Министерство науки и высшего образования Российской Федерации

Федеральное государственное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

А.М. ГОЛИКОВ

ИССЛЕДОВАНИЕ МЕТОДОВ АНАЛОГОВОГО СКРЕМБЛИРОВАНИЯ

Учебно-методическое пособие по лабораторной работе

Томск 2019

Голиков, А. М. Исследование методов аналогового скремблирования: Учебно-методическое пособие по лабораторной работе [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2019. — 25 с.

В лабораторной работе проводится исследование методов аналогового скремблирования на основе разработки программы для моделирования такой системы в среде LabVIEW. Лабораторная работа предназначен для направления подготовки магистров 11.04.02 "Инфокоммуникационные технологии и системы связи" по магистерским программам подготовки: "Радиоэлектронные системы передачи информации", "Оптические системы связи и обработки информации", "Инфокоммуникационные системы беспроводного широкополосного доступа", "Защищенные системы связи", для направления подготовки магистров 11.04.01 "Радиотехника" по магистерской программе подготовки: "Радиотехнические системы и комплексы", "Радиоэлектронные устройства передачи информации", "Системы и устройства передачи, приема и обработки сигналов", "Видеоинформационные технологии и цифровое телевидение" и специалитета 11.05.01 "Радиоэлектронные системы и комплексы" специализации "Радиолокационные системы и комплексы", "Радиоэлектронные системы передачи информации", "Радиоэлектронные системы космических комплексов", а также бакалавриата направления 11.03.01 "Радиотехника" (Радиотехнические средства передачи, приема и обработки сигналов), бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи (Системы мобильной связи, Защищенные системы и сети связи, Системы радиосвязи и радиодоступа, Оптические системы и сети связи) и может быть полезна аспирантам.

ОГЛАВЛЕНИЕ

1 ВВЕДЕНИЕ

Вступление человечества в 21 век знаменуется бурным развитием информационных технологий во всех сферах общественной жизни. Информация все в большей мере становится стратегическим ресурсом государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам противника (конкурента) и защиты своих информационных ресурсов.

Безопасность связи при передаче речевых сообщений основывается на использовании большого количества различных методов закрытия сообщений, меняющих характеристики речи таким образом, что она становится неразборчивой и неузнаваемой для подслушивающего лица, перехватившего закрытое речевое сообщение. При этом главной целью при разработке систем передачи речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем.

В речевых системах связи известно два основных метода закрытия речевых сигналов, различающихся по способу передачи по каналам связи:

— аналоговое скремблирование;

— цифровое скремблирование (дискретизация речи с последующим шифрованием).

Каждый из этих методов имеет свои достоинства и недостатки, но рассмотрим аналоговое скремблирование

В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется в первую очередь снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры, а их криптостойкость превосходит, и порой довольно значительно, криптостойкость скремблеров. Тем не менее, знать основы функционирования скремблеров, как этап в истории защиты речевой информации, необходимо. Во-первых, аналоговые до сих пор используются там, где невозможно, по ряду причин, использовать другие средства. Во-вторых, фундаментальные принципы и понятия, заложенные в скремблирующие алгоритмы, также распространяются и на другие методы защиты речевых сообщений.

2. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Аналоговые скремблеры

Под аналоговым скремблированием понимается изменение характеристик речевого сигнала так, чтобы полученный сигнал, обладая свойствами речевой неразборчивости, занимал такую же полосу частот, что и исходный открытый сигнал. При использовании этого метода в закрытом сигнале присутствуют фрагменты исходного открытого речевого сообщения, преобразованные в час-

тотной или временной областях. Это означает, что злоумышленники могут попытаться перехватить и проанализировать передаваемую информацию на уровне звуковых сигналов. Поэтому ранее считалось, что, несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры могут обеспечивать лишь низкую или среднюю, по сравнению с цифровыми системами, степень закрытия. Однако новейшие алгоритмы аналогового скремблирования способны обеспечить не только средний, но очень высокий уровень закрытия.

Системы скремблирования подразделяются на два класса:

— статические, схема шифрования которых остается неизменной в течение всей передачи сообщения; такие системы не обладают сколько-нибудь значительной стойкостью, но вполне приемлемы как модели реальных систем скремблирования;

— динамические, с дополнительным повышением уровня закрытия информации за счет изменения параметров преобразования сигнала во времени при постоянном генерировании кодовых подстановок в ходе передачи/приема; такие скремблеры принято обозначать термином роллинговые скремблеры.

Аналоговое скремблирование обеспечивает меньшую степень закрытия речевых сигналов по сравнению с цифровыми методами шифрования, однако при практической реализации аналоговые скремблеры более просты, дешевы, применимы в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц и обеспечивают коммерческое качество восстановления речевого сигнала с гарантией достаточно высокой стойкости закрытия речи, передаваемой по каналу связи.

Большинство структур безопасности оснащено профессиональными средствами УКВ радиосвязи зарубежных фирм таких, как Motorola, Kenwood, Icom и др., использующими аналоговые виды модуляции сигнала (частотный или фазовый). Для подобного

рода радиосредств в подавляющем большинстве в качестве устройств защиты информации применяются аналоговые речевые скремблеры.

Аналоговые скремблеры преобразуют исходный речевой сигнал посредством изменения его амплитудных, частотных и временных параметров в различных комбинациях. Скремблированный сигнал может быть передан по каналу связи в той же полосе частот, что и исходный, открытый.

Рис.1 – Обобщенная структурная схема аналогового скремблера

Виды преобразований аналоговых скремблеров

При скремблировании возможно преобразование речевого сигнала по трем параметрам: амплитуде, частоте и времени. Однако в системах подвижной радиосвязи практическое применение нашли в основном частотные и временные методы преобразования сигнала, а также их комбинации. Возможные помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, в связи с чем амплитудные преобразования при скремблировании практически не применяются [1].

При частотных преобразованиях сигнала в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

— частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);

— разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки;

— разбиение полосы частоты речевого сигнала на несколько поддиапазонов, их частотные перестановки и частотная инверсия спектра в каждом относительно средней частоты поддиапазона.

При временных преобразованиях производится разбиение сигнала на речевые сегменты и применение к ним операций инверсии и перестановок во времени. При этом используются следующие способы закрытия:

— инверсия по времени протяженных сегментов речи;

— временные перестановки коротких фрагментов в сегментах речевого сигнала;

— временные перестановки коротких фрагментов и их инверсия в сегментах речевого сигнала.

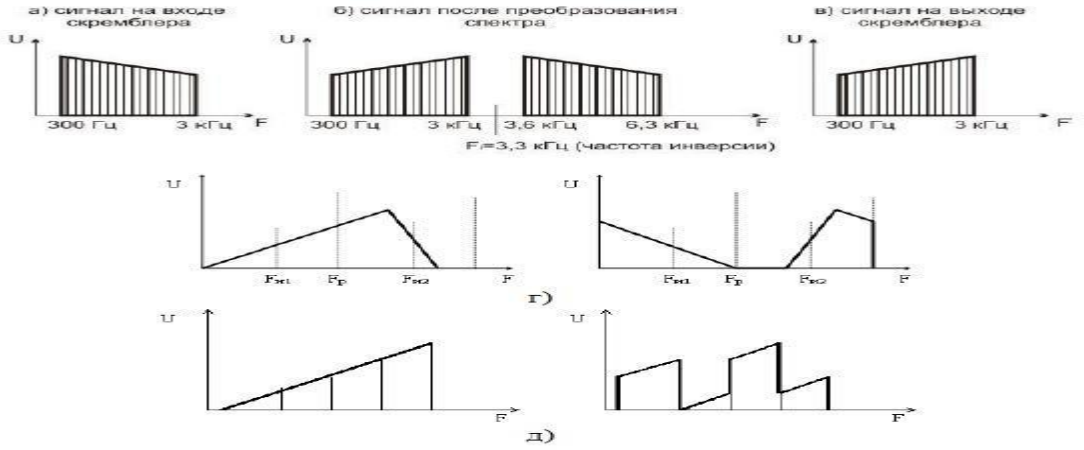
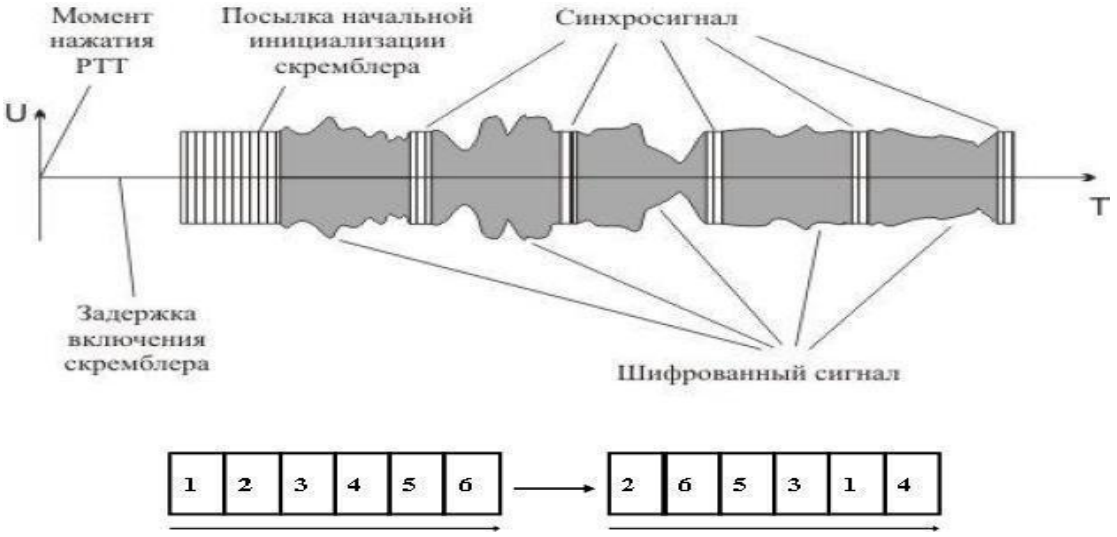


