Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГАОУ ВО «ЮФУ»)

Инженерно-технологическая Академия

Институт компьютерных технологий и информационной безопасности

Кафедра Систем Автоматизированного Проектирования

им. В. М. Курейчика

Выполнил

студент КТбо2-4 \_\_\_\_\_\_\_\_\_\_\_\_\_ А. А. Воронов

Принял

доцент каф. ИБТКС, к. т. н. \_\_\_\_\_\_\_\_\_\_\_\_\_ Д. А. Петров

Таганрог 2024

ЛАБОРАТОРНАЯ РАБОТА №3

**на тему: «Скремблирование речевого сигнала»**

по дисциплине «Безопасность информационных технологий»

Содержание

[Введение 3](#_Toc181027116)

[1 ПРАКТИЧЕСКАЯ ЧАСТЬ 4](#_Toc181027117)

[2 КОНТРОЛЬНЫЕ ВОПРОСЫ 6](#_Toc181027118)

[2.1 Какие способы шифрации речевых сигналов вы знаете. 6](#_Toc181027119)

[2.2 Чем отличается скремблирование речевого сигнала от метода шифрования 6](#_Toc181027120)

[2.3 Какие методы скремблирования вы знаете. 6](#_Toc181027121)

[2.4 Расскажите о достоинствах и недостатках различных методов скремблирования. 6](#_Toc181027122)

[2.5 Какую частотную полосу занимает речевой сигнал. 7](#_Toc181027123)

[2.6 Какая допустимая задержка для скремблированного сигнала. 7](#_Toc181027124)

[2.7 Напишите выражение для спектра мощности Фурье. 7](#_Toc181027125)

[ЗАКЛЮЧЕНИЕ 8](#_Toc181027126)

Введение

Цель данной лабораторной работы – изучение функционирования программной модели скремблера. Программа позволяет выполнять скремблирование речевых сигналов разными способами: во временной и частотной областях, а также проводить сравнительный анализ для определения наиболее эффективного метода (наименее узнаваемого сигнала). В ходе работы также исследуется, как разные параметры скремблирования, такие как длина окна сигнала, количество блоков и тип перестановки блоков, влияют на конечный сигнал.

Порядок выполнения работы:

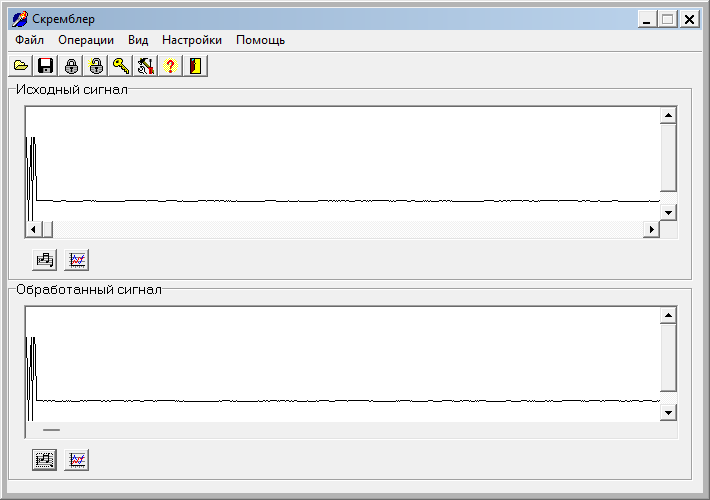
* изучение теоретического материала и рекомендованной литературы
* выполнение лабораторного задания
* ответы на контрольные вопросы

# ПРАКТИЧЕСКАЯ ЧАСТЬ

Таблица 1. Результаты скремблирования, 16 блоков

|  |  |  |
| --- | --- | --- |
| Тип скремблирования | Размер окна | Разборчивость, % |
| Перестановка во времени | 512 | 70 |
| 1024 | 60 |
| 2048 | 80 |
| 4096 | 50 |
| Временная инверсия | 512 | 80 |
| 1024 | 50 |
| 2048 | 20 |
| 4096 | 10 |
| Спектральная перестановка | 512 | 10 |
| 1024 | 75 |
| 2048 | 70 |
| 4096 | 80 |
| Спектральная инверсия | 512 | 75 |
| 1024 | 30 |
| 2048 | 10 |
| 4096 | 10 |

Графики всех обработанных сигналов (рисунок 1) практически не отличаются друг от друга и представляют собой прямую линию с малой амплитудой.

1.  — График сигнала

# КОНТРОЛЬНЫЕ ВОПРОСЫ

## 2.1 Какие способы шифрации речевых сигналов вы знаете.

Способы шифрации речевых сигналов: скремблирование, дискретизация речи.

## 2.2 Чем отличается скремблирование речевого сигнала от метода шифрования

Скремблирование — изменение исходного сигнала так, чтобы новый сигнал занимал такую же полосу частот, что и исходный сигнал, но был неразборчив;

Дискретизация речи — речь кодируются в цифровой поток данных, который смешивается со случайной последовательностью выбранного генератора.

## 2.3 Какие методы скремблирования вы знаете.

* перестановка во времени;
* временная инверсия;
* спектральная перестановка;
* спектральная инверсия.

## 2.4 Расскажите о достоинствах и недостатках различных методов скремблирования.

Перестановка во времени:

* достоинства: простота реализации, защита от простых атак.
* недостатки: требует точной синхронизации отправителя и получателя, уязвим к более сложным атакам.

Временная инверсия:

* достоинства: более безопасный, сложнее анализировать.
* недостатки: чем дольше инверсия, тем менее понятны данные.

Спектральная перестановка:

* достоинства: более безопасный, сложно восстановить исходный сигнал.
* недостатки: сложно реализовать, эффективность зависит от алгоритма перестановки.

Спектральная инверсия:

* достоинства: сложнее анализировать сигнал и декодировать его.
* недостатки: требует точных расчётов и в процессе инверсии может быть потеряна часть информации.

## 2.5 Какую частотную полосу занимает речевой сигнал.

Речевой сигнал занимает полосу частот в 300-3200 Гц. Таким образом гарантируется высокая разборчивость речи.

## 2.6 Какая допустимая задержка для скремблированного сигнала.

Допустимая задержка для программной модели скремблера равна 250 мс.

## 2.7 Напишите выражение для спектра мощности Фурье.

Выражение для спектра мощности Фурье выглядит таким образом:

# ЗАКЛЮЧЕНИЕ

В ходе данной лабораторной работы была достигнута цель исследования работы программной модели скремблера для речевых сигналов. В рамках работы были реализованы и протестированы различные методы скремблирования, включая скремблирование во временной и частотной областях, а также проведен сравнительный анализ эффективности этих методов в контексте изменения узнаваемости исходного сигнала. Были исследованы влияния различных параметров, таких как длина окна, количество блоков и тип перестановки, на выходной сигнал.