функция для расчета количества информации

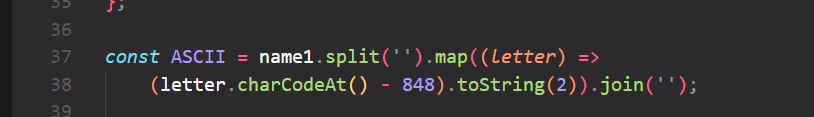


Рисунок 5 — Функция для расчета количества информации в кодах ASCII

**Задание №4**

В данном задании нам надо было рассчитать количество информации в сообщении при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0,1; 0,5; 1,0.

Данная функция в качестве параметра принимает значение вероятности ошибочной передачи единичного бита сообщения.

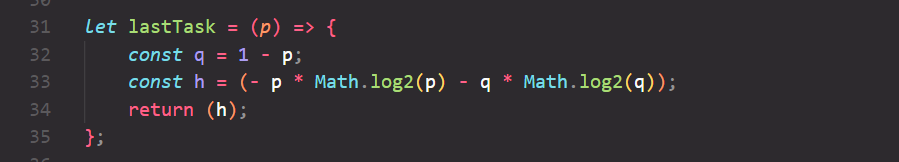


Рисунок 6 —  Функция для расчета количества информации с различными вероятностями ошибочной передачи единичного бита сообщения

Итог выполнения данной лабораторной работы представлен на рисунке 7. В первом и втором задании представлена посчитанная энтропия для таджикского, чешского и бинарного алфавита соответственно.

В 3 задании посчитано количество информации в сообщении состоящего из ФИО учащегося. Количество информации для таджикского и чешского представляет собой произведение их энтропий на количество символов в сообщении. Для подсчета количества информации в кодах аски, надо было сообщение перевести согласно данному алфавиту и использовать энтропию бинарного алфавита.

При расчете количества информации с вероятностью ошибочной передачи единичного бита сообщения надо было учитывать количество символов в алфавите. Так как если алфавит состоит из двух символов, как бинарный алфавит, то количество информации будет больше нуля, так как мы просто поменяем значения на противоположные. Если алфавит состоит более чем из двух символов, то количество информации будет стремиться к нулю.

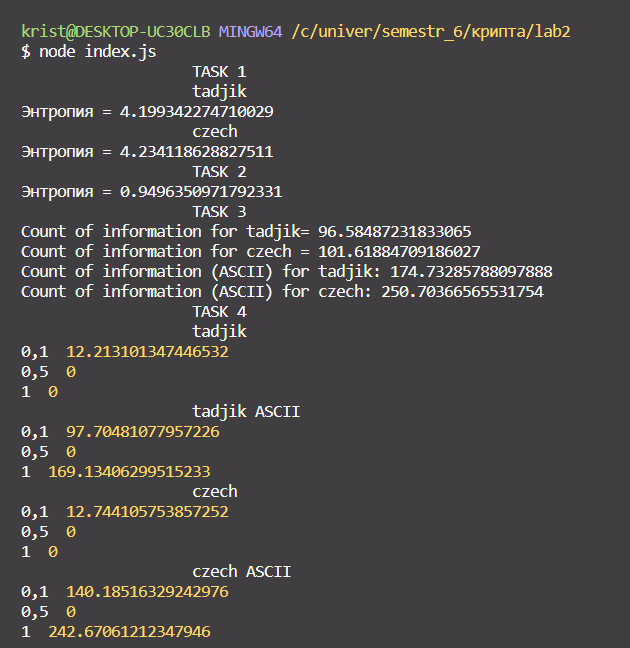


Рисунок 7 —  Вывод

**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.