Разработка помехоустойчивого кодека с применением технологий дизассемблирования и реверс инжиниринга

Студент Чеботарев Г.М. 43501/4
Научный руководитель Богач Н.В.

Помехоустойчивое кодирование

Описание проекта

Исходные данные к проекту:

- Прошивка устройства на базе TMS320C54

Поставленная задача:

- Провести обратную разработку
- Реализовать аналогичный кодек средствами языка программирования Си
- Ввести промежуточный режим кодирования в кодек

Дизассемблирование

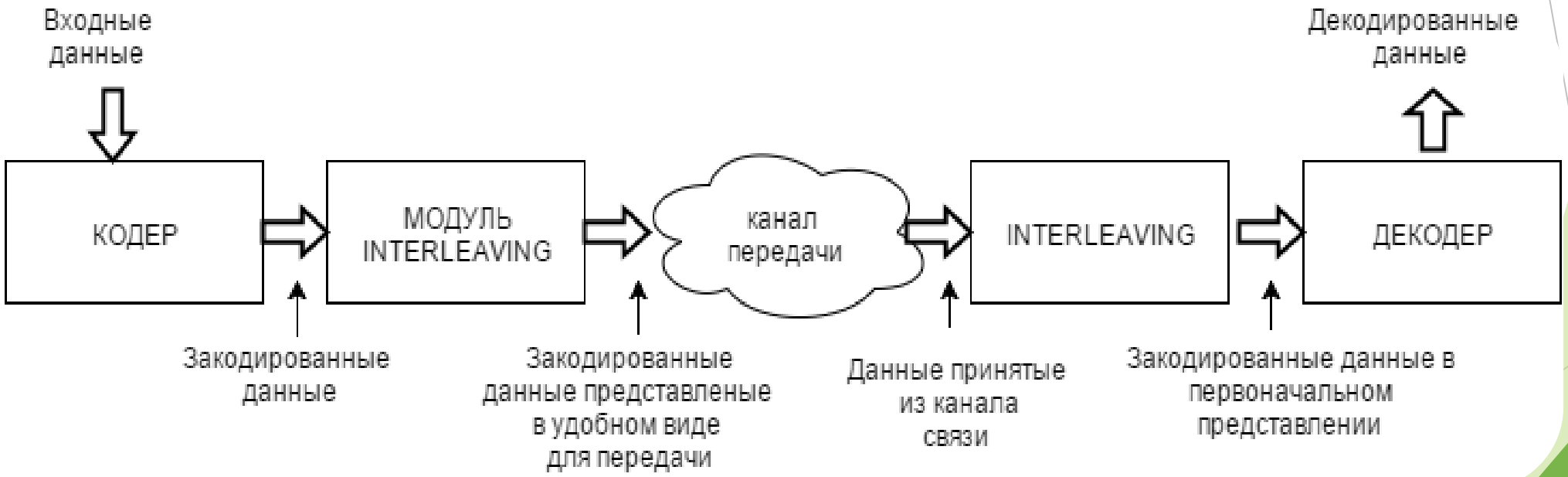
- Выбор дизассемблера -> *IDA Pro*
- Выбор симулятора -> *Code Composer Studio*

Процесс дизассемблирования

1) Прошивка.bin → *IDA Pro*
2) *IDA Pro → hex code + assemble code*
3) *hex code → Code Composer Studio*

Анализ полученного кода

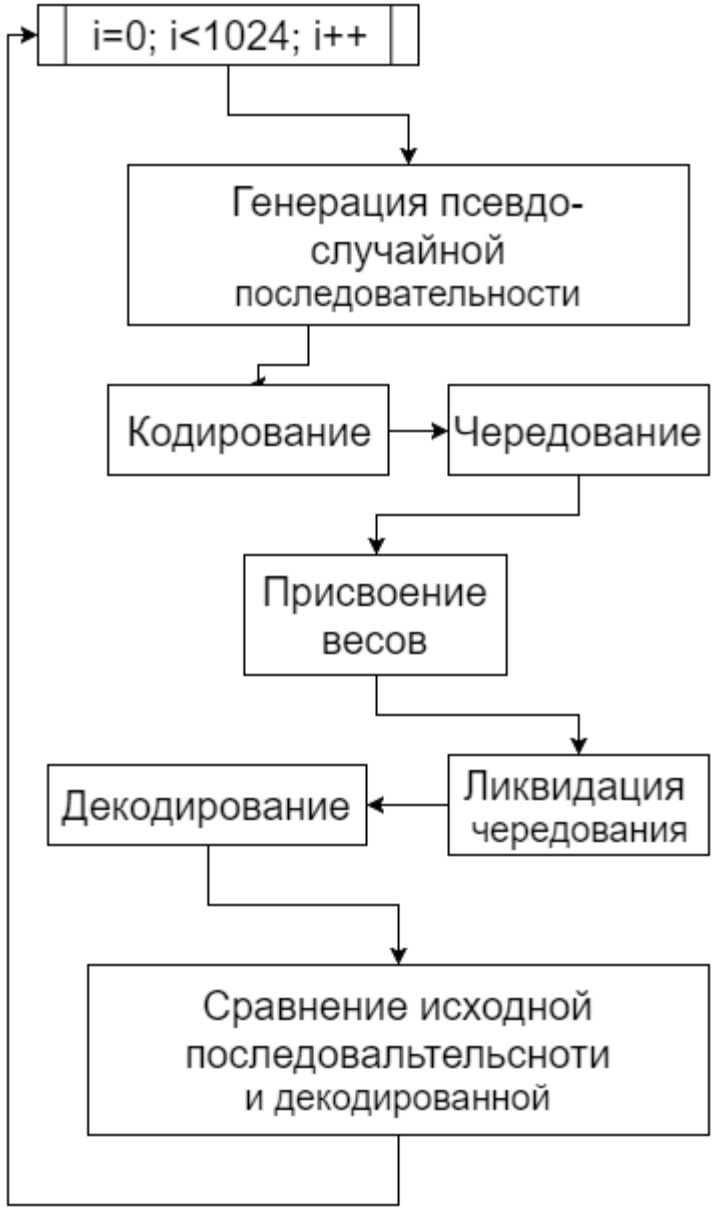
- Определение функции кодека в коде прошивки;
- Тестирование работоспособности дизассемблированного кодека;
- Анализ структуры кодека и его составляющих:



