МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Помехоустойчивое кодирование: циклические коды

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Швецовой Елизаветы Максимовны

Научный руководитель
доцент, к.п.н. _____ А. С. Гераськин
22.01.2024 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2024 г.

Саратов 2024

ВВЕДЕНИЕ

С развитием современных информационных технологий и распространением применения беспроводных средств связи, цифровых телекоммуникаций и передачи данных, вопрос об эффективной защите информации от ошибок при передаче становится более актуальным и критическим. Одним из ключевых элементов, обеспечивающих надежность передачи данных и их целостности, являются системы помехоустойчивого кодирования.

Система помехоустойчивого кодирования представляет собой методологию обработки данных, направленную на защиту информации от возможных ошибок, возникающих в процессе передачи или хранения данных в условиях наличия помех. Эта система использует специальные коды, добавляемые к исходным данным, чтобы обеспечить возможность обнаружения и исправления ошибок при их возникновении. Целью систем помехоустойчивого кодирования является повышение надежности передачи данных и обеспечение целостности информации в условиях неблагоприятного воздействия различных факторов, таких как электромагнитные помехи, шумы в канале связи или ошибки в памяти устройств хранения.

Анализ систем помехоустойчивого кодирования представляют собой важный научно-исследовательский вопрос, стоящий перед специалистами в области информационных технологий. Эффективные кодировочные схемы не только способствуют устранению ошибок при передаче данных, но и играют важную роль в повышении производительности современных коммуникационных систем.

Целью настоящей дипломной работы является построение системы помехоустойчивого кодирования, включающей в себя модель цифрового канала связи и выбранный алгоритм помехоустойчивого кодирования.

В процессе исследования будут рассмотрены различные типы циклических кодов. Также будет проведен разбор методов декодирования, используемых для восстановления информации в условиях наличия помех.

При этом объектами исследований являются циклические коды и системы защиты информации, основанные на помехоустойчивых циклических кодах, а предметом исследований — методы построения циклических кодов и способы их декодирования.

Для достижения указанной цели в работе решаются следующие задачи:

- Теоретическое изучение различных типов циклических помехоустойчивых кодов и алгоритмов их реализации;
- Изучение алгоритма модели построения цифрового канала связи;
- Реализация цифрового канала связи и выбранного алгоритма помехоустойчивого кодирования.

Дипломная работа состоит из введения, 3-х разделов, заключения, списка использованных источников и 1-го приложения. Общий объем работы – 62 страницы, из них 40 страниц – основное содержание, включая 12 рисунков и список использованных источников из 23-х наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Ниже описано краткое содержание глав дипломной работы.

В **первом разделе** приводятся основы помехоустойчивого кодирования, подробно рассматриваются циклические коды и конкретные коды данного типа. Т.к. этот раздел самый объёмный рассмотрим краткое содержание по главам.

Первая глава первого раздела представляет собой введение в область помехоустойчивого кодирования. Кратко описывается процесс помехоустойчивого кодирования, определяя этапы кодирования и декодирования. Также приводится структура цифровой системы передачи данных.

Приводится определение ошибки в контексте передачи данных через каналы связи и их влияние на передаваемую информацию. Также рассматриваются основные параметры, характеризующие корректирующие свойства кодов:

- избыточность;
- кодовое расстояние (характеризует степень различия любых двух кодовых комбинаций);
- кратность гарантированно обнаруживаемых и исправляемых ошибок;
- основание кода (количество возможных значений для отдельного символа кодовой последовательности).

Вторая глава первого раздела посвящена классификации помехоустойчивых кодов по различным признакам. Описывается схема классификации помехоустойчивых кодов и их основных характеристик.

Рассматривается различные методы классификации помехоустойчивых кодов. Первым приводится разделение на блочные и непрерывные коды. Кратко приведён процесс преобразования поступающего блока информационных символов в кодовую последовательность из выходных

символов для блочных кодов. Также рассматривается понятие непрерывных кодов и описывается работа кодера для таких кодов. Кратко приведены классификации по способу кодирования на систематические и несистематические, по типу корректирующей способности на коды, для исправления случайных ошибок, и коды, предназначенные для коррекции пакетов ошибок, а также разделяющая коды на линейные и нелинейные.

