Министерство образования и науки Российской Федерации

Санкт-Петербургский Политехнический Университет Петра Великого

**Институт кибербезопасности и защиты информации.**

**ЛАБОРАТОРНАЯ РАБОТА 10**

**Методы надежного хранения и передачи информации.**

по дисциплине «Основы информационной безопасности»

Выполнил

студент гр. 4851003/10002 Лобов Е.А

Преподаватель Зубков Е.А.

Санкт-Петербург

2022

**Цель работы**

Цель работы - ознакомление с методом Хэмминга помехоустойчивого кодирования, позволяющим обнаруживать и автоматически исправлять ошибки, возникающие при хранении и передаче информации в ненадежных средах.

# 1.ход работы

## 1.1 Расчет кода Хэмминга для 16-разрядного числа.

Возьму случайное 16-разрядное число:

1010 0011 0110 0011. Поставлю \* на позиции степеней двойки:

\*\*1\*010\*0011011\*00011. Рассчитаю значения контрольных бит:

1)\* 1 0 0 0 1 0 1 0 0 1 - четное кол-во единиц => 0

2)\*1 10 01 11 00 - нечетное кол-во единиц => 1

4)\*010 1011 11 - четное кол-во единиц => 0

8)\*0011011 - четное кол-во единиц => 0

16)\*00011 - четное кол-во единиц => 0

Ответ: 011001000011011000011.

## 1.2 Блок-схема алгоритма вычисления помехоустойчивого кода.

## 1.3 Описание однобитных и групповых ошибок, внесенных в файл.

Сообщение до кодирования.

Сообщение после кодирования.

Применю код Хэмминга для сообщения длинной в 100 символов. Внесу несколько однобитных ошибок.

Внесенные изменения.

При однобитных ошибках процесс декодирования будет успешен.

Результат декодирования.

Результат декодирования в hex-редакторе.

Это доказывает работоспособность кода Хэмминга, ошибки были найдены и исправлены автоматически.Теперь внесу множественные изменения.

Внесение множественных ошибок.

При множественных ошибках код Хэмминга не поможет в их поиске и устранении, поэтому результат декодирования будет неправильным.

Результат декодирования при множественных ошибках

## 1.4 График зависимости изменения объема закодированной информации от размера кодируемых блоков.

График зависимости изменения объема закодированной информации от

размера кодируемых байтов.

# 2.Ответы на контрольные вопросы.

1.Что такое расстояние Хэмминга?

Число позиций, в которых соответствующие символы двух слов одинаковой длины различны. В более общем случае расстояние Хэмминга применяется для строк одинаковой длины любых *q*-ичных алфавитов и служит метрикой различия объектов одинаковой размерности.

2.Опишите метод кодирования Рида-Соломона.

Коды Рида – Соломона – это линейные недвоичные систематические циклические коды, символы которых представляют собой r-битовые последовательности, где r – целое положительное число, большее 1.

Коды Рида – Соломона (n, k) определены на r-битовых символах при всех n и k, для которых:

0 < k < n < 2r + 2, где

k – число информационных символов, подлежащих кодированию,

n – число кодовых символов в кодируемом блоке.

Для большинства (n, k)-кодов Рида – Соломона; (n, k) = (2r–1, 2r–1–2∙t), где

t – количество ошибочных символов, которые может исправить код, а

n–k = 2t – число контрольных символов.

3.Как контролировать ошибку в бите 8?

Добавив контрольный бит, т.к в данном случае им можно пренебречь, ведь этот бит не несет контрольного значения и ничем не контролируется.

4.На что влияет размер кодируемого блока в методе Хэмминга?

На объем кодируемой информации. Чем меньше размер кодируемого блока, тем больше будет объем и наоборот. Код Хэмминга предполагает исправлении лишь одного неверно переданного бита, поэтому при передаче нескольких неправильных бит независимо от длины кодируемого блока результат будет неверным.

5.Постройте схему размещения информационных и контрольных бит в блоке размером 16 разрядов.



к - контрольный бит.

и - информационный бит.

**3.Вывод.**

В ходе работы был разработан код для помехоустойчивого кодирования Хэмминга, позволяющий исправить одну ошибку в кодируемом блоке, также были затронуты другие алгоритмы помехоустойчивого кодирования, позволяющие исправить большее количество ошибок. Была изучена зависимость объема информации после кодирования от длины кодового слова. Возможность “застраховать” передаваемые данные от ошибки очень важна, поэтому применяются подобные алгоритмы кодирования. Однако вместе с безопасностью передаваемых данных увеличивается также их объем, поэтому важно найти оптимальное решение. Для этого необходимо изучить канал передачи данных и частоту ошибок для него.