ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

Кафедра информационно-телекоммуникационных систем и технологий

РАЗРАБОТКА АЛГОРИТМА СКРЫТНОЙ ПЕРЕДАЧИ РЕЧЕВОГО СИГНАЛА

Выпускная квалификационная работа студентки

очной формы обучения
направления подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
4 курса группы 07001208
Бака Яны Витальевны

Научный руководитель
ст. преп. кафедры
Информационно-
телекоммуникационных
систем и технологий
НИУ «БелГУ» Лихолоб П.Г.

Рецензент
к.ф.-м.н., начальник отдела ОСС
АО «НПП «Спец-Радио»»,
Туяков С.В.

БЕЛГОРОД 2016

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для крупных коммерческих и корпоративных структур существует необходимость осуществлять защищенный обмен данными представляющими коммерческую тайну. Использование стеганографических методов скрытия факта передачи информации[26] позволяет осуществить не только защиту коммерческой информации, но и в частности, позволяет скрыть косвенные признаки факта осуществления переговоров.

Наиболее часто для передачи информационных сообщений не содержащей чисел используют устную речь. Использование устной речи как средства коммуникации вызвано так же простотой её восприятия человеком. Далее речевое сообщение, скрытно передаваемая информация, зарегистрированная в виде речевого сигнала и преобразованная в цифровую форму.

Стоит отметить, что зачастую ресурсы для скрытной передачи речевых сообщений, методами стеганографии ограничены. Вызвано это тем, что для скрытия защищаемого речевого сообщения необходимо использовать данные, объем которых в несколько раз должен превышать объем защищаемого речевого сообщения. Поэтому количество методов и алгоритмов, которые возможно использовать для целей скрытной передачи речевых сообщений не велико [22, 25, 26].

Разработка метода и алгоритма реализующих принципы скрытной передачи речевого сообщения в речевых данных, может позволить повысить оперативность скрытного обмена речевыми сообщениями, за счет более эффективного использования скрытности и емкости речевого материала. Под эффективностью в работе понимается, использование подхода для кодирования речевого сообщения с обеспечением его скрытности, позволяющего увеличить объём передаваемых речевых сообщений без необходимости увеличения объема речевого материала [27,28].

Целью работы является развитие методов скрытого внедрения информации в звуковые файлы посредством разработки нового алгоритма скрытной передачи информации.

Для успешного выполнения поставленной цели необходимо выполнить ряд задач, а именно:

1. Разработать алгоритм скрытного кодирования/декодирования речевого сообщения в речевые данные.
2. Проанализировать отобранный речевой материал и выбрать наиболее оптимальный сигнал для скрытия в него информационного сообщения.
3. Провести качественную оценку скрытности передаваемого речевого сообщения.
4. Провести количественную оценку скрытности передаваемого речевого сообщения.
5. Разработать программную поддержку алгоритмов стеганографического кодирования речевого сообщения в речевые данные и их декодирования.
6. Выполнить экономическое обоснование результатов исследования.

Иными словами, необходимо выявить закономерности изменения качества звучания и восприятия искажений при скрытном кодировании информации модифицированным методом расширения спектра.

Пояснительная записка к дипломной работе состоит из 89 стр., включает в себя 4 раздела и 2 приложения, 30 рисунков, 9 таблиц, использовано 27 литературных источников.

1 ПРЕДСТАВЛЕНИЕ РЕЧЕВОГО СИГНАЛА

1.1 Способы представление речи для скрытной передачи информации

Направление информационных технологий невозможно представить и реализовать без коммуникаций. Передача информация является важным компонентом любой системы, выполняющей какую-либо работу с данными (хранение, обработка, преобразование). В данном случае, под *информацией* понимается совокупность каких-либо сведений, данных, которые, в свою очередь, должны быть достоверны, полны, актуальны, информативны. Стандарты, разработанные специалистами в области связи позволяют передавать данные различного типа. Таким образом, в канале связи имеется возможность передавать неподвижные и подвижные изображения, пакетные сообщения, данные и речевые сигналы. Стоит отметить, что именно работа с речевым материалом как сигналом, который необходимо передать является актуальным и стремительно развивающимся направлением информационно – телекоммуникационных систем связи, а именно областей аналоговой телефонии, сотовой и спутниковой связи.