Третья глава первого раздела содержит краткое писание основных классов циклических кодов: циклические эквидистантные коды (коды максимальной длины), Рида–Маллера, Боуза–Чоудхури–Хоквингема (БЧХ), Рида–Соломона. Приводится их особенности и недостатки. Также обосновывается применение циклических кодов для обнаружения и исправления ошибок при передаче данных.

Четвёртая глава первого раздела представляет собой обзор основных принципов и свойств циклических кодов. В данной главе рассматривается структура циклических кодов, их математические основы и принципы построения. Особое внимание уделяется полиномиальному и векторному представлению кодовых комбинаций их связи и свойствам циклических кодов, которые определяют их построение.

В **пятой главе** первого раздела рассматриваются два основных метода кодирования в циклических кодах: систематическое и несистематическое. Особенность несистематического кодирования заключается в том, что среди элементов кодовой комбинации не может быть выделено отдельных информационных и проверочных элементов, в систематические наоборот избыточные элементы будут занимать определенные позиции.

В **шестой главе** первого раздела описан принцип обнаружения ошибок в классических циклических кодах: если при передаче сообщения ошибок не было, то принятая комбинация равна переданной кодовой комбинации. Кратко описываются операции для восстановления сообщения из кодового слова с ошибкой.

В **седьмой и восьмой главах** первого раздела описываются коды Боуза-Чаудхури-Хоквингхема(БЧХ) и Рида-Соломона(РС) соответственно, их особенности, способы кодирования и декодирования. После рассмотрения особенности обоих кодов для программной реализации был выбран код Рида-Соломона, так как он обеспечивает наибольшее минимальное расстояние и допускает более простую техническую реализацию

Второй раздел посвящен описанию принципов работы канала связи и его моделированию с использованием битового буфера. В данном разделе рассматриваются основные понятия и определения, связанные с передачей данных через канал связи, а также описываются методы моделирования канала связи с использованием битового буфера.

Подробно описывается принципиальная схема цифровой системы связи, которая включает в себя источник информации, кодер, канал связи, декодер и приемник.

Особое внимание уделяется битовому буферу, который является временным хранилищем для битовых данных, подвергающихся различным видам искажений и помех в канале связи. Описываются основные требования, предъявляемые к программной реализации битового буфера для создания модели системы кодирования информации и связи:

- размер битового буфера должен быть предопределенным и фиксированным;
- способность записи и чтения битовых полей с различной длиной;
- механизм контроля за уровнем заполненности;
- функции битового буфера должны быть ограничены только операцией записи (при кодировании данных) или только операцией чтения (при декодировании данных).

В **третьем разделе** приведена практическая часть работы, в которой рассматривается реализация битового буфера и кода Рида-Соломона.

Для реализации модели битового буфера и кода Рида-Соломона был выбран язык программирования C++ и интегрированная среда разработки Visual Studio 2019.

В разделе описываются основные функции работы битового буфера. Для хранения и доступа к данным будем использовать класс cBitStream. Переменная CurMode инициализируется при создании объекта класса cBitStream и может принимать одно из двух значений, определенных перечисляемым типом ModeType и соответствующих текущему режиму работы буфера – "чтение" или "запись". Для перемещения по буферу с целью чтения/записи данных, а также контроля состояния заполненности буфера требуется хранить смещение текущего байта ptrCurrentByte и указатель на текущий бит в буфере ptrCurrentBit.

Схема программы приведена на рисунке 1.

