МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

| Доцент, канд. техн. наук | | А. В. Окатов |
|---|---|---|
| должность, уч. степень, звание | подпись, дата | инициалы, фамилия |

# ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

# СКРЕМБЛИРОВАНИЕ МЕТОДОМ ЧАСТОТНОЙ ИНВЕРСИИ

по курсу: ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

| СТУДЕНТ ГР. № 5912 | | М. С. Фомин |
|---|---|---|
| | подпись, дата | инициалы, фамилия |

Санкт-Петербург 2022

## 1. Цель работы:

Произвести и исследовать скремблирование информационных сигналов методом частотной инверсии.

## 2. Выполнение работы:

**1)** Сформировать модельный временной информационный сигнал, содержащий по 4 гармонических колебания *с различающимися амплитудами и частотами* из диапазона частот от $F_{min}$ = 300 Гц до $F_{max}$ = 3400 Гц. Построить график сигнала и визуально попробовать оценить его основные частотно-временные свойства.

В качестве составляющих модельного сигнала были взяты 4 гармонических колебания вида $S = A * \cos(2 * \pi * F_i + \theta)$ со следующими параметрами:

**Частоты колебаний:**
F1 = 315;
F2 = 721;
F3 = 1658;
F4 = 3207;

**Амплитуды колебаний:**
A1 = 2;
A2 = 4;
A3 = 3;
A4 = 1;

Итоговый сигнал $S = S_1 + S_2 + S_3 + S_4$

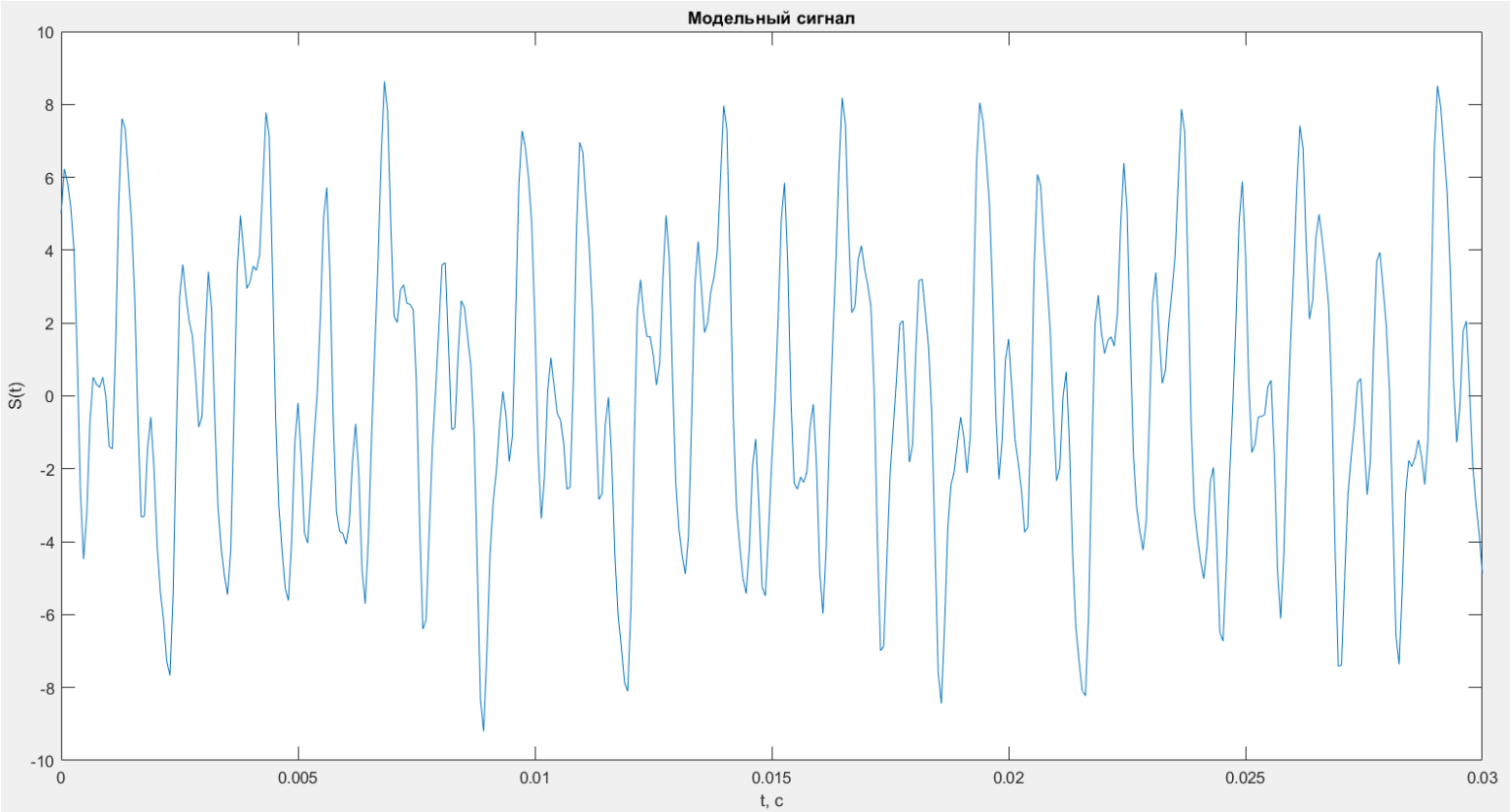


*Рис. 1 – График сигнала S*

Посмотрев на получившийся сигнал (рис. 1), можно сделать вывод, что он не похож на простую гармоническую кривую. В нем присутствуют резкие скачки и спады, а количество различающихся по высоте пиков говорит о том, что у сигнала есть несколько амплитудных составляющих (то есть сигнал может являться суммой двух и более гармонических сигналов).

**2)** Выполнить БПФ модельного сигнала, построить график спектра модельного временного сигнала и оценить соответствие полученного результата частотно-временным параметрам модели, которая была ранее задана во временной области.

Для анализа полученного сигнала применим преобразование Фурье и выведем спектр модельного сигнала.

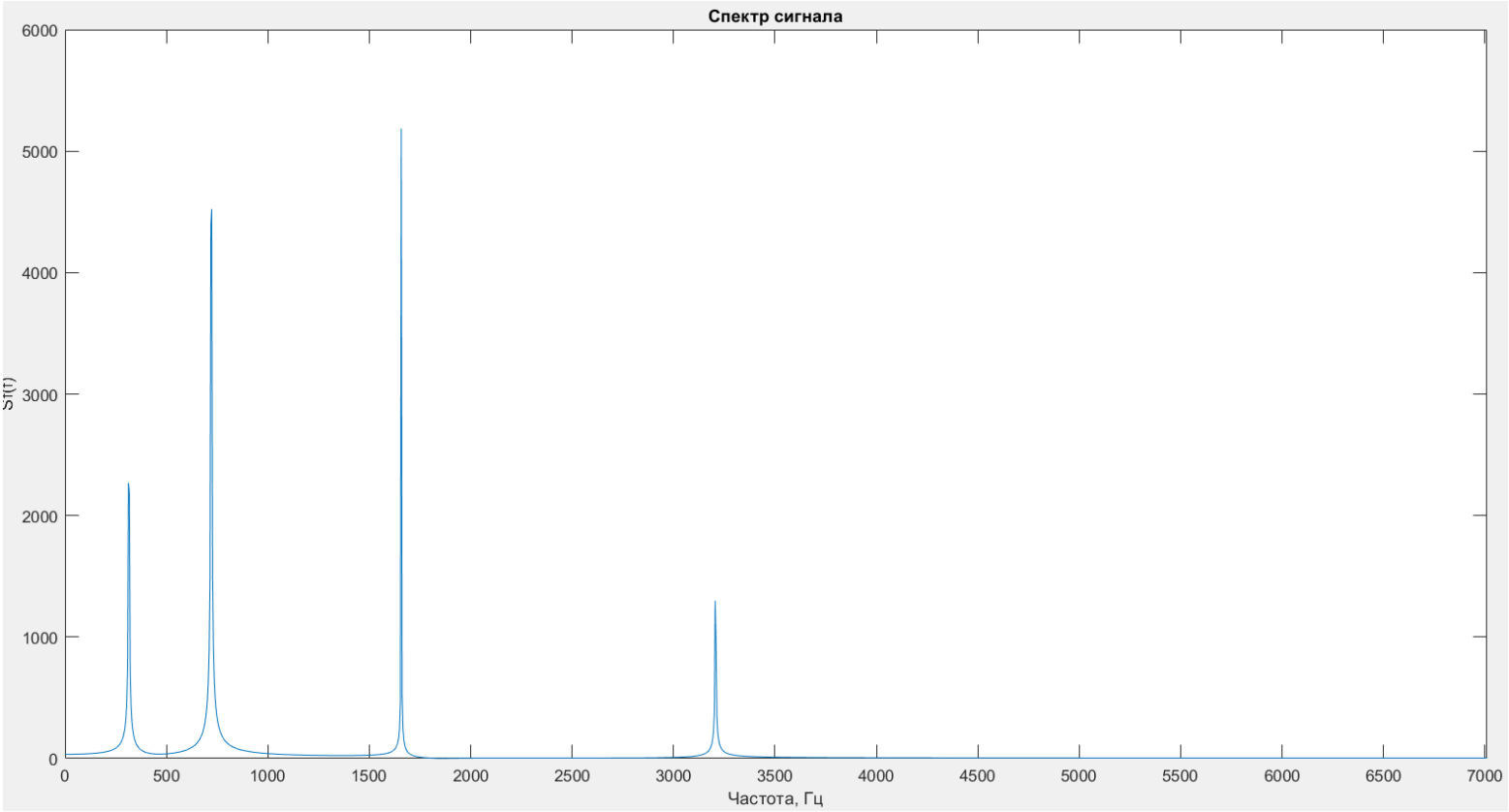


*Рис. 2 – График спектра сигнала S*

БПФ - это переход из временной области в частотную, где ось x – частота, а ось y – спектральная плотность сигнала.

Посмотрев на действительную часть амплитудного спектра (рис. 2), можно смело утверждать, что модельный сигнал S состоит из четырех различных гармоник с разными частотами и амплитудами, соответствующих заданным нами в начале выполнения работы.

Выполнив ОБПФ, мы получим исходный модельный сигнал (рис. 3).