Рис. 2 - Инверсия спектра при скремблировании сигнала – а), б), в); последовательность преобразований; – г); частотные перестановки фрагментов спектра сигнала

В скремблерах с временной перестановкой сигнал делится на сегменты и фрагменты над которыми осуществляется перестановка или инверсия, причем сегмент (кадр) может быть, как фиксированным, так и скользящим. Такие скремблеры

обеспечивают ограниченный уровень закрытия, зависящий от длительности фрагментов в сегментах, а также создают значительные поддержки при работе, требуют дополнительной синхронизации, поэтому их практическое использование затруднено, но они весьма полезны в системах, где требует простота устройства



.

Рис. 3 - Скремблированный сигнал с перестановками во времени фрагментов сегмента речевого сигнала

Комбинированные методы преобразования сигнала предполагают использование одновременно нескольких различных способов скремблирования (как частотных, так и временных), число которых ограничивается, как правило, возможностями технической реализации аналоговых скремблеров.

Динамические скремблеры существенно дороже скремблеров с фиксированными параметрами преобразования сигнала, сильнее влияют на характеристики радиосредств и требуют начальной синхронизации. Однако их применение действительно затрудняет возможности перехвата переговоров, в особенности в реальном масштабе времени. Это объясняется тем, что изменение ключевых параметров во времени теоретически делает возможным резкое увеличение количества ключей. Ключом может быть начальное значение генератора псевдослучайной последовательности, в соответствии с которой меняется определенный ключевой параметр.

Временные преобразования сигнала в сочетании с изменением ключевых параметров во времени достаточно сложны для реализации и требуют относительно длительной синхронизации, поэтому они пока не нашли свое применение в роллинговых скремблерах. Для способов частотного преобразования сигнала изменяемыми ключевыми параметрами могут быть частота инверсии (для

частотного инвертора), частота разбиения полосы сигнала (для полосно-сдвигового инвертора), комбинация частотной перестановки поддиапазонов сигнала (для полосового скремблера). Большинство известных моделей роллинговых скремблеров используют наиболее простой принцип спектрального преобразования – частотный инвертор с изменением частоты инверсии сигнала во времени.

Технические характеристики

Основными техническими характеристиками аналоговых скремблеров являются уровень закрытия информации, остаточная разборчивость и качество восстановления сигнала.

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил. В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера.

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала. Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров как правило, произведением чисел состояний всех ключевых параметров.

Обзор известных моделей скремблеров

Наибольшее количество известных моделей скремблеров реализуют частотную инверсию сигнала. Все они имеют близкие параметры. Одними из первых на отечественном рынке появились модели скремблеров фирмы Selectone (ST-20 и ST-022),

работающие в диапазоне частот 300-2400 Гц и обеспечивающие инверсию сигнала относительно 8 возможных номиналов частот в диапазоне от 2,6 до 3,7 КГц (частота инверсии устанавливается программно).

Простейшие модели скремблеров фирмы Transcrypt SC20-400 и SC20-401 обладают характеристиками, аналогичными ST-20 и ST-022; речевой диапазон частот, 4 варианта частоты инверсии.

Более сложное преобразование сигнала предлагают полосно-сдвиговые инверторы, разработанные НТЦ "ИНТЕР-ВОК" Принцип работы микросборок 04ХК011 ("Сонет"), 04ХК012, 04ХК014А, 04ХК015А, 04ХК017А состоит в разделении речевого спектра на две части, низкочастотную и высокочастотную, каждая из которых разворачивается вокруг своих средних частот. Все они работают в диапазоне речевых частот - 300-3400 Гц. Указанные скремблеры обладают повышенной по сравнению с частотными инверторами степенью закрытия информации. В технических данных указывается, что скремблеры обеспечивают остаточную разборчивость речи не более 10 %. В то же время гарантируется сохранение высокого качества речи при прослушивании с помощью радиостанции, оснащенной аналогичным скремблером (сохранение 1 класса разборчивости при измерении по методике ГОСТ 16600-72).

Известны скремблеры для эффективной защиты телефонных переговоров в сетях, работающих по GSM стандарту. Специально разработанный скремблер GUARD GSM, будучи эконом-вариантом, отлично маскирует речь, передаваемую по каналам GSM связи. Данное устройство соединяется с сотовым телефоном по проводной гарнитуре и имеет небольшие размеры.

Принцип работы данного скремблера основан на первоначальном разрушении и временной перестановки звука на передающей стороне с его последующим восстановлением на принимающей стороне. Этот процесс дуплексный. Начало разговора, как правило, начинается в открытом режиме и далее по обоюдной команде устройства, переключаются в режим скремблирования.

Программная реализация виртуальной модели скремблера

Программную реализацию виртуальной модели скремблера можно выполнить в среде LabVIEW, Simulink или на одном из языков объектно-ориентированного программирования. Приведенная реализация программной модели выполнена в виде виртуальных приборов, созданных в среде LabVIEW. Данная программная система моделирует скремблер работающий с телефонным каналом связи на частоте от 200 Гц до 3,4 КГц. В модели представлены несколько видов операций скремблирования:

— временной статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки;

— временной скремблер с инверсией;

— полосовой частотный статический скремблер, производящий операции

— над блоками фиксированного размера с фиксированным порядком перестановки, использует фильтрацию, инверсию спектра, преобразование частоты;

— полосовой частотный статический скремблер, производящий операции над блоками фиксированного размера с фиксированным порядком перестановки, использует прямое и обратное БПФ;

— инвертирующий частотный скремблер, производящий операции над блоками фиксированного размера, использующий прямое и обратное БПФ,

инверсия идет относительно средней точки спектральной последовательности.

В качестве исходных сигналов скремблера использованы звуковые файлы в формате WAV, записанные с частотой дискретизации 8 КГц в формате моно. Скремблер может выполнять загрузку звуковых файлов в формате WAV, их скремблирование или

дескремблирование по одному из нескольких алгоритмов с изменяемыми параметрами, запись результата в файлы в формате WAV, а также визуализировать и озвучить как исходный, так и обработанный звук.

Временное скремблирование

Разработан виртуальный прибор для осуществления временных видов скремблирования/дескремблирования, лицевая панель которого для осуществления скремблирования речевого сигнала во временной области на основе его инверсии. На лицевую панель прибора выведены: временные диаграммы входного сигнала, скремблированного сигнала, все необходимые регулировочные ручки для настроек параметров скремблера и органы индикации параметров речевого сигнала.

Рис. 4 – Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала на основе временной инверсии

Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска и для записи скремблированного сигнала в файл, а также блоки для преобразований типов данных для осуществления временной инверсии. Лицевая панель виртуального прибора при переключении тумблера для осуществления скремблирования речевого сигнала во временной области на основе перестановок временных сегментов сигнала приведена на рис.3, а фрагмент диаграммной панели – на рис.4. Как видно, на диаграммной

панели использованы вложенные приборы для чтения звукового файла с диска, осуществления временных перестановок с фиксированным ключом и для записи скремблированного сигнала в файл. Временные перестановки на приведенном виртуальном приборе на рисунке 3 выбраны с фиксированным ключом: 87214365, где цифры обозначаю номер временного фрагмента в сегменте исходного речевого сигнала.

При программировании алгоритма на диаграммной панели можно использовать case- структуру для выбора временной инверсии и временных перестановок. Дальнейшая модернизация скремблера предусматривает задание ключей скремблирования при перестановке временных сегментов с помощью case-структуры. Это же касается и модели дескремблера.