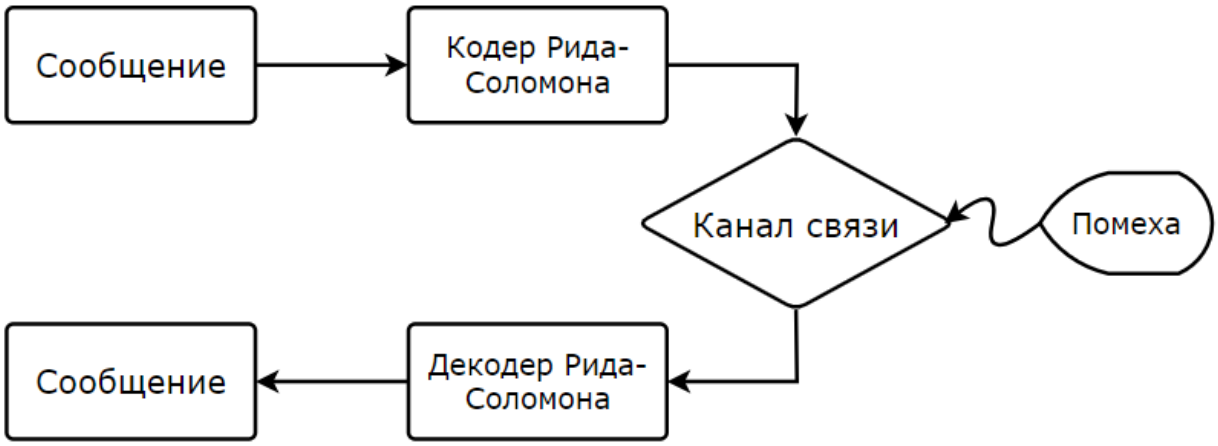

Рисунок 1 – Схема программы

В программе имеются 3 опции: предлагается ввести размер буфера (Enter buffer size:), выбрать режим работы программы – побитовый или блочный (Choose the encoding method: bits or fields (0/1)), в первом случае программа сразу перейдёт в исполнение, во втором же потребуется ввести размер файла.

Для оценки времени работы программы были использованы файлы различных размеров, а также были проведены эксперименты с разными режимами передачи данных. Результаты работы программы были представлены

в виде вывода на экран, что позволило оценить производительность алгоритмов обработки данных в различных условиях. Результаты работы программы приведены рисунках 2, 3, 4.

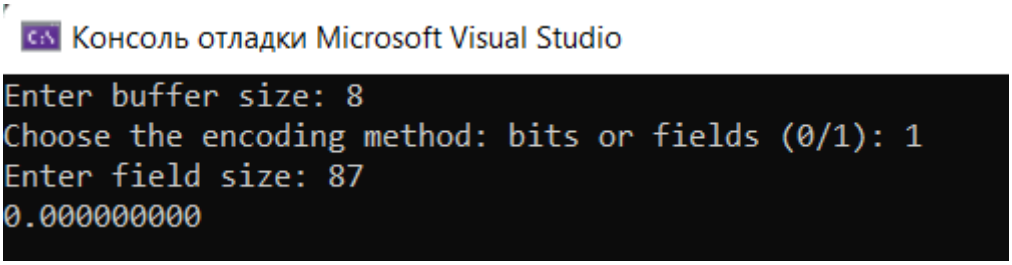

Рисунок 2 – Вывод работы программы в блочном режиме для файла размером 87 байт

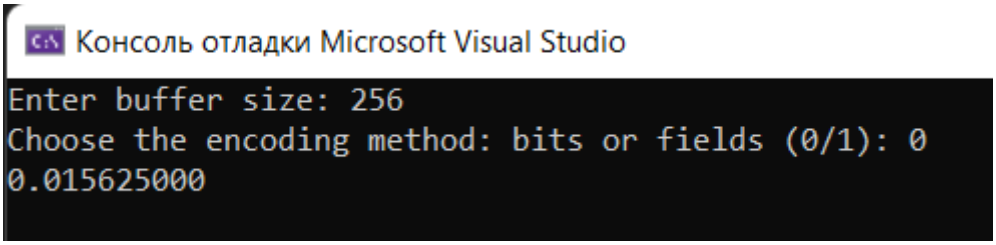

Рисунок 3 – Вывод работы программы с файлом размером 3000 байта в битовом режиме с размером буфера 256 бит

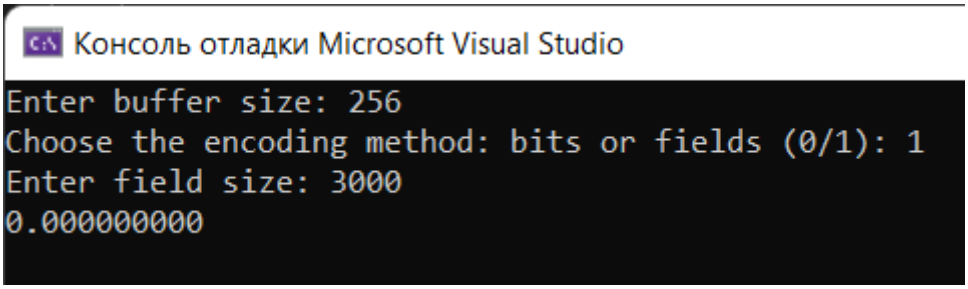

Рисунок 4 – Вывод работы программы с файлом размером 3000 байта в блочном режиме с размером буфера 256 бит

Описана реализация помехоустойчивого кодирования Рида-Соломона и реализация программы, эмитирующей передачу данных по цифровому каналу связи. Источником данных является сообщение, введенное с консоли. Кодирование и декодирование происходит кодом Рида-Соломона. Саму передачу сообщения эмитирует битовый буфер. После декодирования сообщение выводится в консоль как показано на рисунке 5.