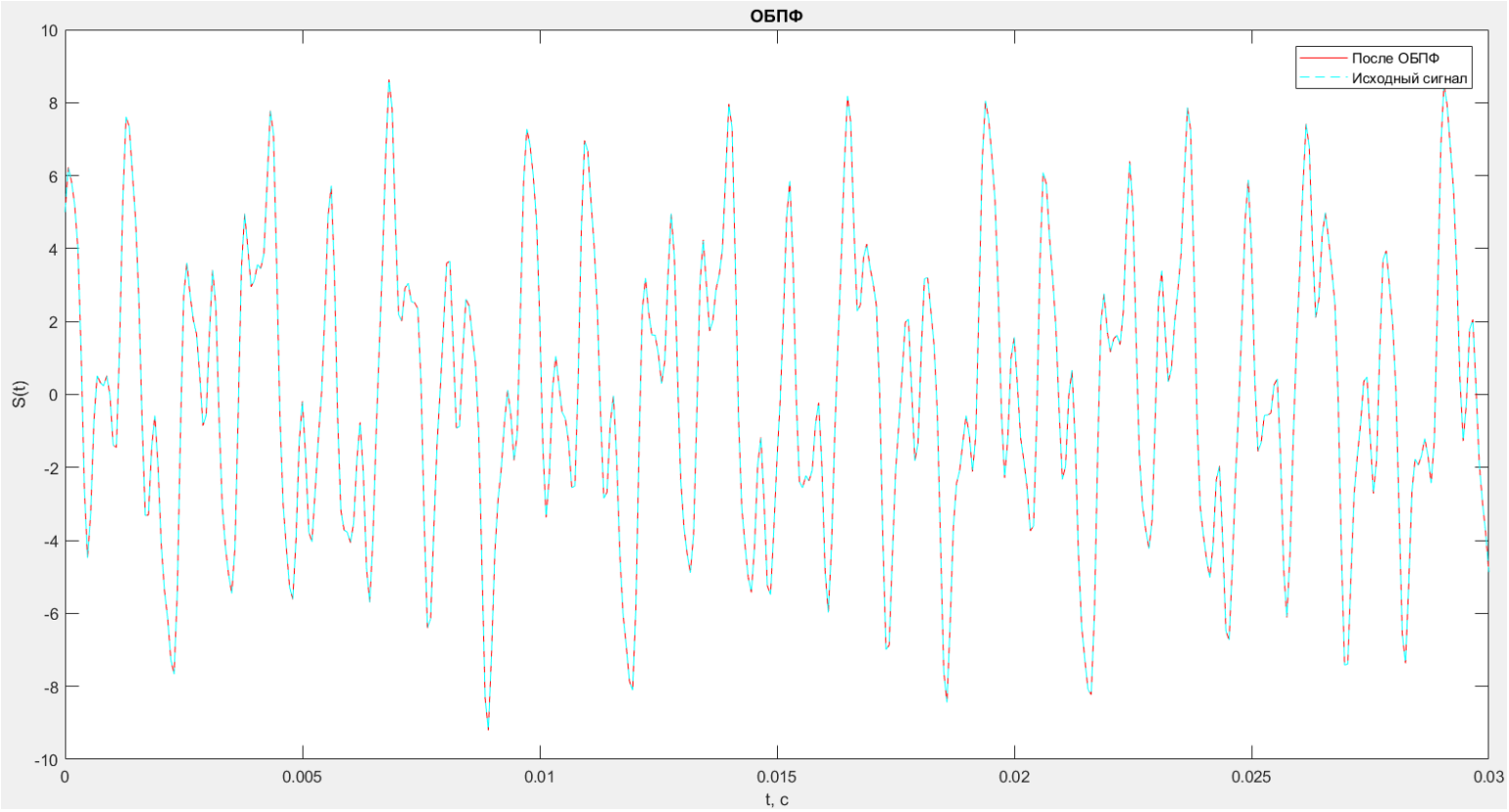


*Рис. 3 – Сравнение восстановленного и изначального сигналов*

**3)** Выполнить скремблирование модельного сигнала методом частотной инверсии. Частоту скремблирования $F_{скр}$ выбрать равной *не меньше*, чем $F_{min} + F_{max}$. Для иллюстрации процессов выполнить БПФ скремблированного сигнала, построить график соответствующего спектра. Объяснить полученные результаты по как смыслу скремблирования, так и количественно, показать, что (и почему) это дает для закрытия информации от посторонних.

Чтобы выполнить скремблирование сигнала S методом частотной инверсии, требуется умножить данный сигнал на другой сигнал вида $A * \cos(2 * \pi * F_{ск} + \theta)$. Частоту скремблирующего сигнала возьмем равной сумме минимальной и максимальной частот стандартного аналогового телефонного канала связи: $F_{ск} = F_{min} + F_{max} = 3700$ Гц

В основе данного алгоритма скремблирования лежит общеизвестная тригонометрическая формула:

$$\cos(x) * \cos(y) = \frac{\cos(x-y)+\cos(x+y)}{2}$$

Из формулы видно, что в результате умножения *cos*(*x*) на *cos*(*y*) получаем сумму двух составляющих: разностную *cos*(*x* - *y*) и суммарную *cos*(*x* + *y*). То есть полезное колебание *cos(x)* «расщепилось» на две составляющие, существенно различные по спектральному составу. В правой части формулы

в слагаемом *cos*(*x* - *y*) из аргумента x (полезный сигнал) вычитается аргумент y (вспомогательный – «скремблирующий» сигнал), в итоге для него мы получаем разность частотных составляющих. В слагаемом *cos*(*x* + *y*) получаем сумму частотных составляющих.

Полученная сумма представляет собой скремблированный исходный сигнал.

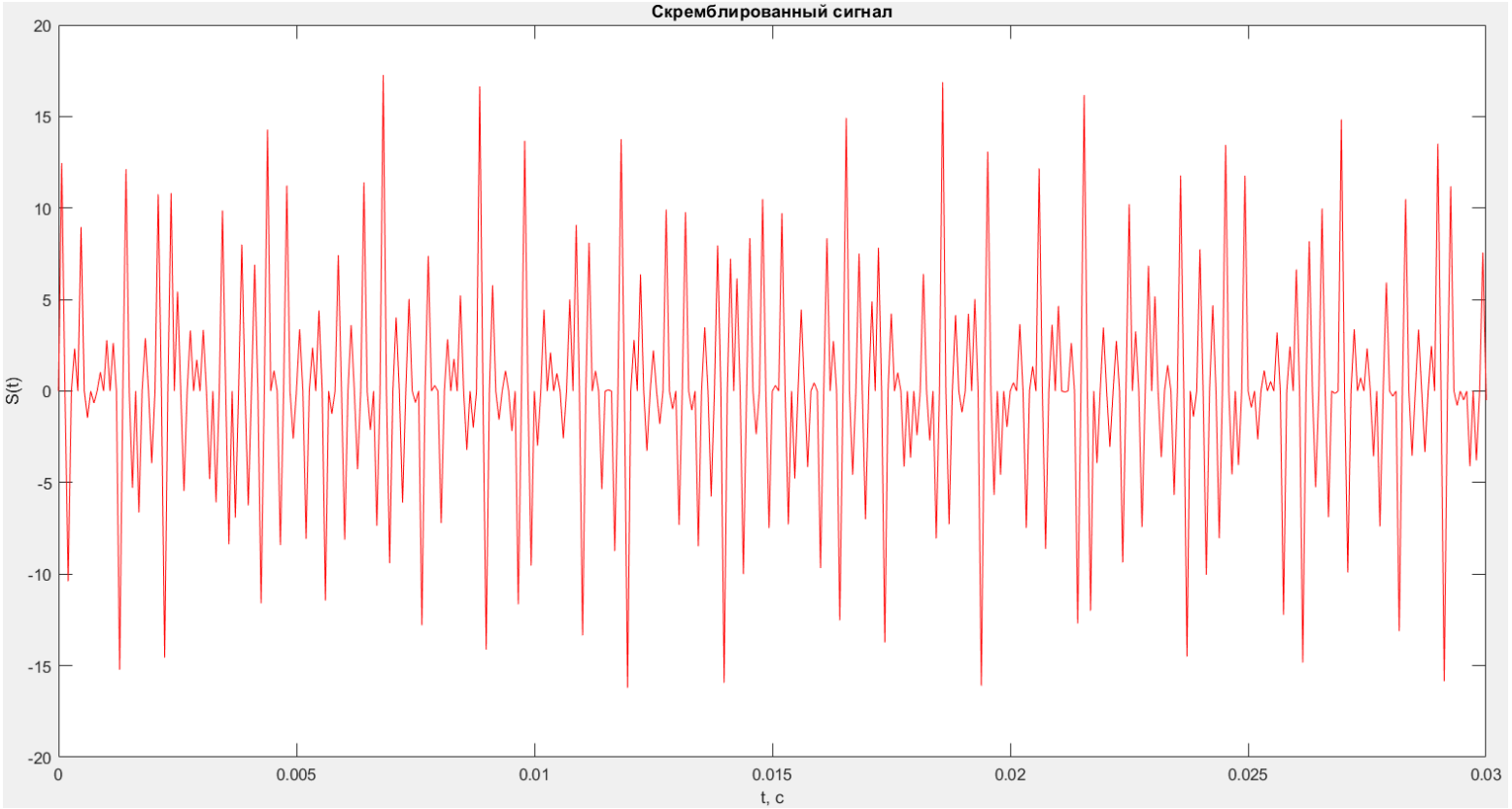


*Рис. 4 – Сигнал после скремблирования*

Как видно из графика (рис. 4), после скремблирования существенно изменилась форма сигнала: увеличилось количество различных по амплитуде пиков, а также увеличилась частота скачков и спадов (в сигнале появились гармоники с более высокими частотами). То есть мы достигли следующего результата: скремблированный сигнал визуально не похож на модельный. Остаётся оценить качество закрытия информации и разобраться в деталях алгоритма.

Применив БПФ к данному сигналу, получаем:

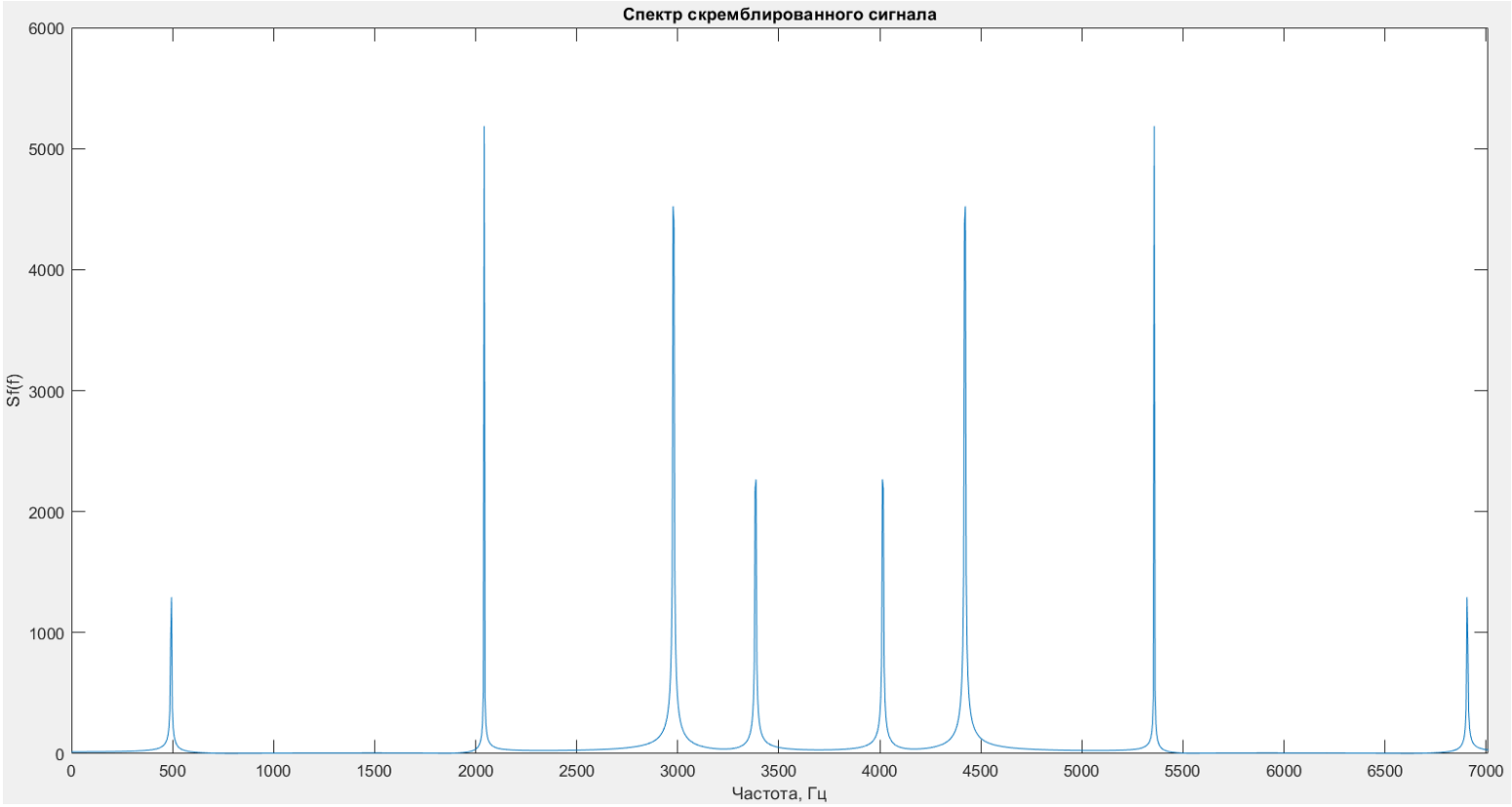


*Рис. 5 – Спектр скремблированного сигнала*

Исследуя данный график (рис. 5), можно сделать вывод, что левые четыре пика являются зеркальным отражением правых (ранее – исходных) четырех пиков относительно частоты скремблирования $F_{\text{ск}} = 3700$ Гц.