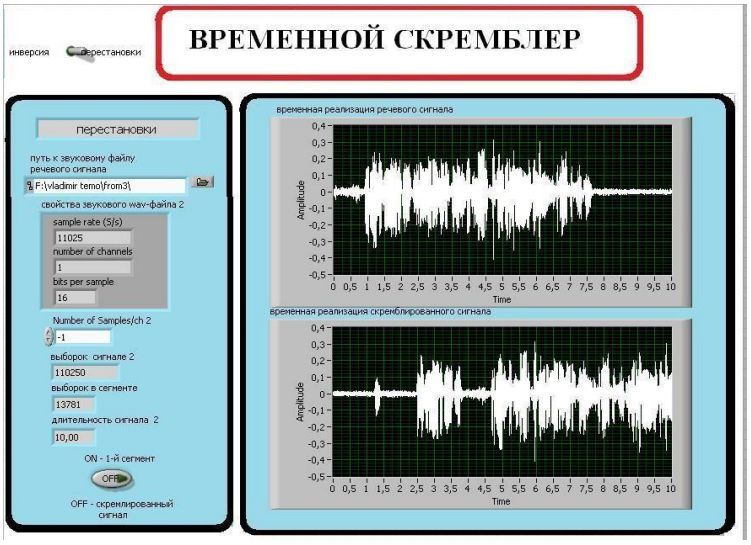


Рис. 5 – Лицевая панель виртуального прибора для осуществления временного скремблирования речевого сигнала с перестановками

Виртуальный прибор позволяет при каскадном наращивании разработанных библиотечных модулей временного скремблирования/ дескремблирования реализовать код скремблирования любой сложности.

— Необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала.

— Основным источником шума при скремблировании и дескремблировании является длительность элементарного временного сегмента при разбиении, которая в пределе равна шагу дискретизации сигнала.

— При учете всех выше сказанных особенностях и должных настроек элементов виртуального прибора, обеспечивается хорошее закрытие информации, а затем её восстановление при дескремблировании с хорошей словесной разборчивостью.

Частотное скремблирование

Реализовать виртуальные приборы для осуществления частотного полосового скремблирования можно различными способами: параллельно-

последовательной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с преобразованием частоты и фильтрацией, параллельной обработкой с использованием БПФ и др. Приведем некоторые варианты реализации первых двух способов.

Параллельно-последовательная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на две полосы, осуществление их перестановок и инверсии спектра, а затем последовательно к каждому частотному диапазону применения аналогичных преобразований. Таким образом, можно последовательно увеличивать число частотных полос при разбиении спектра в 2 раза (2 полосы, 4, 8, 16, и т.д.), тем самым, увеличивая количество ключей скремблирования. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 4 полосы) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования.

Лицевая панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена на рисунке 6.

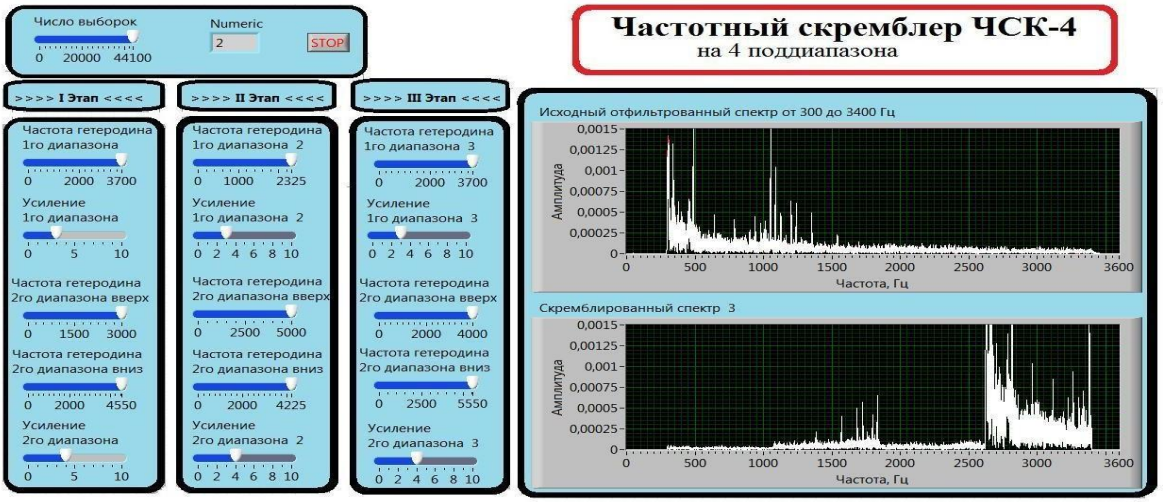


Рис. 6 - Лицевая панель виртуального прибора частотного скремблирования речевого сигнала

На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл. Скремблер состоит из трёх последовательно соединенных смесителей с подключенными регулировочными ручками.

В качестве фильтра выбран эллиптический фильтр 6-го порядка из-за высокой крутизны АЧХ, сопровождающейся колебательным характером плоской вершины в полосе пропускания, и наличием боковых лепестков в полосе заграждения.

Каждый смеситель делит входной сигнал на два диапазона частот. На 1 этапе сигнал делится по 1550Гц. Первый диапазон (300Гц-1850Гц) инвертируется и перемещается (1850Гц-3400Гц) с помощью гетеродина с частотой 3700Гц.

Второй диапазон (1850Гц- 3400Гц) перемещается (300Гц-1850Гц) без инвертирования, с помощью двух гетеродинов с частотами 3000Гц и 4550Гц.

На выходе 1-го смесителя два диапазона складываются. В результате получается скремблированный сигнал I этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход второго смесителя, где делится на два диапазона. Первый диапазон (2625Гц-3400Гц) перемещается (300Гц-1075Гц) без инверсии, с помощью гетеродина с частотой 2325Гц.

Второй диапазон (300 Гц-2625Гц) перемещается (1075 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 5000Гц и 4225Гц.

На выходе 2-го смесителя два диапазона складываются. В результате получается скремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего смесителя, где делится на два диапазона. Первый диапазон (300Гц-1850Гц) перемещается (1850Гц-3400Гц) с инверсией, с помощью гетеродина с частотой 3700Гц.

Второй диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850Гц) без инверсии, с помощью двух гетеродинов с частотами 4000Гц и 5550Гц.

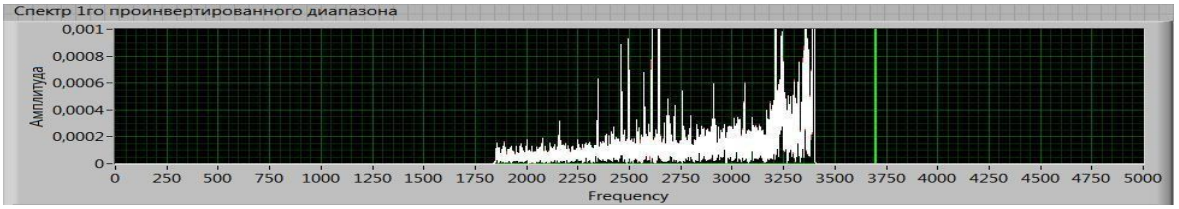


Рис. 7. Спектр первого проинвертированного диапазона

На выходе 3-го смесителя два диапазона складываются. В результате получается скремблированный сигнал III этапа на частотах от 300Гц до 3400Гц – спектр результирующего скремблированного сигнала.

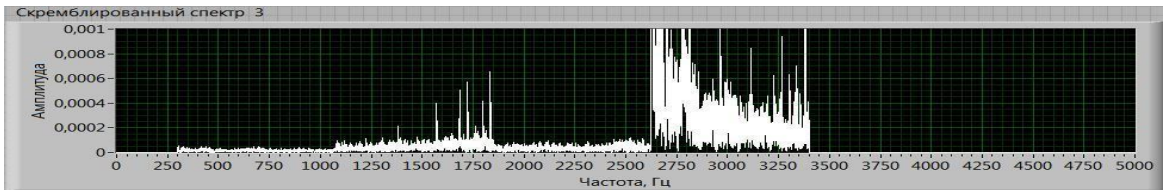


Рис. 8 - Спектр скремблированного сигнала третьего этапа

Дескремблер. Для восстановления скремблированного речевого сигнала был спроектирован частотный дескремблер. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр дескремблированного.

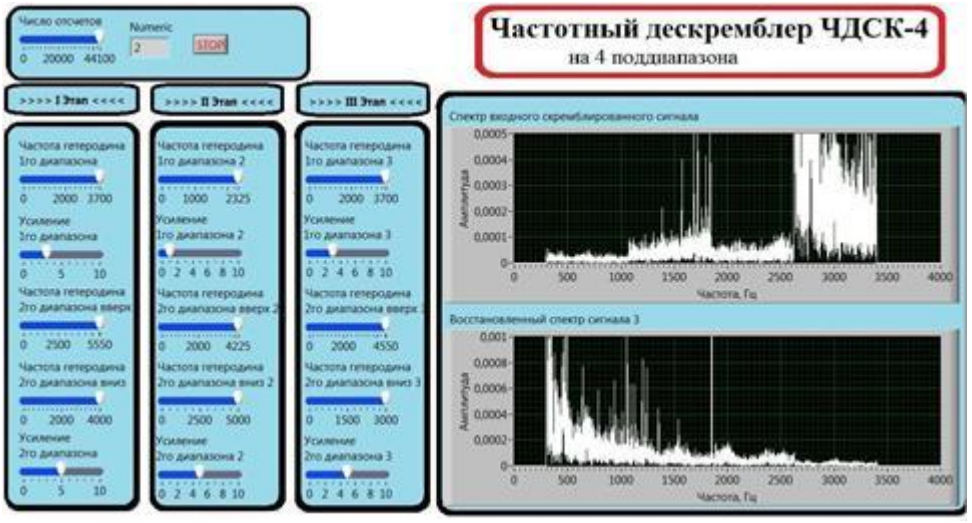


Рис. 9 - Лицевая панель виртуального прибора дескремблера: три последовательно соединенных разделителя с регулировочными ручками

Каждый разделитель делит входной сигнал на два диапазона частот (см. рисунок 6.13). Сигнал поступает на вход первого разделителя, где первый диапазон (1850 Гц- 3400 Гц) инвертируется и перемещается (300 Гц-1850 Гц) с помощью гетеродина с частотой 3700Гц.