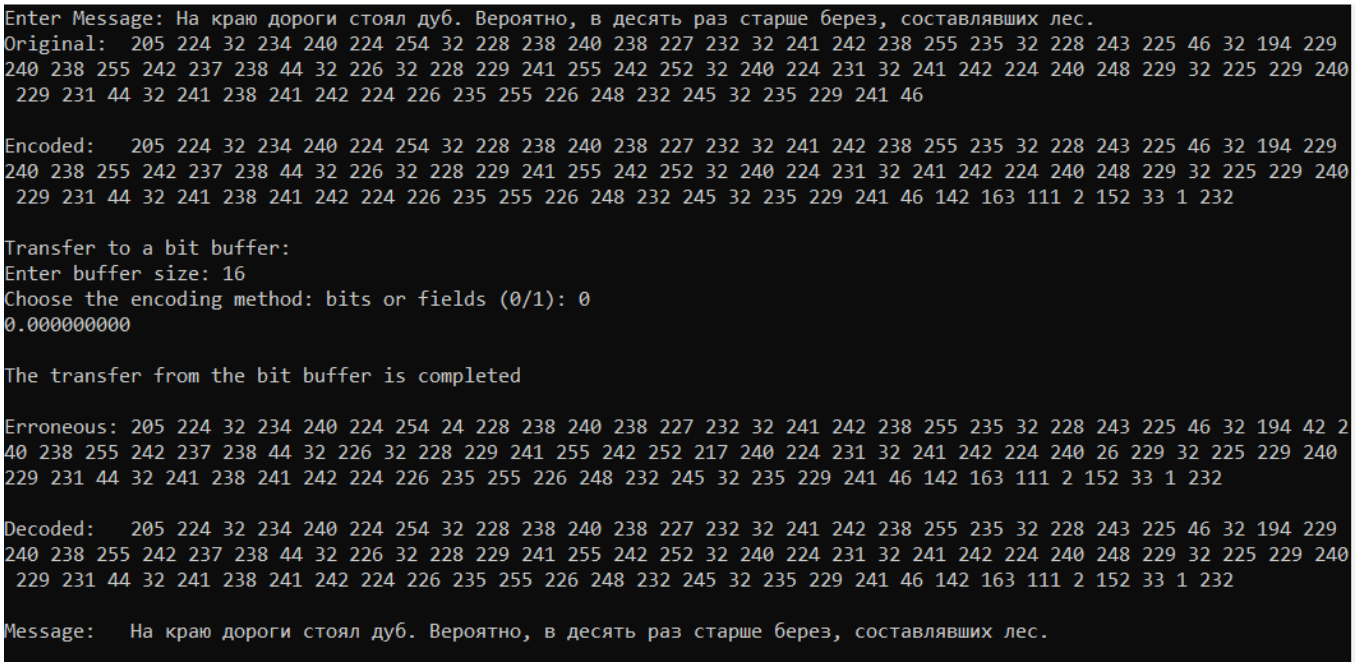

Рисунок 5 – Результат работы программы

ЗАКЛЮЧЕНИЕ

В ходе выполнения исследования были углубленно изучены основы помехоустойчивого кодирования, а также рассмотрен класс циклических кодов. Особое внимание было уделено анализу кода Рида-Соломона, поскольку он является максимальным и представляет собой эффективный вариант кодирования, обеспечивающий высокую степень помехоустойчивости.

Дополнительно была проведена детальная оценка возможности применения битового буфера в контексте моделирования цифрового канала связи. Результаты этого анализа позволили определить эффективность битового буфера для эмуляции передачи данных.

В рамках исследования была успешно реализована программа, в которой осуществлялось кодирование и декодирование сообщений с использованием кода Рида-Соломона. Кроме того, проводилась передача данных, эмулируемая битовым буфером. Этот подход позволил не только теоретически оценить работу алгоритмов кодирования и декодирования, но и протестировать их на практике через эмулированный канал связи.