Это происходит из-за применения тригонометрической формулы, приведенной выше:

**Разностная составляющая:**

- $F_{\text{ск}} - F_4 = 3700 - 3207 = 493$ Гц
- $F_{\text{ск}} - F_3 = 3700 - 1658 = 2042$ Гц
- $F_{\text{ск}} - F_2 = 3700 - 721 = 2979$ Гц
- $F_{\text{ск}} - F_1 = 3700 - 315 = 3385$ Гц

**Суммарная составляющая:**

- $F_{\text{ск}} + F_4 = 3700 + 3207 = 6907$ Гц
- $F_{\text{ск}} + F_3 = 3700 + 1658 = 5358$ Гц
- $F_{\text{ск}} + F_2 = 3700 + 721 = 4421$ Гц
- $F_{\text{ск}} + F_1 = 3700 + 315 = 4015$ Гц

Если обратить внимание на разностную составляющую, то можно увидеть, что она является инверсией нашего изначального спектра (то есть низкочастотные составляющие переместились в область высоких частот и наоборот).

**4)** Выполнить полосную фильтрацию скремблированного модельного сигнала, объяснить зачем надо фильтровать скремблированный сигнал и что это дает для практики.

Но чтобы передать полученный сигнал, необходимо увеличить пропускную способность в два раза, так как у нас в два раза увеличилась частотная область. Это повлечет за собой увеличение объема передаваемых данных, а также увеличит шанс возникновения ошибок при передаче. То есть так делать не выгодно и не целесообразно, ведь результат в левой части амплитудного спектра сам по себе уже существенно отличается от модельного сигнала.

Таким образом, мы можем отфильтровать суммарную составляющую (правую часть спектра) без потери важной информации и снова уменьшить частотную полосу в 2 раза (рис. 6).

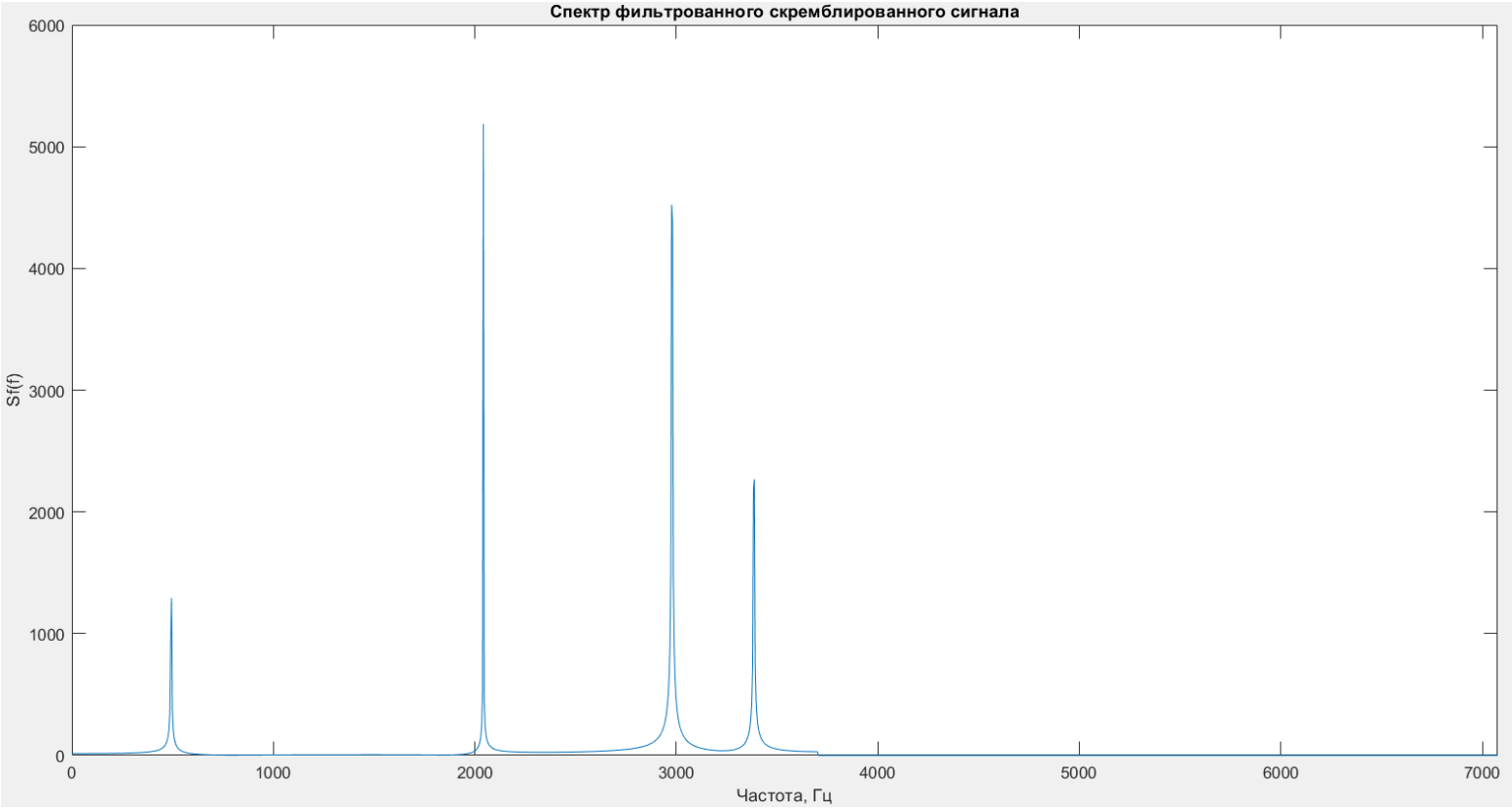


*Рис. 6 – Отфильтрованный спектр*

**5)** Выполнить обратное преобразование (на приемном конце) - дескремблирование. ***Пошагово выполнить процедуру*** дескремблирования модельного сигнала с построением соответствующих графиков, сопровождаемых необходимыми пояснениями.

Для того, чтобы получить исходный модельный сигнал, требуется повторно выполнить ту же операцию - умножить скремблированный сигнал на скремблирующий сигнал.

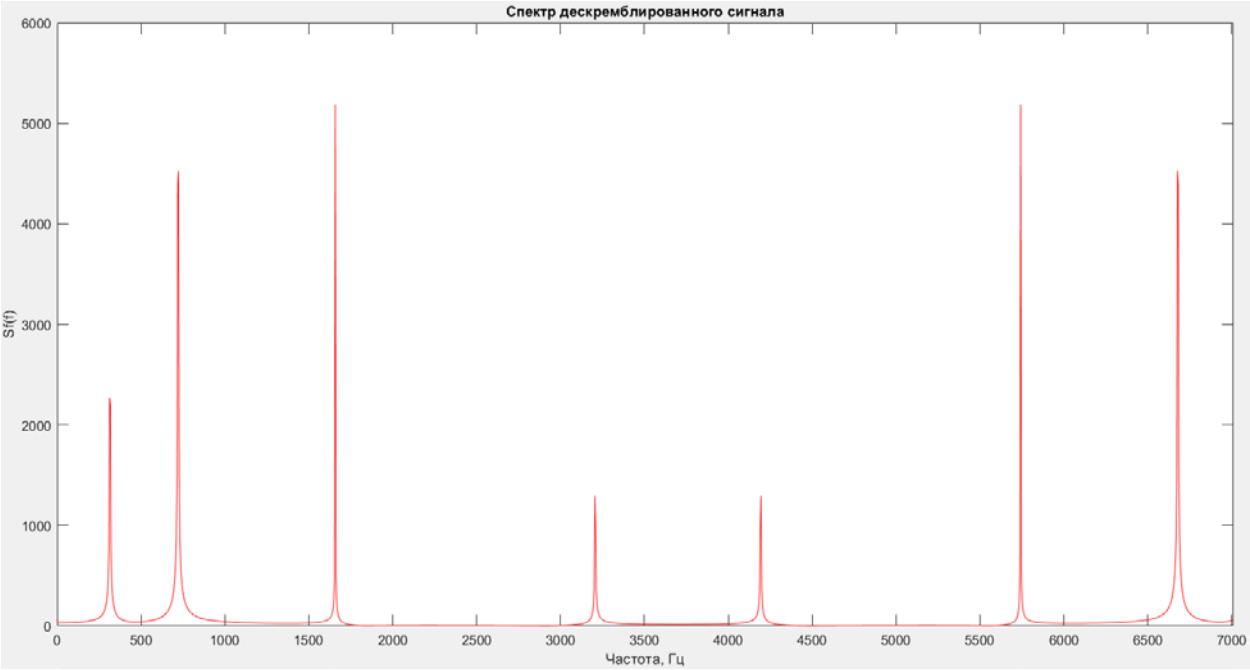


*Рис. 7 – Спектр дескремблированного сигнал без фильтрации*

Свойства такого преобразования остались те же: так как мы опять умножаем на скремблирующий сигнал, нам вновь придется отфильтровать спектр, чтобы получить спектр исходного сигнала и остаться в том же диапазоне частот (рис. 8).