Второй диапазон (300 Гц-1850 Гц) перемещается (1850Гц-3400Гц) без инвертирования при помощи двух гетеродинов с частотами 5550 Гц и 4000 Гц

На выходе 1-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал I этапа на частотах от 300Гц до 3400 Гц.

Далее сигнал поступает на вход второго разделителя, где делится на два диапазона. Первый диапазон (300Гц-1075Гц) перемещается (2625Гц-3400Гц) без инверсии, при помощи гетеродина с частотой 2325Гц.

Второй диапазон (1075Гц-3400Гц) перемещается (300 Гц-2625Гц) без инверсии, с помощью двух гетеродинов с частотами 4225 Гц и 5000 Гц.

На выходе 2-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал II этапа на частотах от 300Гц до 3400Гц.

Далее сигнал поступает на вход третьего разделителя, где делится на два диапазона. Первый диапазон (1850Гц-3400Гц) перемещается (300 Гц-1850 Гц) с инверсией, с помощью гетеродина с частотой 3700 Гц.

Второй диапазон (300 Гц-1850Гц) перемещается (1850 Гц-3400Гц) без инверсии, с помощью двух гетеродинов с частотами 4550Гц и 3000Гц.

На выходе 3-го разделителя два диапазона складываются. В результате получается дескремблированный сигнал III этапа на частотах от 300Гц до 3400Гц.

Виртуальные приборы, осуществляющие аналоговое частотное скремблирование речевых сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Параллельная обработка при осуществлении частотно скремблирования предполагает разбиение частотного диапазона спектра сигнала на заданное число полос, осуществление их перестановок и инверсии спектра. Созданный виртуальный прибор, как один из вариантов для осуществления заданного вида (разбиение на 8 полос) частотного полосового скремблирования речевого сигнала, позволяет отображать временные реализации сигналов и их спектров, а также прослушивать речевой сигнал как до скремблирования, так и после осуществления скремблирования и дескремблирования.

Исходный спектр речевого сообщения разбивается на 8-поддиапазонов, как изображено на рисунок

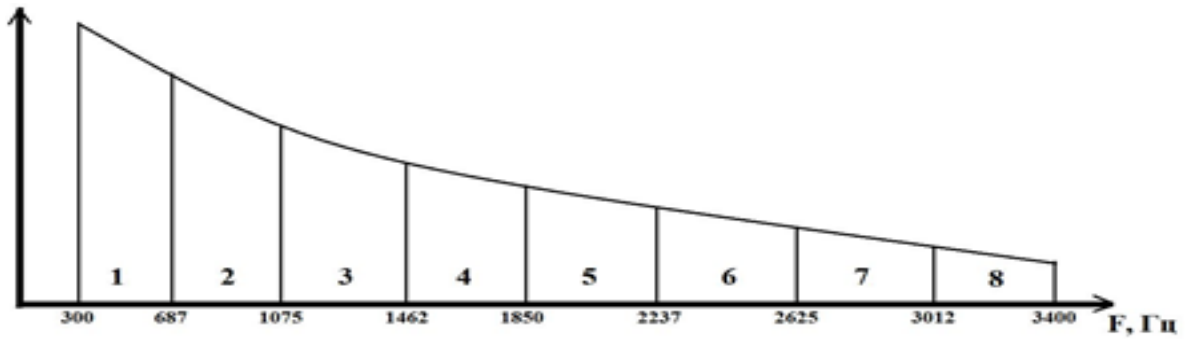


Рис. 9. Разбиение сигнала на 8 поддиапазонов

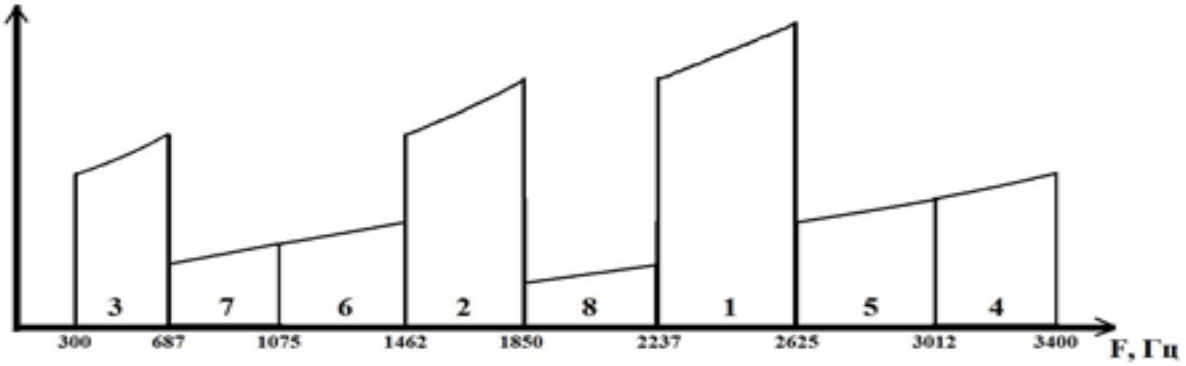


Рис. 10 - Структура спектра после скремблирования

В зависимости от кода скремблера, диапазоны инвертируются и расставляются в определенном порядке. Диаграммная панель виртуального прибора для осуществления скремблирования речевого сигнала в частотной области в диапазоне частот от 300Гц до 3400Гц приведена на рисунке 11. На лицевую панель прибора выведены: спектр входного сигнала, отфильтрованного от 300Гц до 3400Гц; спектр скремблированного сигнала и все необходимые регулировочные ручки для настроек параметров скремблера. Как видно, на диаграммной панели использованы вложенные приборы для чтения звукового файла с диска, для осуществления преобразования частоты, для расчета спектра, для осуществления частотной фильтрации и для записи скремблированного сигнала в файл

Исходный сигнал подается на 8 полосовых эллиптических фильтров 7-го порядка, после чего, для того, чтобы проинвертировать спектр и перенести его в диапазон 2237 Гц -2625 Гц, используется гетеродинное преобразование частоты с частотой генератора 2925 Гц, в результате. Теперь, чтобы отделить необходимую часть спектра, сигнал пропускается через полосовой эллиптический фильтр 6-го порядка. Параметры 2-го фильтра выбираются с меньшим порядком и большим частотным захватом фильтруемого спектра, чтобы меньше искажать форму сигнала.

Элемент (SubVI) является вложенным виртуальным прибором, который выполняет фильтрацию и перестановку поддиапазонов, формируя на выходе два канала. После усиления они объединяются в один канал, и сигнал записывается в файл. Диаграммная панель вложенного виртуального прибора представлена на рисунке. На выходе вторых фильтров используются сумматоры для объединения 1, 2, 4 и 7-го поддиапазонов во второй канал и объединения 3, 5, 6 и 8-го поддиапазонов в первый канал.

На рисунке представлена лицевая панель виртуального прибора.