Разработка модулей кодека на языке Си

- Реверс инжиниринг
- Спецификация модулей
  - Работа с общей памятью посредством передачи указателей в модули
  - Используемые внешние библиотеки (math.h, stdlib.h)
- Оформление в виде библиотеки

Тестирование реализации на языке Си

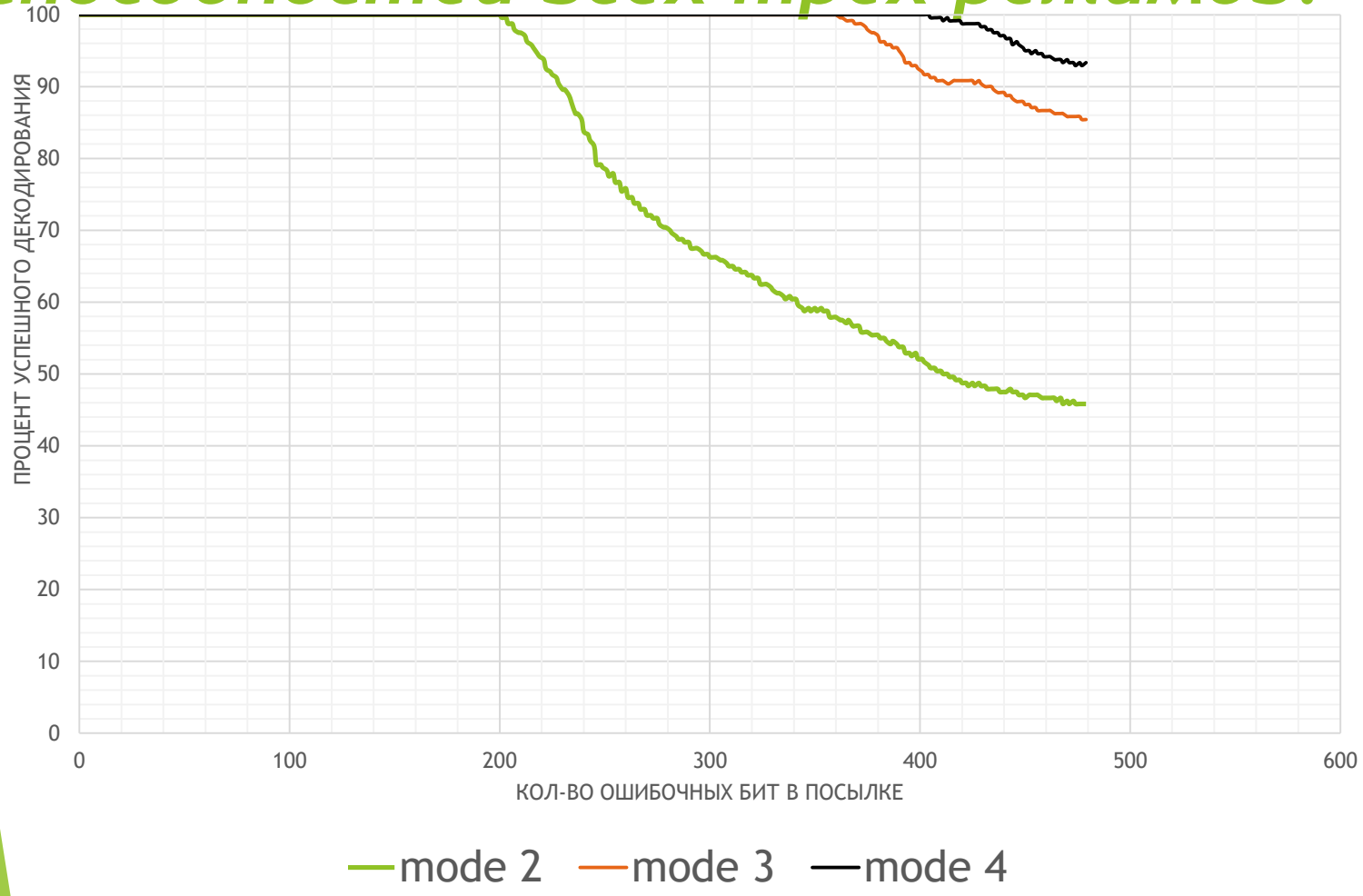


- Проверить работоспособность;
- Проверить совместимость разработанного кодека и кодека с прошивки.

Модернизация кодека

- Минимальное вмешательство во внутреннюю структуру
- Кодирование тремя битами

Тестирование декодирующих способностей всех трех режимов.



Предельное кол-во ошибок на сообщение:

Mode 2: 201 (13,9%)
Mode 3: 360 (21,4%)
Mode 4: 400 (20,8%).

Результаты разработки:

- Дизассемблирована прошивка
- Определен и проанализирован кодек, скрытый в прошивке
- Добавлен промежуточный режим кодирования
- Создана библиотека кодека
- Проведен сравнительный анализ режимов кодирования

спасибо за внимание!