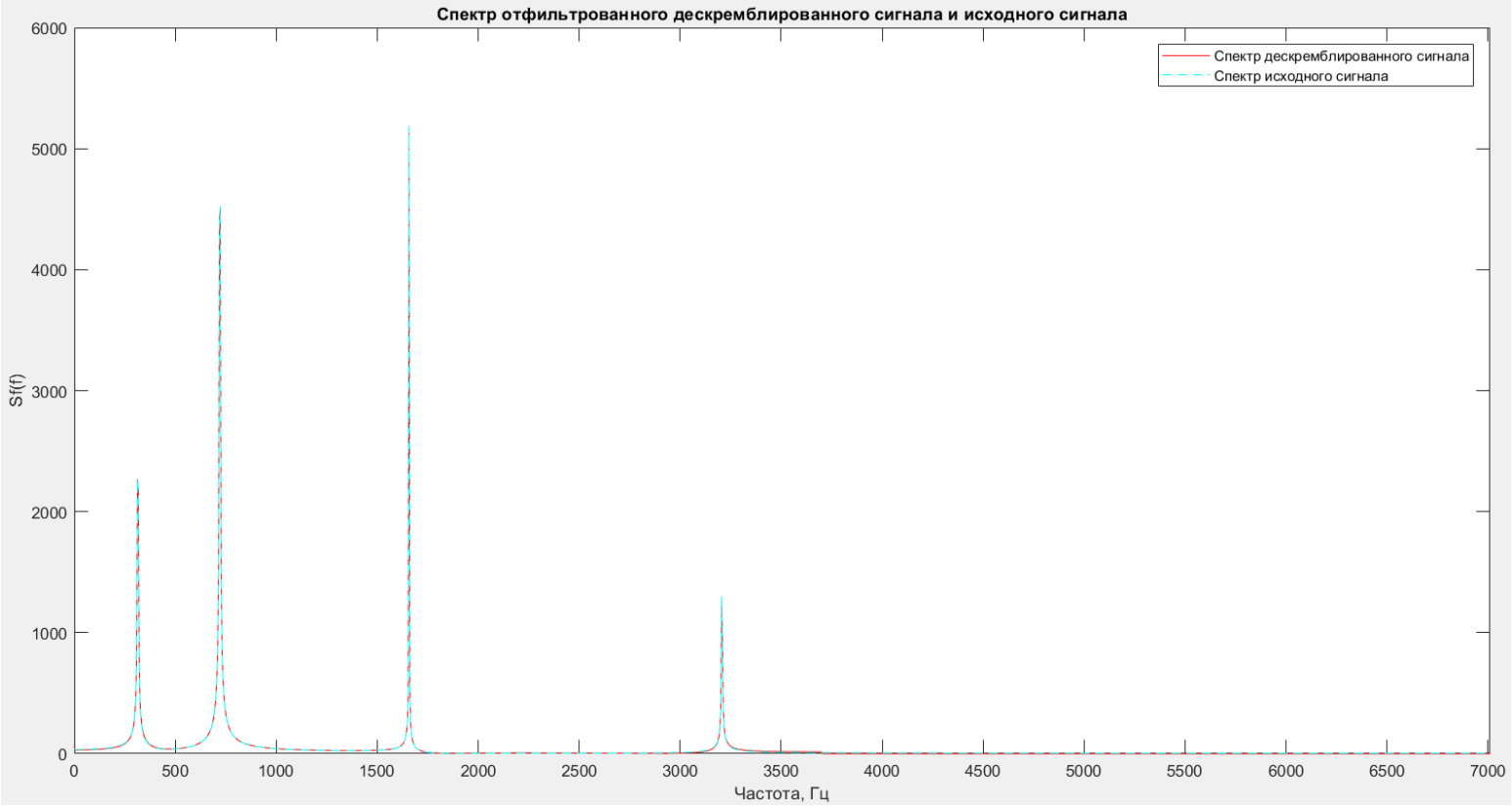


*Рис. 8 – Спектр исходного и дескремблированного сигналов*

**6)** Сопоставить графически результат дескремблирования с исходным сигналом, сделать соответствующие выводы.

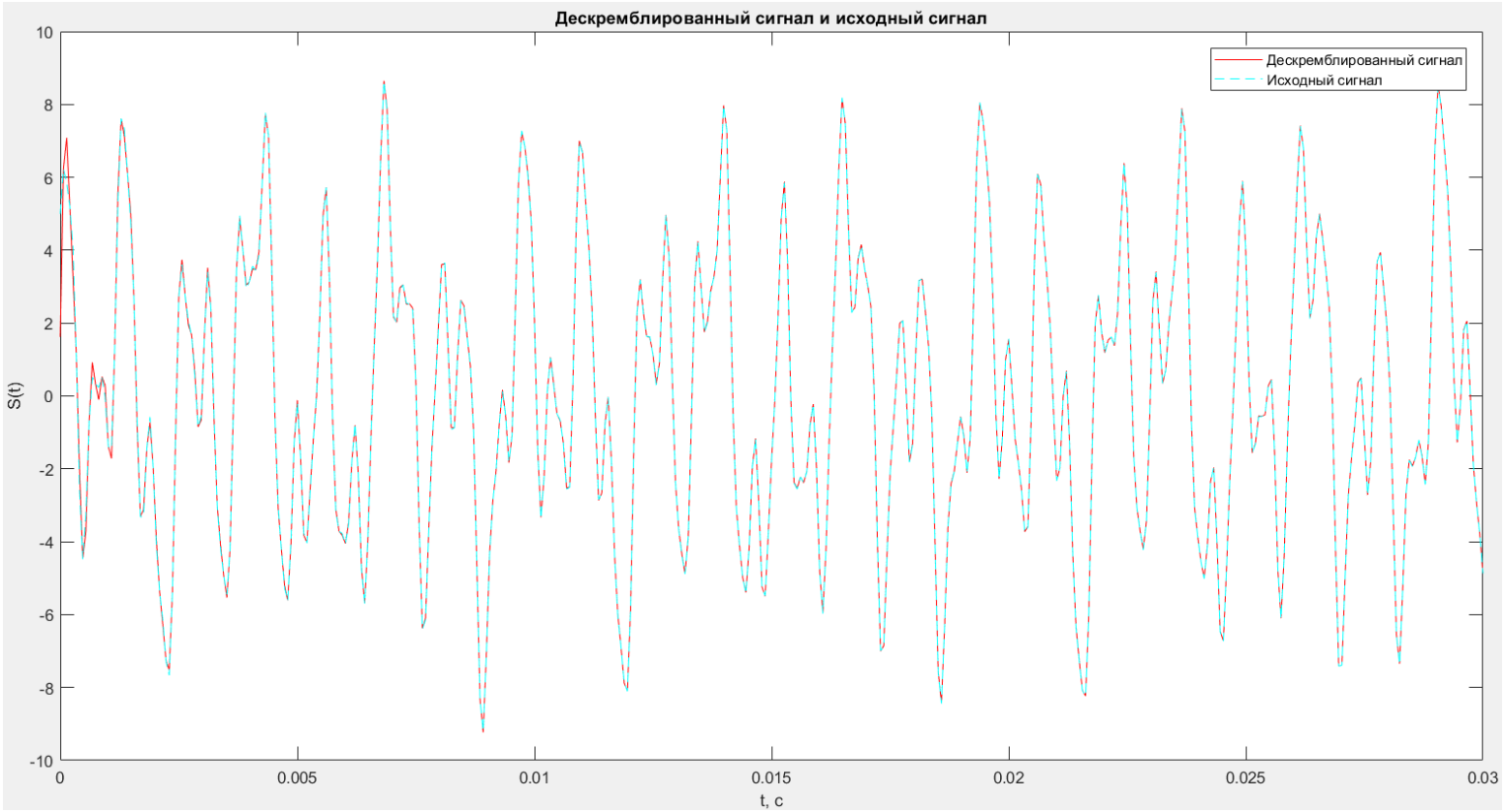


*Рис.9 – Сравнение исходного и дескремблированного сигналов*

Из графика видно (рис. 9), что в целом исходный модельный сигнал и его дескремблированная версия совпали, кроме начала.

Различие на концах вызвано тем (рис. 10), что при фильтрации мы резко обрезаем спектральную составляющую сигнала. После нескольких подобных процедур спектральная плотность сигнала получается отличной от исходной, и при восстановлении сигнал на концах искажается. Кроме того, в аналоговых приборах нет такой возможности резко обрезать ненужную часть сигнала, поэтому искажений на концах не избежать.

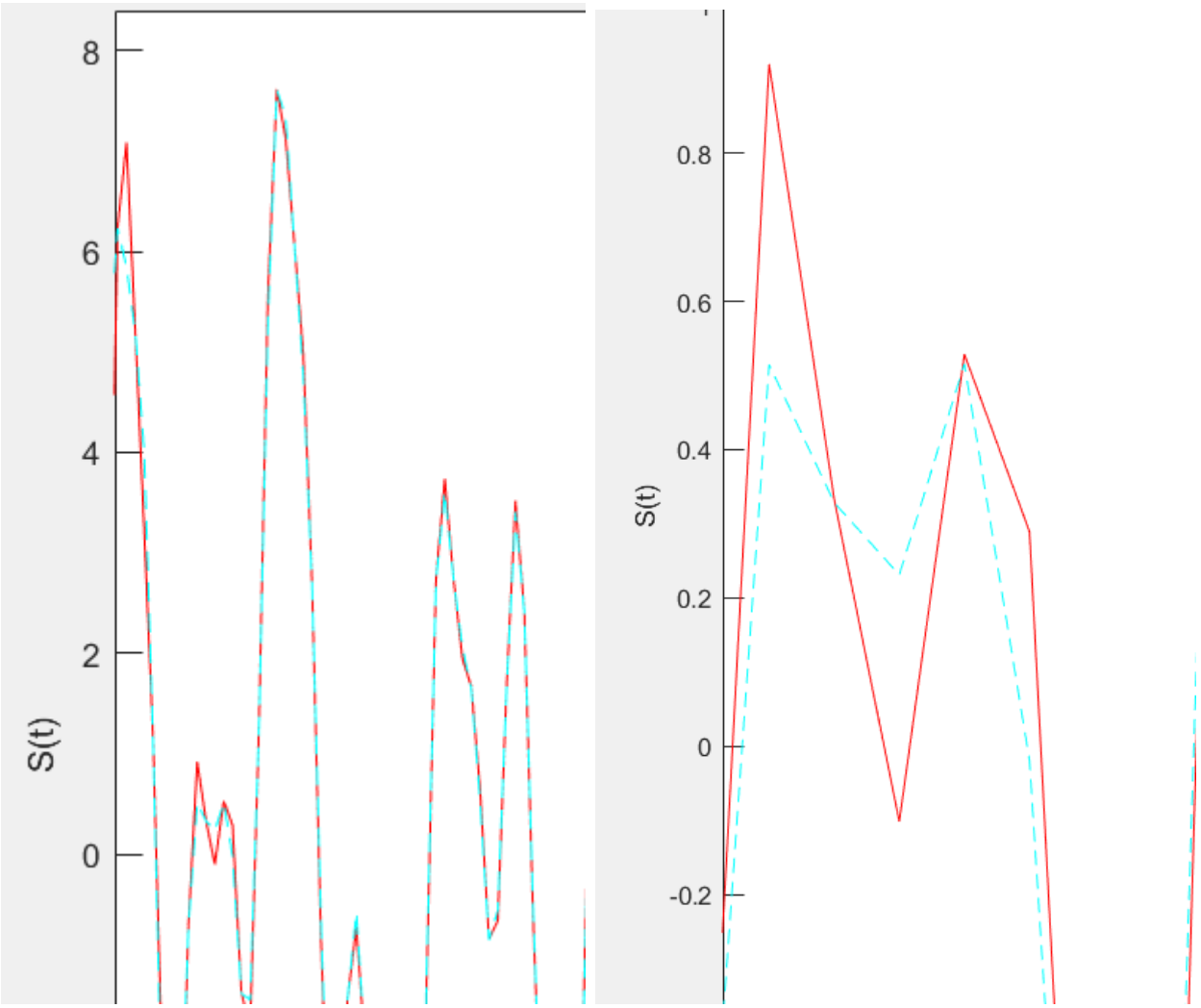


*Рис.10 – Несовпадение исходного и дескремблированного сигнала на концах*

**7)** Проанализировать влияние несовпадения начальной фазы скремблирующего и дескремблирующего сигналов (колебание с частотой скремблирования $F_{скр}$) на результат обратного преобразования.

На практике передача сигналов происходит без синхронизации, и чаще всего принятый сигнал будет сдвинут по фазе. Посмотрим, влияет ли сдвиг по фазе на восприятие информации:

Фаза скремблирующего сигнала = 0

Фаза дескремблирующего сигнала = $\frac{\pi}{2}$

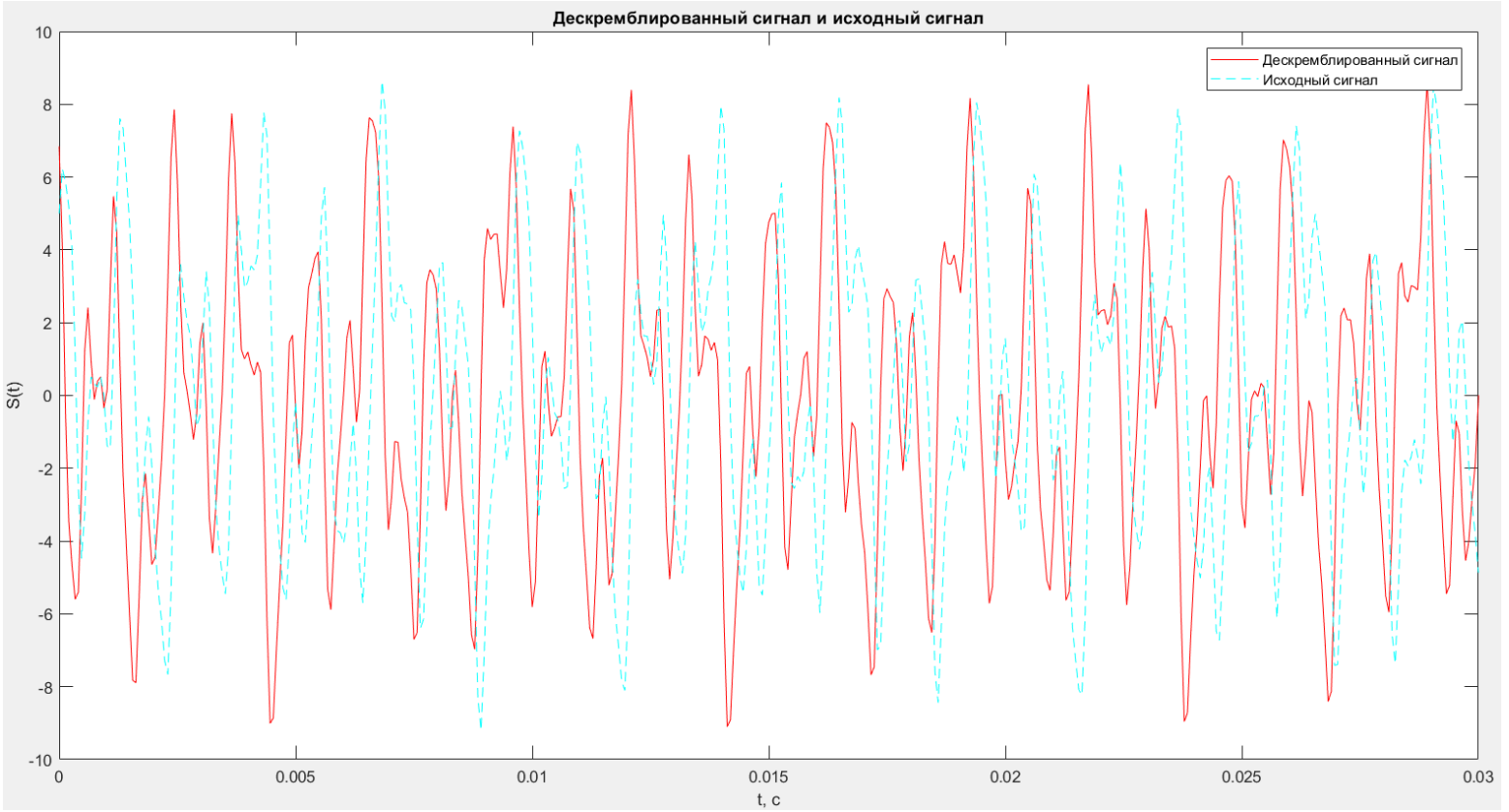


*Рис.11 – Сравнение сигналов*

Фаза скремблирующего сигнала = 0
Фаза дескремблирующего сигнала = $\pi$

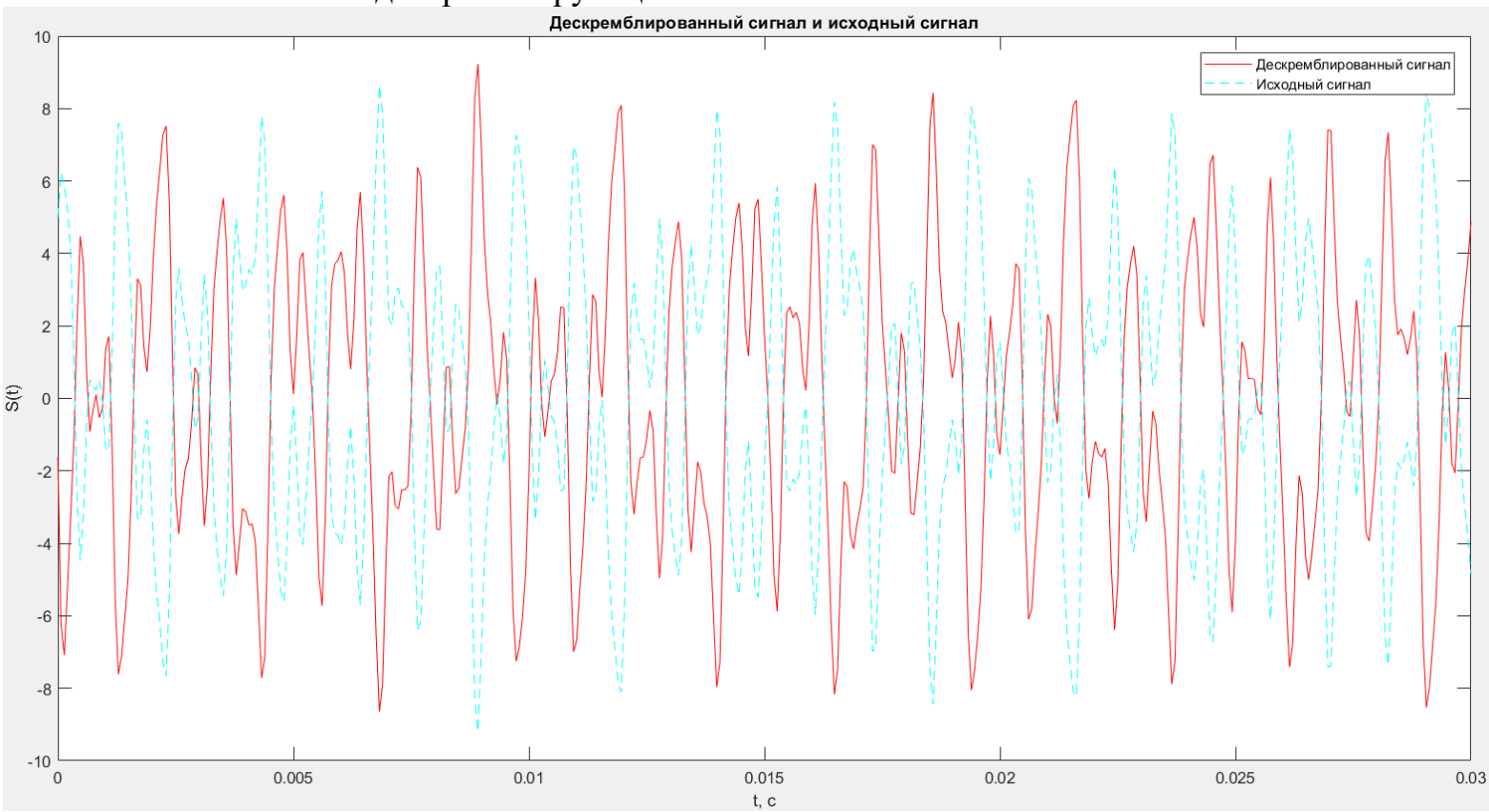


*Рис.12 – Сравнение сигналов*

Фаза скремблирующего сигнала = 0

Фаза дескремблирующего сигнала = $2 * \pi = 0$

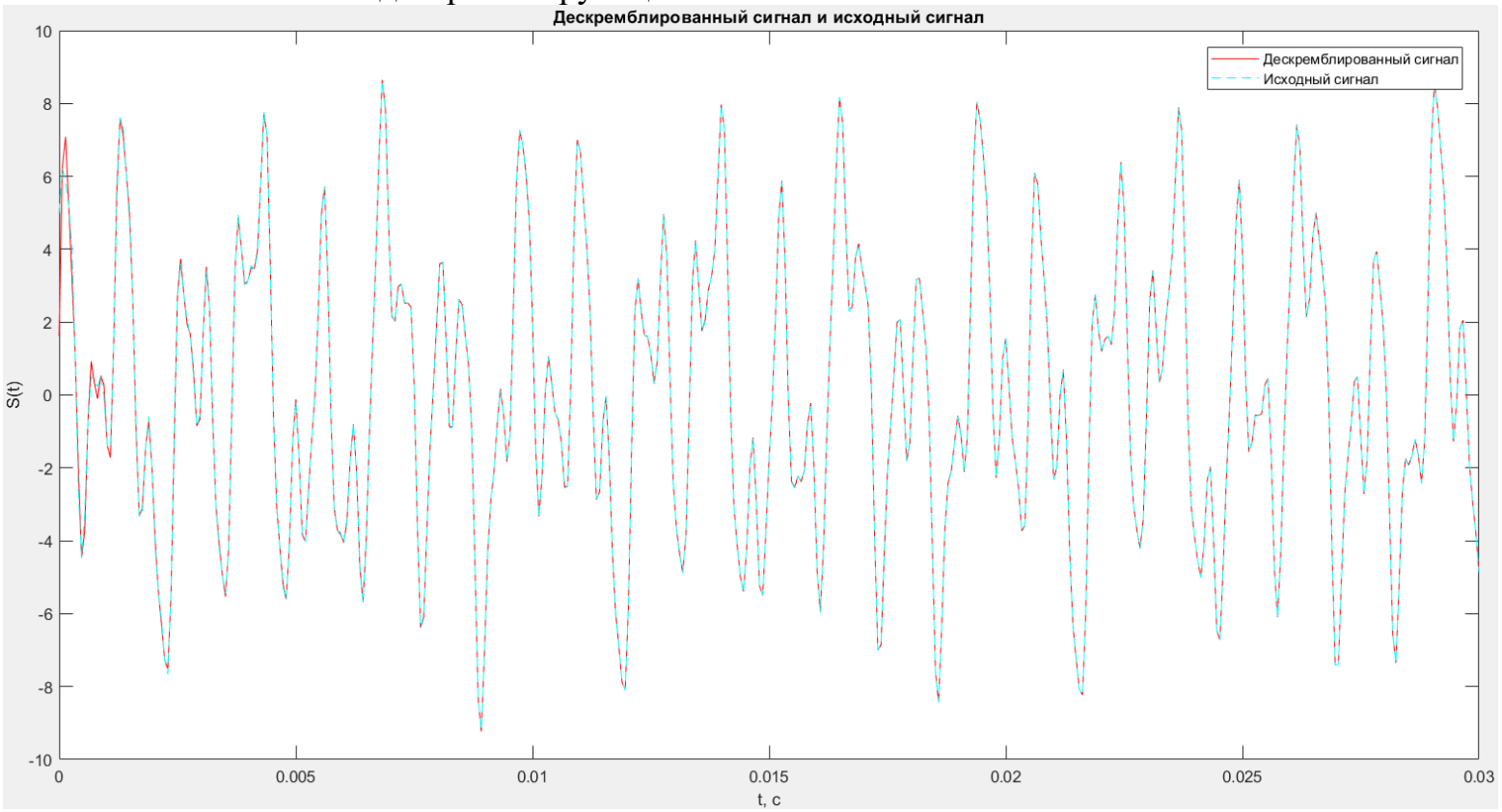


*Рис.13 – Сравнение сигналов*

По графикам видно (рис. 11, 12, 13), что несовпадение фаз влияет только на сдвиг во временной области, а не на форму сигнала. То есть сдвиг по фазе не является способом повышения защиты информации и не мешает ее восприятию.

**8)** Выполнить все эти же действия для скремблирования звукового файла, содержащего любую фразу.

Прежде чем работать с звуковым файлом, его необходимо дискретизировать. В программной среде MatLab воспользуемся командой [voice, Fd] = audioread('Sound.m4a'). В параметр Fd запишется число 44100 – стандартная частота дискретизации для современных устройств. Кроме нее, определим количество отсчетов N = length(voice(:,1)). В нашем случае N = 249856. Дискретизированный сигнал представлен на рис. 14.