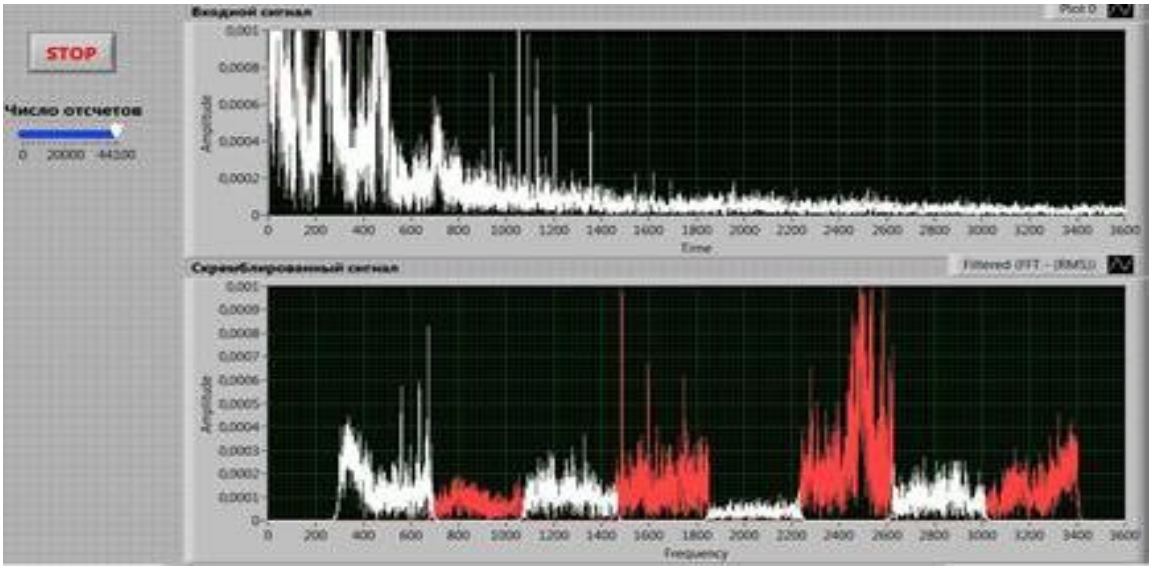


Рис. 11 - Лицевая панель виртуального прибора скремблера

Анализ качества и криптостойкости скремблеров

Наиболее важной характеристикой скремблера для пользователя, желающего обеспечить защиту информации в своих каналах связи, является уровень закрытия информации. Для сложных цифровых систем передачи речи и данных понятие уровня закрытия строго регламентируется и определяется криптографической стойкостью информации, то для аналоговых скремблеров (особенно в системах подвижной радиосвязи) данное понятие носит условный характер, так как к настоящему времени на этот счет не выработано четких стандартов или правил.

В ряде случаев в качестве критериев уровня закрытия информации при сравнении различных средств подвижной радиосвязи с аналоговым скремблированием можно использовать количество ключевых параметров и количество возможных ключей скремблера.

Под ключевым параметром аналогового скремблера обычно понимают какой-либо параметр преобразования речевого сигнала, значение которого необходимо знать для осуществления обратного преобразования сигнала на приемной стороне. Ключом аналогового скремблера (по аналогии с цифровыми системами шифрования), как правило, называют конкретное секретное состояние некоторых параметров преобразования речевого сигнала.

Количество ключей скремблера определяется множеством всевозможных значений ключа. Для скремблеров с одним ключевым параметром оно определяется числом возможных состояний этого параметра, для скремблеров с несколькими ключевыми параметрами - количеством возможных комбинаций значений этих параметров (как правило, произведением чисел состояний всех ключевых параметров). В связи с вышесказанным, лучше всего речь закрывает мозаичный скремблер с шестнадцатью возможными положениями ключа и инверсией, и перестановками по времени, на втором месте по защищенности – шестнадцати диапазонный скремблер также с шестнадцатью возможными положениями ключа, но с отсутствием скремблирования по времени. Замыкает тройку частотный четырех диапазонный скремблер. Временные скремблеры, в данном определении уровня закрытия речевой информации, расположились на последнем месте, по той причине, что они статичны и у них отсутствует возможность изменения ключей. Справедливости ради стоит отметить, что на слух, временной скремблер более лучше закрывает информацию, чем скажем четырех диапазонный частотный скремблер. Оценка разборчивость речи мной согласно ГОСТу Р 50840–95 затруднительна, так как требует специальных знаний, средств и обученных людей.

Был разработан программный комплекс, позволяющий проводить аналоговое скремблирование. Таким образом, из описанных моделей скремблеров/дескремблеров следуют следующие выводы:

— даже при разделении сигнала на четыре поддиапазона, скремблированный сигнал имеет низкую словесную разборчивость, что указывает на сильное закрытие информации виртуальным прибором;

— так как в данном устройстве используются гетеродины, к ним должны предъявляться жесткие требования, иначе вследствие нестабильности

их частоты полезный сигнал будет подавлен фильтром, что снизит качество восстанавливаемого сигнала;

— в результате гетеродинного преобразования полезный сигнал теряет часть энергии, в виду этого необходимо производить усиление в каждом диапазоне на всех этапах скремблирования и дескремблирования;

— необходимо учитывать при разработке прибора, что скремблирование и дескремблирование вносит задержки в передаче речевого сигнала;

— Основным источником шума при скремблировании и дескремблировании являются эллиптические фильтры

— Также при проектировании прибора необходимо учитывать, что фильтр с высоким порядком является высокодобротной системой и имеет долгий незатухающий отклик - «звон», что влечет за собой появление помехи

Виртуальные приборы, осуществляющие аналоговое временное, частотное скремблирование речевых сигналов, а также библиотечные модули (вложенные виртуальные приборы) для частотного, временного скремблирования и дескремблирования с перестановками и инверсией, позволяют при каскадном наращивании смесителей и разделителей, реализовать код скремблирования любой сложности.

Исследование аналогового временного скремблера

Временные скремблеры основаны на двух основных способах закрытия: инверсии по времени сегментов речи и их временной перестановке. В скремблерах с временной

инверсией речевой сигнал делится на последовательность временных сегментов и каждый из них передается инверсно во времени - с конца. Такие скремблеры обеспечивают ограниченный уровень закрытия, зависящий от длительности сегментов. Для достижения неразборчивости медленной речи необходимо, чтобы длина сегмента составляла около 250 мс. Это означает, что задержка системы будет равна примерно 500 мс, что может оказаться неприемлемым для некоторых приложений.

Для повышения уровня закрытия прибегают к способу перестановки временных отрезков речевого сигнала в пределах фиксированного кадра (рисунок 1). Правило перестановок является ключом системы, изменением которого можно существенно повысить степень закрытия речи. Остаточная разборчивость зависит от длительностей отрезков сигнала и кадра и с увеличением последнего уменьшается.

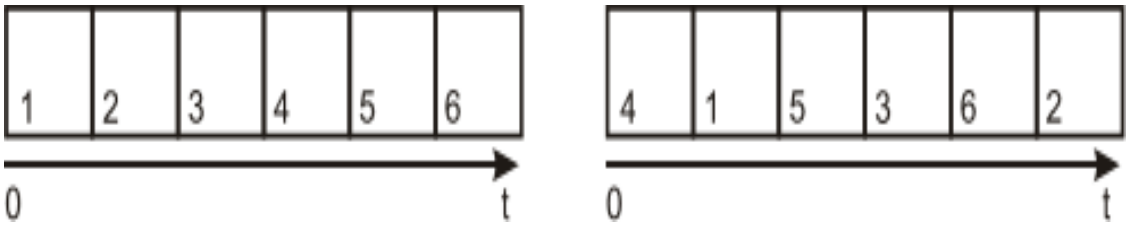


Рис. 12 - Схема работы временного скремблера с перестановкам
и в фиксированном кадре

Главным недостатком скремблера с фиксированным кадром является большая величина времени задержки системы, равная удвоенной длительности кадра. Этот недостаток устраняется в скремблере с перестановкой временных отрезков речевого сигнала со скользящим окном. В нем число комбинаций возможных перестановок ограничено таким образом, что задержка любого отрезка не превосходит установленного максимального значения. Каждый отрезок исходного речевого сигнала как бы имеет временное окно, внутри которого он может занимать произвольное место при скремблировании. Это окно скользит во времени по мере поступления в него каждого нового отрезка сигнала. Задержка при этом снижается до длительности окна.

3 ПРАКТИЧЕСКАЯ ЧАСТЬ

Для проведения лабораторной работы понадобится звуковой файл в формате wav, для его создания необходимо открыть программу Audacity.

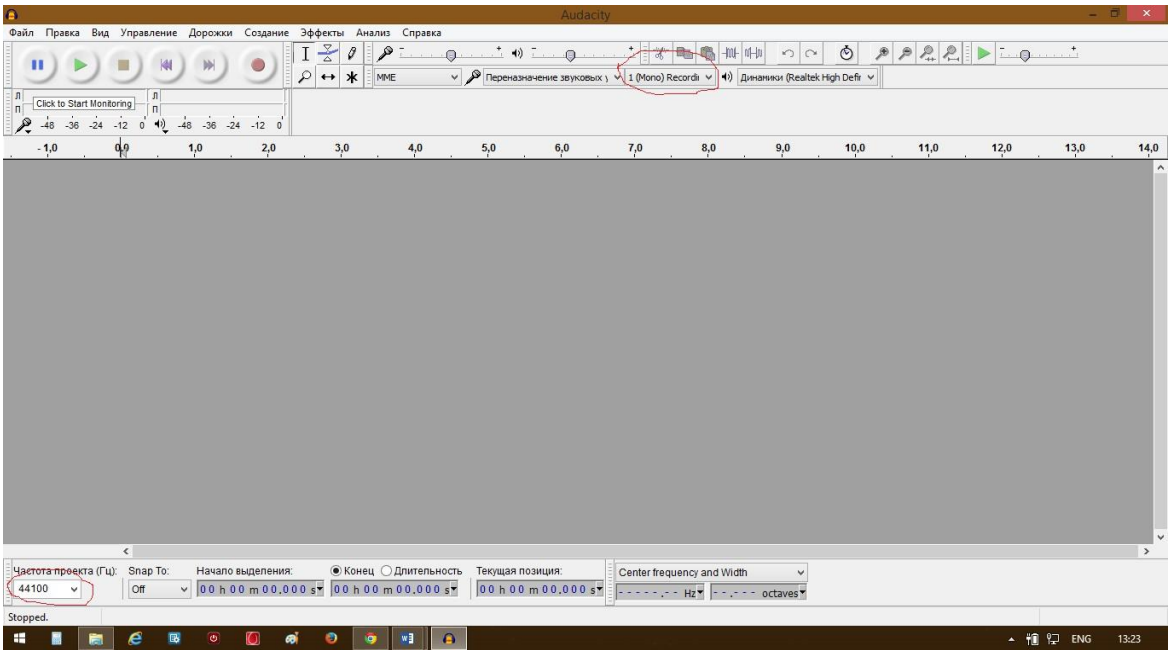


Рис. 13 - Окно программы Audacity с нужными настройками (выделено красным)

После этого нужно нажать кнопку запись (круглая кнопка с красным кругом в центре), и записать.