Определим значение частоты скремблирования $F_s$ следующим образом: посмотрев на рис. 15, можно сделать вывод, что половина всего частотного диапазона отводится под мнимую часть спектра. Следовательно, нас интересует только область до 22050 Гц. Также заметим, что больше 90% энергии полезного сигнала сосредоточено в области до 10кГц. Значит, мы можем разделить участок от 0 до 22050 Гц пополам, и полученное значение 11025 Гц присвоить частоте скремблирования. Тогда в процессе

скремблирования спектр не вылезет за действительную область частот и не наложится на полезную часть. Таким образом $F_s = \frac{F_d}{4}$

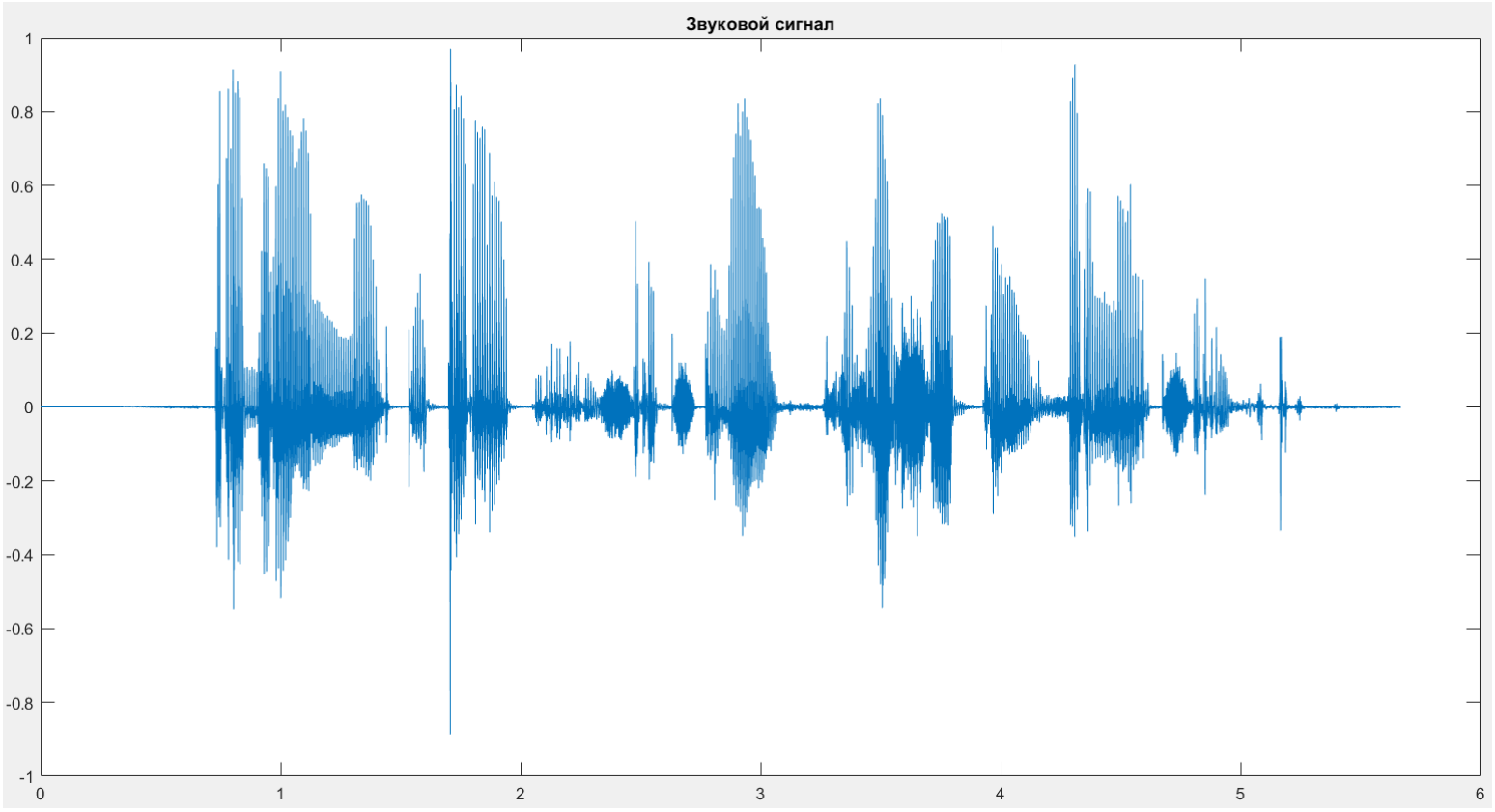


*Рис.14 – Звуковой сигнал*

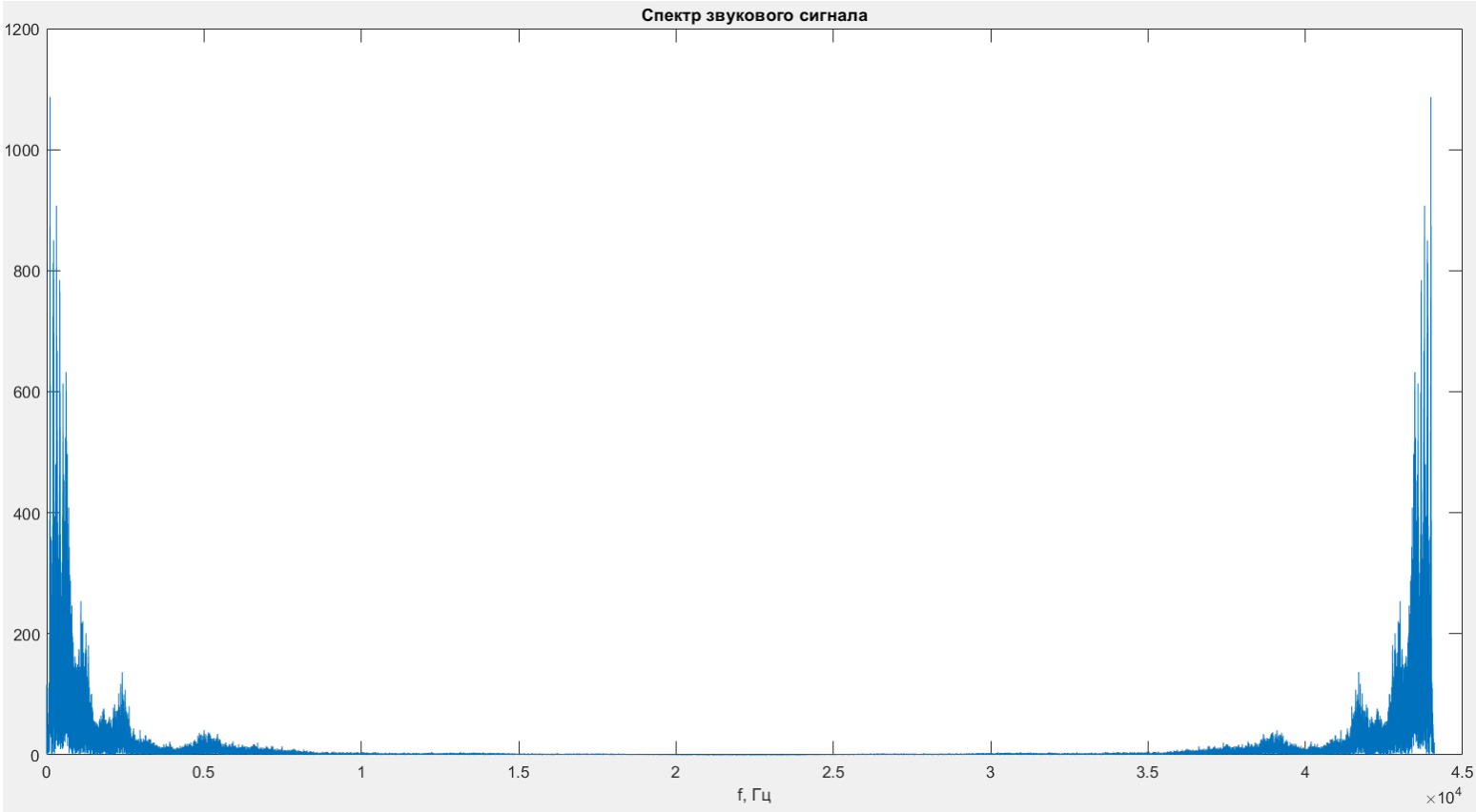

*Рис.15 – Спектр звукового сигнала*

После скремблирования сигнал будет выглядеть следующим образом (рис. 16), а его амплитудный спектр так, как показано на рис. 17.

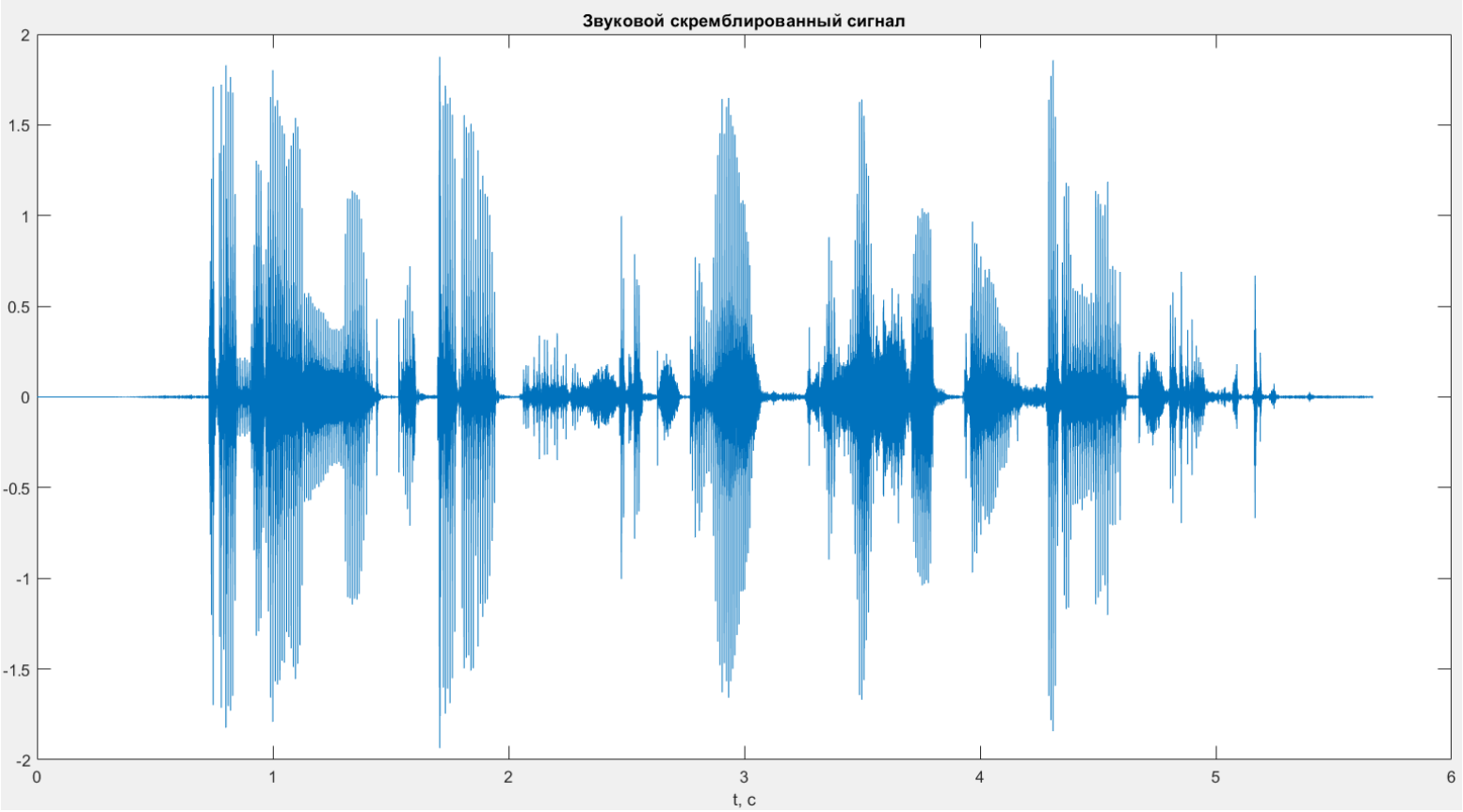


*Рис.16 – Скремблированный сигнал*

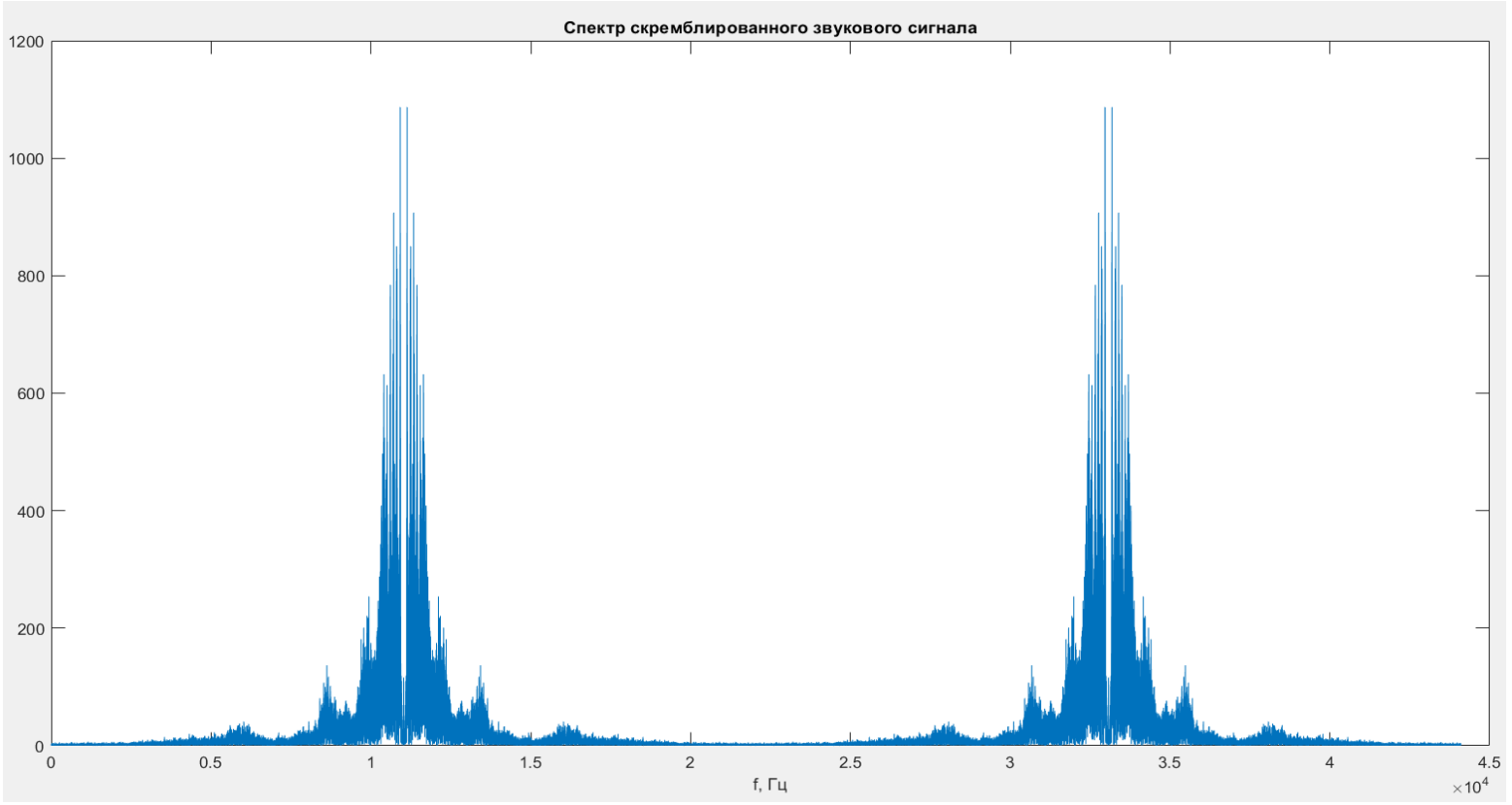


*Рис.17 – Спектр скремблированного звукового сигнала*

Произведем линейную фильтрацию скремблированного сигнала и получим следующий результат (рис. 18):

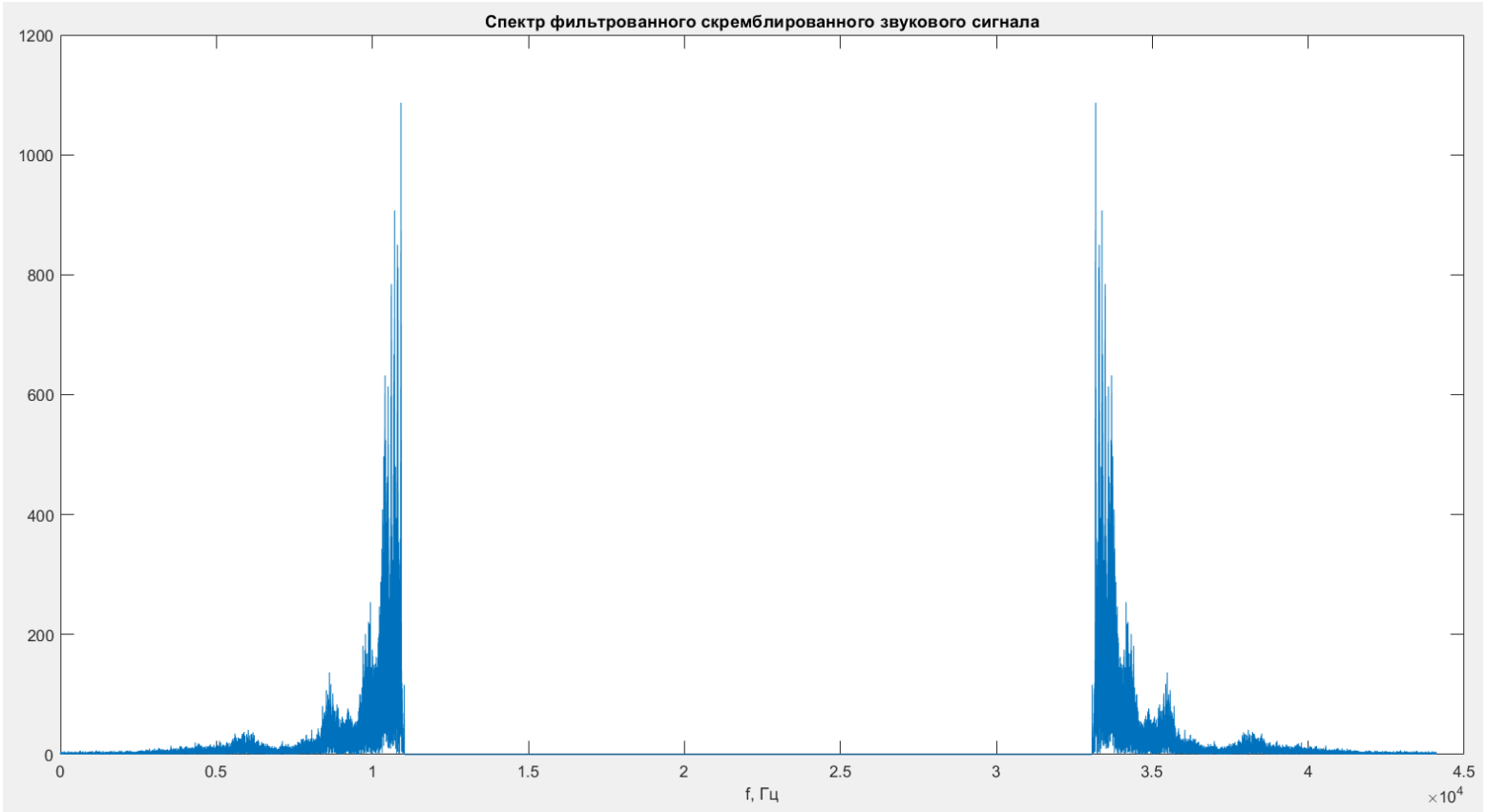


*Рис.18 – Спектр фильтрованного скремблированного звукового сигнала*

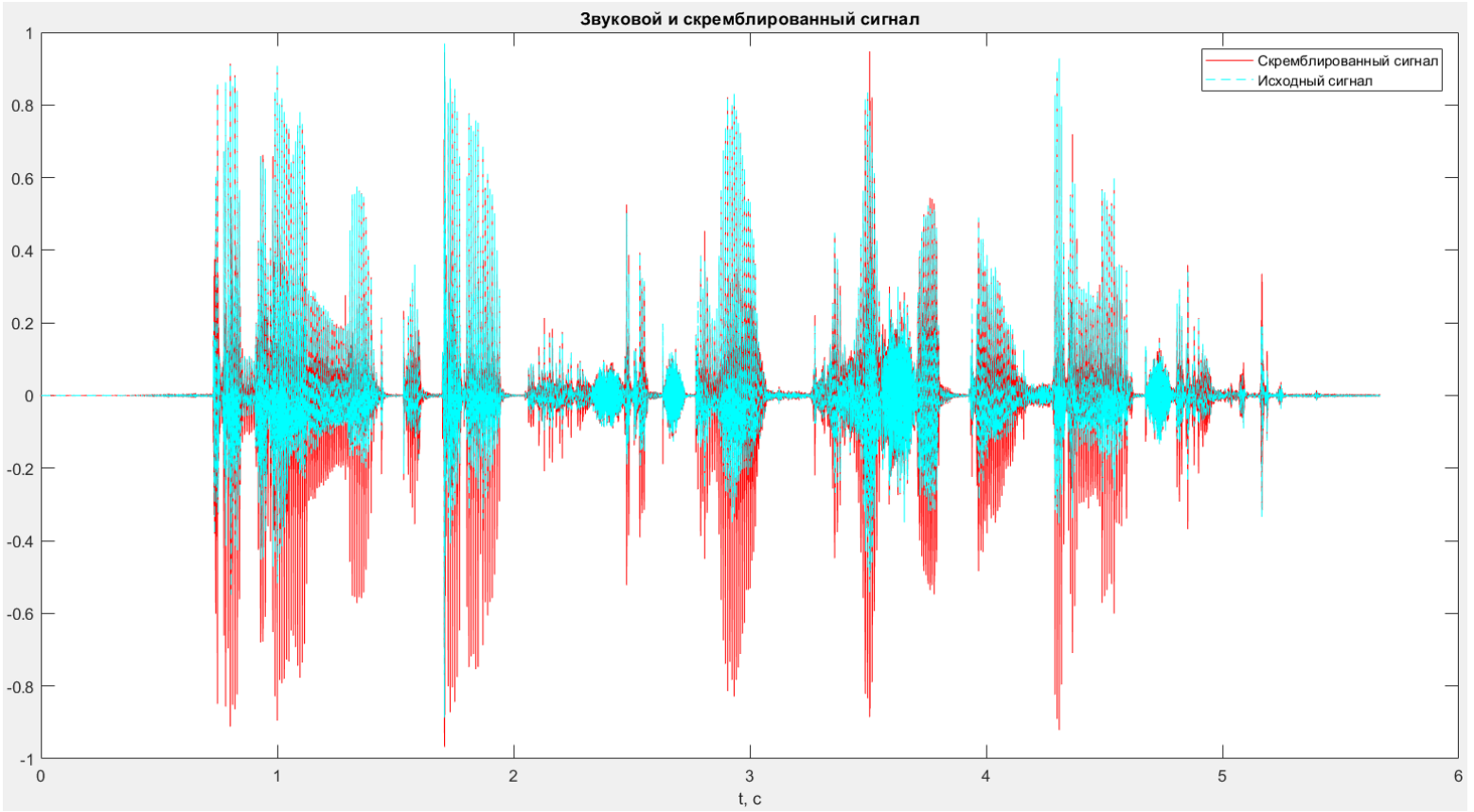


*Рис.19 – Сравнение исходного и скремблированного сигналов*

**9)** Субъективно (на слух) оценить степень разборчивости полученного результата скремблирования исходного сообщения.

Визуальное различие скремблированного и исходного сигнала представлено на рис. 19.

Скремблированный сигнал похож на скрип, половину из которого невозможно разобрать на слух. Однако остаются паузы между словами, и по интонации можно что-то разобрать. Можно сделать вывод, что скремблирование методом частотной инверсии в чистом виде не дает 100% гарантии сокрытия информации.

**10)** Выполнить обратное преобразование - дескремблирование. Убедиться в правильности восстановления исходного звукового файла.

Операция дескремблирования такая же, как и в первом опыте. Результаты работы представлены на рис. 20, 21 и 22.