Затем нужно нажать на копку стоп. В меню нажать Файл->Export Audio, в появившемся окне нужно выбрать место куда следует сохранить файл, задать имя файла и убедиться что в поле тип файла выбрано значение: WAV (Microsoft) signed 16-bit PCM.

Для начала работы нужно запустить файл test.vi, запустить программу, установить количество сэмплов, и нажать кнопку старт, в появившемся окне следует выбрать файл, который был записан с помощью программы Audacity.

После этого сигналы исходного и скремблированного файла отображатся на соответствующих экранах, после этого появится окно для выбора места сохранения скремблированного файла.

Инверсный скремблер

Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

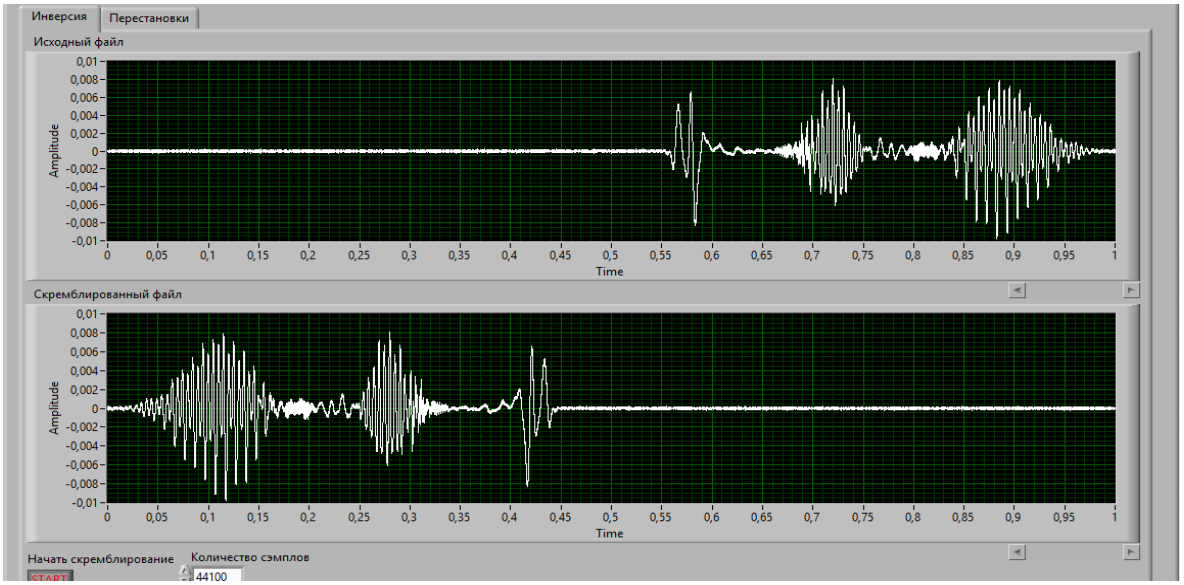


Рис. 14 - Результат работы инверсного скремблера
с количеством семплов 44100

Параметры выходного файла: длительность 1 секунда, размер файла 86,1 кб. Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного файла.

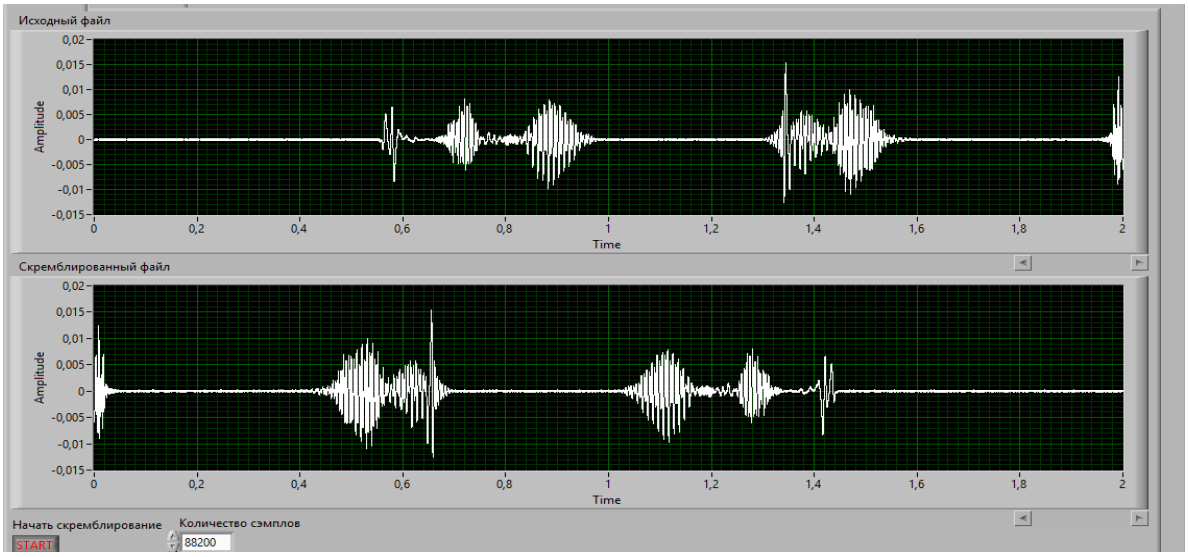


Рис. 15 - Результат работы инверсного скремблера
с количеством семплов 88200

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб. Скремблирование прошло со значительными потерями так как оно за-

вершилось примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла.

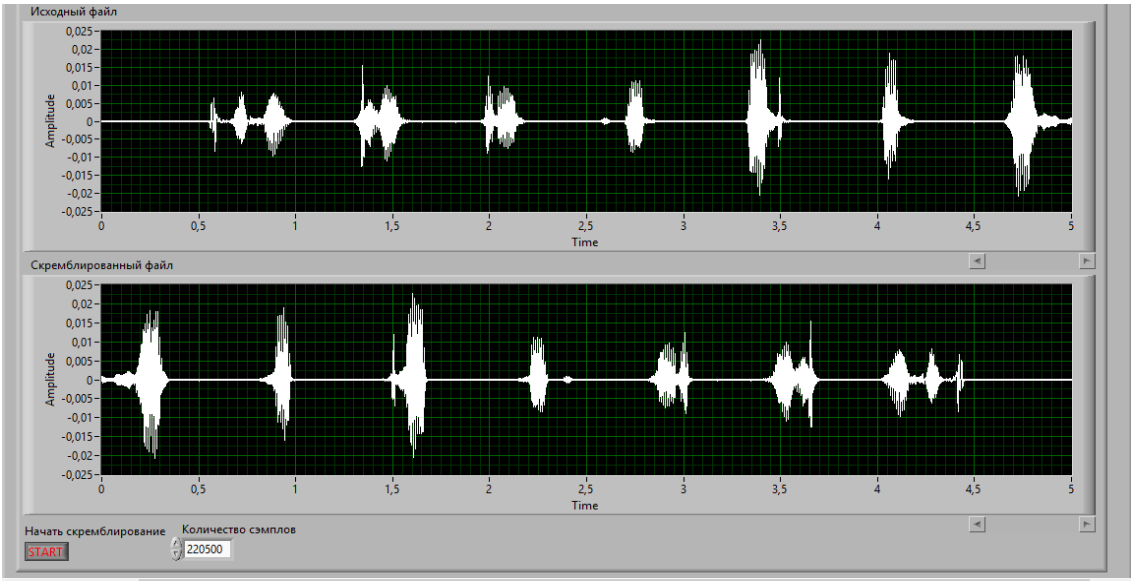


Рис. 16 - Результат работы инверсного скремблера
с количеством семплов 220500

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб. Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