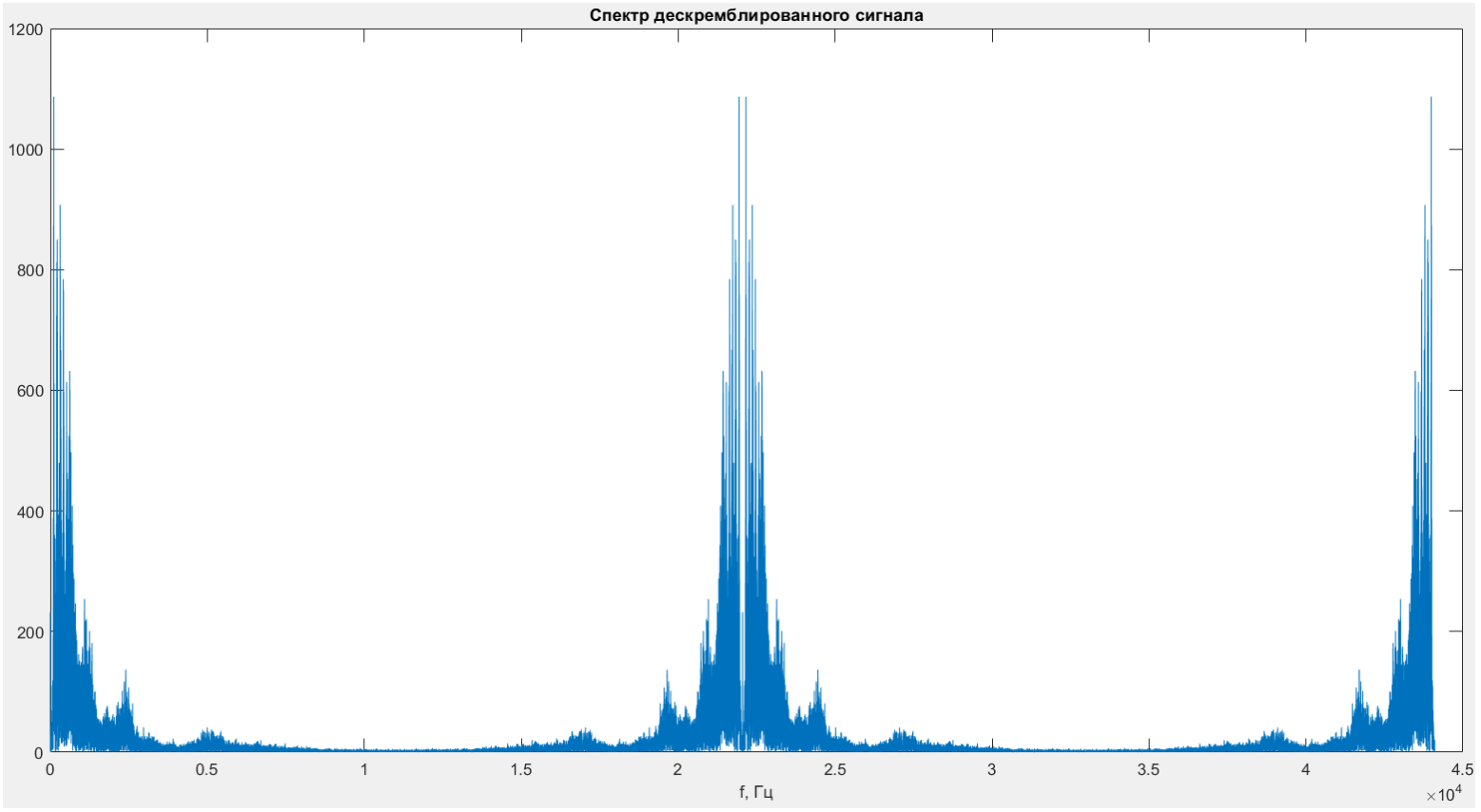


*Рис.20 – Спектр дескремблированного сигнала*

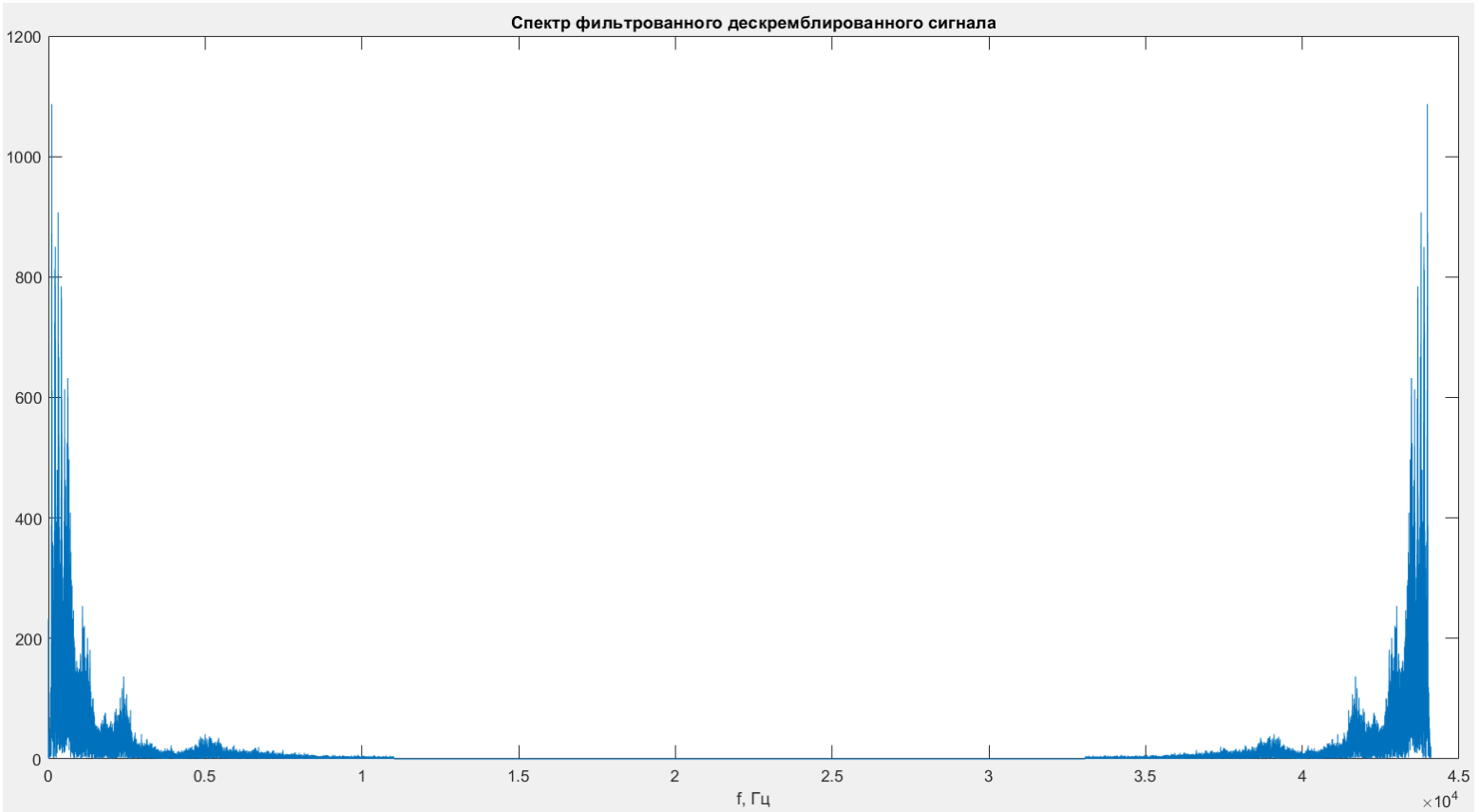


*Рис.21 – Спектр фильтрованного дескремблированного сигнала*

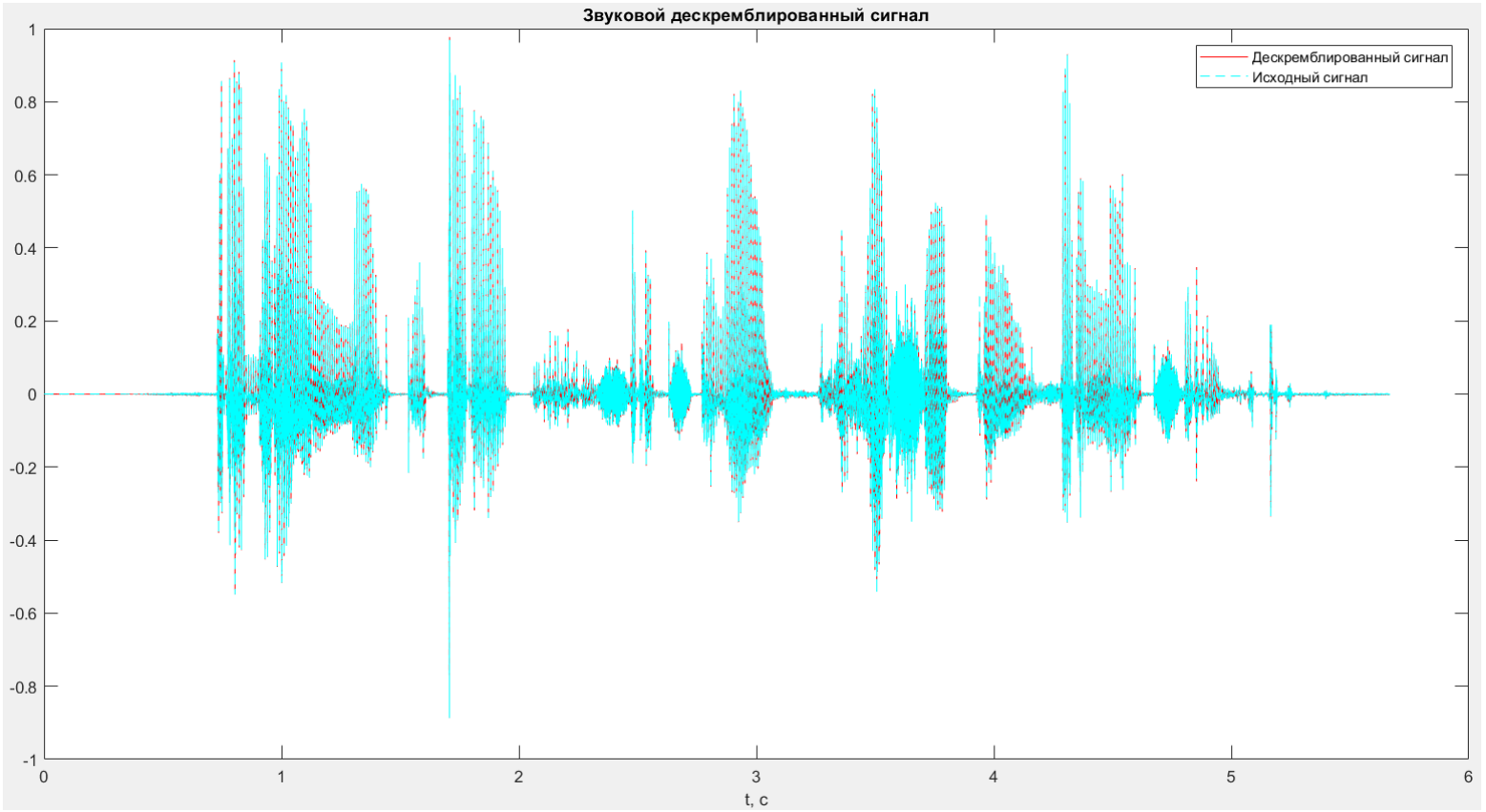


*Рис.22 – Сравнение исходного и дескремблированного сигналов*

Сигнал, полученный в результате дескремблирования, не отличается на слух от оригинального (рис. 22). Это свидетельствует о том, что скремблирование методом частотной инверсии – обратимый процесс с достаточной точностью восстановления информации.

## 3. Выводы:

Основная цель скремблирования - защита передаваемой по открытому каналу информации от злоумышленника.

Метод частотной инверсии позволяет добиться сигнала, похожего на скрип, что делает неудобной интерпретацию такого сигнала на слух, однако сохраняются интервалы между словами, что позволяет частично разобрать информацию.

Сдвиг по фазе не влияет на форму сигнала, а значит не является дополнительным средством сокрытия информации.

Так как мы ограничены частотной областью до 3400Гц, злоумышленнику не составит труда перехватить наш скремблированный сигнал и выполнить те же операции, чтобы получить исходный полезный сигнал.

Таким образом, скремблирование методом частотной инверсии не является очень надежным способом защиты информации.