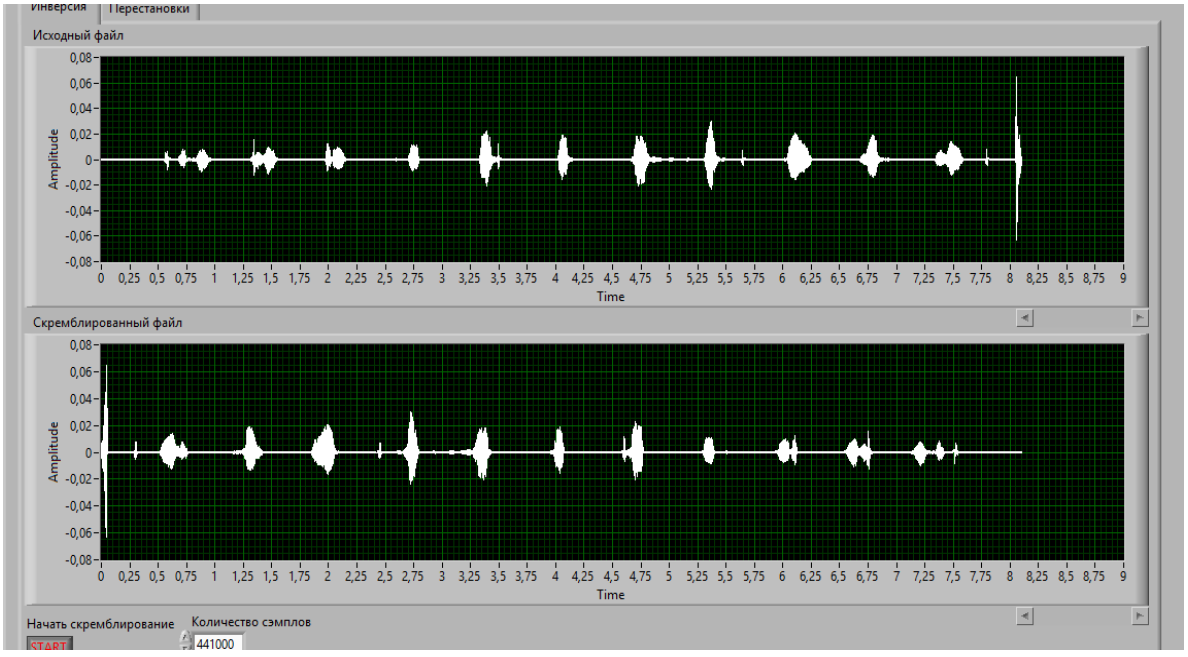


Рис. 17 - Результат работы инверсного скремблера
с количеством семплов 441000

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб. Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

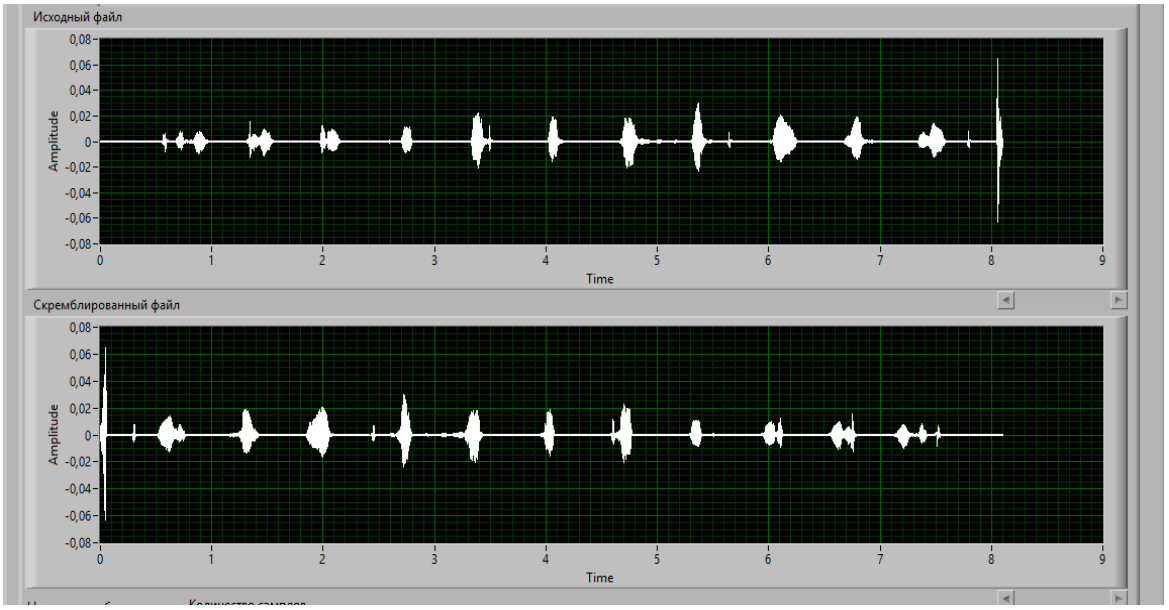


Рис. 18 - Результат работы инверсного скремблера
с количеством семплов 661500

Параметры выходного файла: длительность 8 секунд, размер файла 697 кб. Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

Скремблер перестановки

Задавая количество семплов 44100*n где n=1,2,5,10,15 посмотрим, как изменится выходной файл. Исходный файл был создан в программе “Audacity”, его продолжительность составляет 8 секунд, а размер 697 кб.

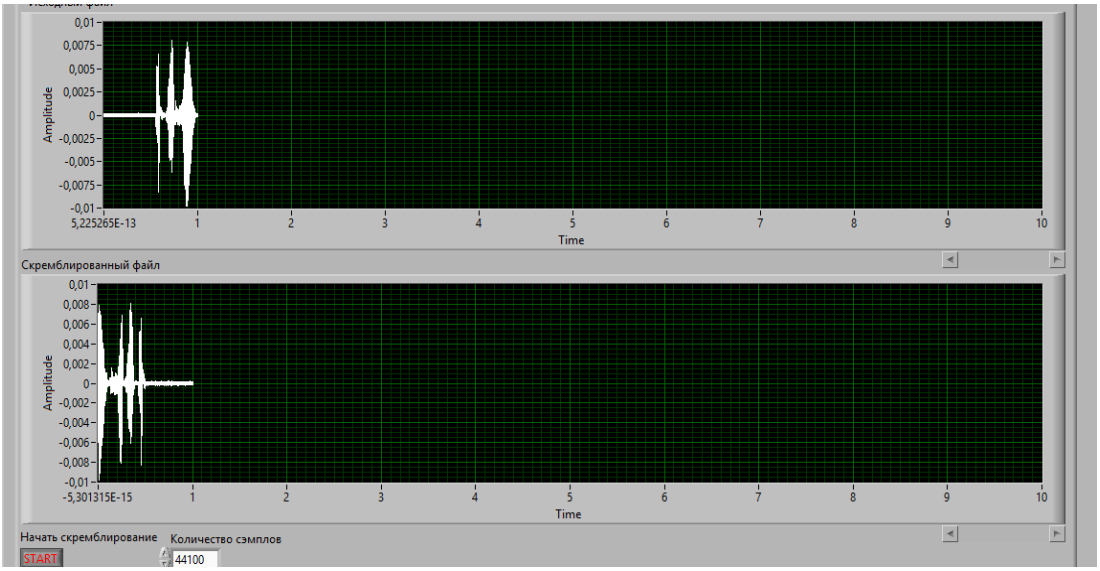


Рис. 19 - Результат работы скремблера перестановки
с количеством семплов 44100

Параметры выходного файла: длительность 1 секунда, размер файла 81,1 кб. Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 87% раньше. Как следствие обратное преобразование не дало исходного файла.

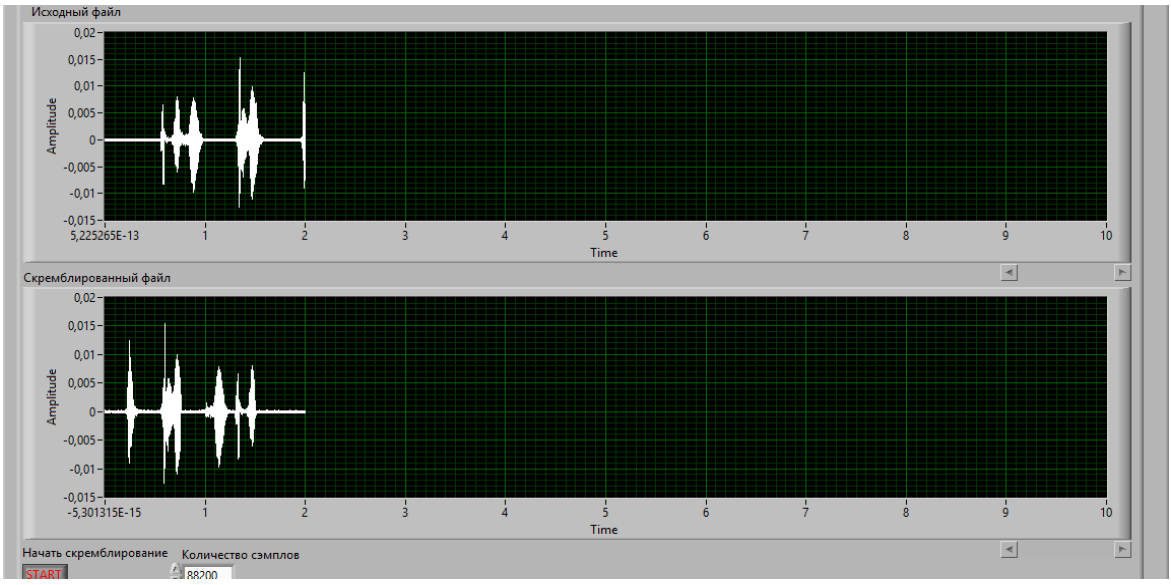


Рис. 20 - Результат работы скремблера перестановки
с количеством семплов 88200

Параметры выходного файла: длительность 2 секунды, размер файла 172,2 кб. Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 75% раньше. Как следствие обратное преобразование не дало исходного файла.

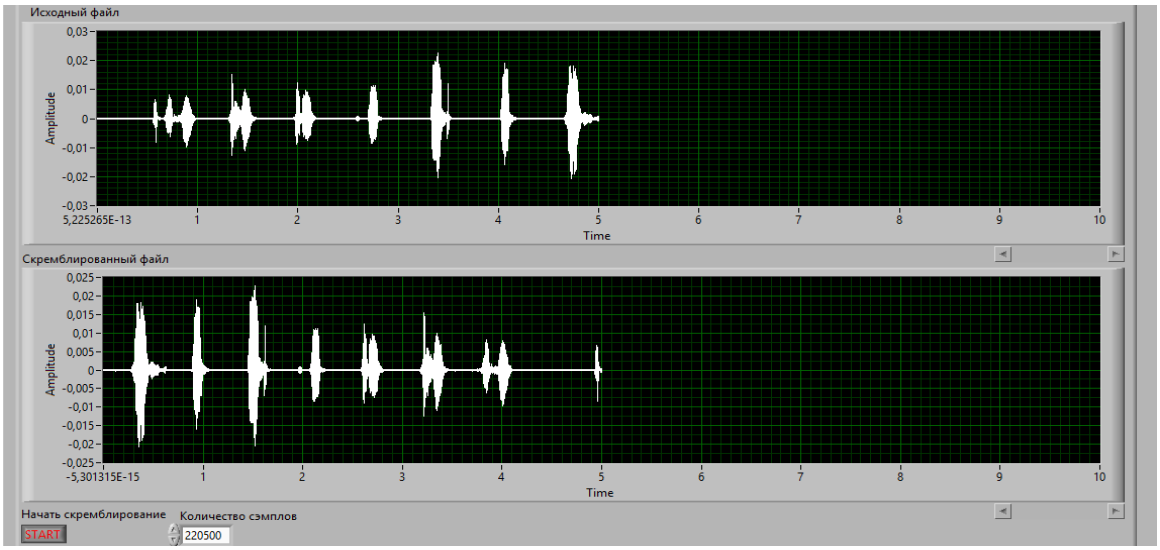


Рис. 21 - Результат работы скремблера перестановки
с количеством семплов 220500

Параметры выходного файла: длительность 5 секунд, размер файла 430 кб. Скремблирование прошло со значительными потерями так как оно завершилось, примерно, на 37% раньше. Как следствие обратное преобразование не дало исходного файла.

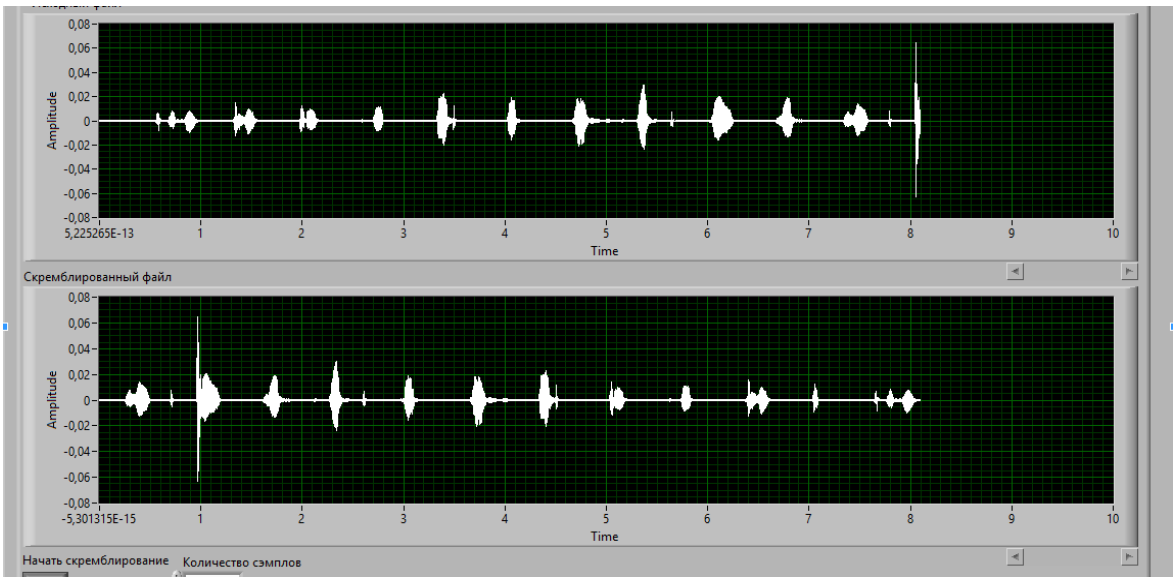


Рис. 22 - Результат работы скремблера перестановки
с количеством семплов 441000

Параметры выходного файла: длительность 8 секунд, размер файла 497 кб

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 25% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

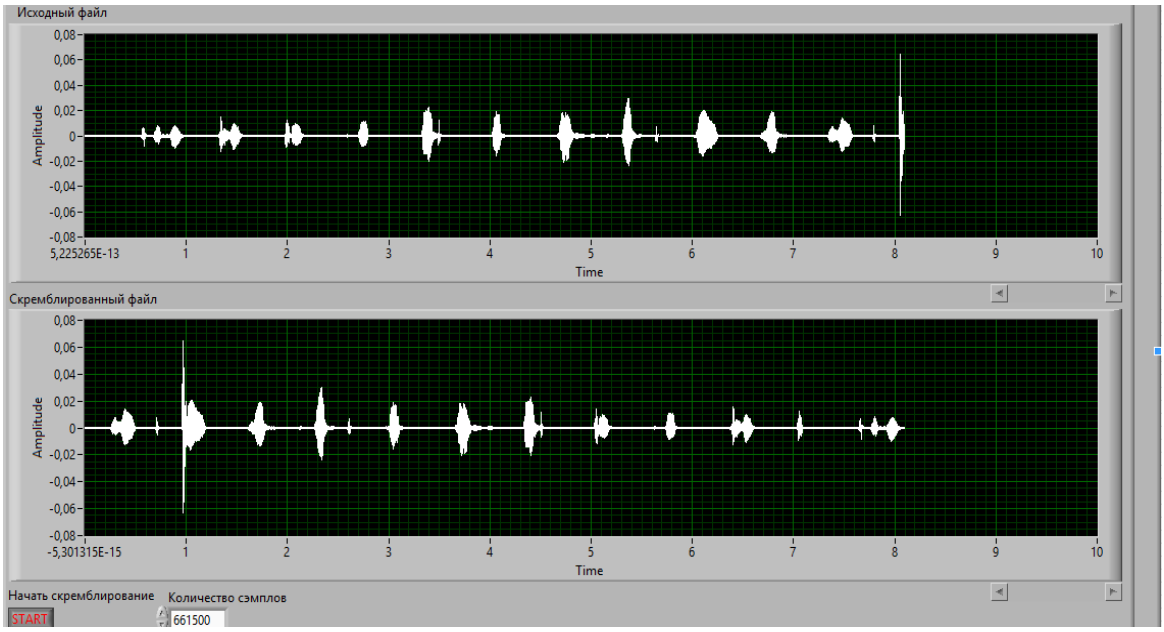


Рис. 23 - Результат работы скремблера перестановки с количеством семплов 661500

Параметры выходного файла: длительность 8 секунд, размер файла 497 кб

Скремблирование прошло без потерь так как процесс скремблирования длился, примерно, на 87% больше. Как следствие обратное преобразование дало исходный файл. Так же стоить отметить что дополнительное время скремблирования не повлияло на размер файла.

Исходя из полученных данных видно, что количество семплов зависит от продолжительности файла и от частоты. Таким образом следует что количество семплов должно быть равно f*(t+1), где t-длительность сигнала в секундах, а f его частота в Гц. Единичка прибавляется для того что бы не потерять часть данных в случае если длительность файла, например, 8.2 секунды.

ЛИТЕРАТУРА

1. Голиков А.М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: Учебное пособие / А.М. Голиков. - СПб.: Издательство «Лань», 2018. – 452с.