Речь, по своей природе, является инструментом общения, взаимодействия, т. е. коммуникации. Как правило, при коммуникации речь изначально формируется в мозге человека в виде абстрактного представления, после чего преобразуется в последовательность нервных импульсов, управляющих артикулярным аппаратом, который, в свою очередь, приходит в движение и формирует речевое сигнал с учётом интонации и дикции человека. В сфере телекоммуникаций *речевой сигнал* целесообразно представлять как акустическое колебание, подверженное распространению в упругой среде.

Сообщение, передаваемое посредством речевого сигнала, может быть представлено конечной последовательностью *фонем* – звуковых символов, составляющих данный речевой сигнал, следовательно, данное сообщение *дискретно*. В русском языке 41 фонема. Для обозначения и передачи звуков

используют символы – *буквы*, которые подразделяются на гласные, воспроизводимые только голосом и согласные, которые, в свою очередь разделяются по способу порождения их голосовым аппаратом. Таким образом, среди согласных звуков различают следующие основные типы:

- Взрывные согласные: [п], [п'], [б], [б'], [т], [т'], [д], [д'], [к], [к'], [г], [г'];
- Фрикативные согласные: [ф], [ф'], [в], [в'], [с], [с'], [з], [з'], [ш], [ш':], [ж], [ж':], [х], [х'];
- Сонорные согласные: [р], [р'].

По мере изменения формы артикулярного аппарата диктора, в формируемом речевом сигнале возникают усиленные резонатором частотные характеристики, называемые *формантами*.

При взаимодействии двух или более дикторов акустический сигнал, представленный речью, преобразуется в механическое колебание, соприкасаясь с ушной барабанной перепонкой. Далее, во внутреннем ухе , сигнал является уже импульсом нервной системы. В центральном отделе нервной системы данный сигнал идентифицируется, т. е. исходное речевое сообщение воссоздается с определенной корреляцией в зависимости от индивидуальных особенностей произношения диктора или же меры воздействия внешних шумов.
В настоящее время используется множество способов передачи, преобразования и хранения речевого сигнала. При использования технических средств необходимо преобразовывать форму представления данного сигнала. Поэтому существуют некоторые особенности, которые необходимо учесть:

- Сохранение информационной составляющей речевого сигнала;
- Представление речевого сигнала в форме, удобной для его обработки, хранения, передачи;
- Возможность преобразовывать сигнал без серьезных информационных потерь;
- Легкое восприятие информации техническими (машинными) средствами или человеком при прослушивании.

1.2 Элементы анализа и синтеза сигналов

Для того, чтобы исследовать методы цифровой обработки сигналов, необходимо начать с того, что речевой сигнал как сформированное в голосовом тракте акустическое колебание имеет *аналоговую* природу, т. е. его можно рассмотреть как непрерывно изменяющийся во времени процесс. Математически такой сигнал можно обозначить как $x_n\ (t)$.

Данный сигнал может быть представлен в виде последовательности $x(n)$ чисел, которая является последовательностью мгновенных значений сигнала $x_n\ (t)$, периодически взятых через равные промежутки времени T. Эта операция описывает процесс *дискретизации* речевого сигнала $x_a(t)$, её можно обозначить как $x_n\ (T)$.

На рисунке 1.1 Представлен дискретный сигнал:

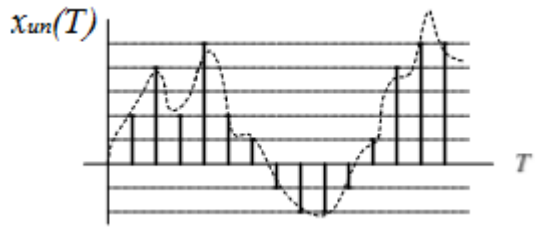

Рисунок 1.1 – Дискретный сигнал

Дискретный сигнал характеризуется длительностью, частотой дискретизации.

Длительность сигнала – временной интервал существования данного сигнала. Длительность, как правило, определяется в секундах, если речь идет о непрерывном сигнале, либо в *отсчетах*, представляющий собой значение амплитуды в данный момент времени.

Частота дискретизации – величина, показывающая меру частоты взятия отсчетов аналогового сигнала при его дискретизации. Интервал T есть период дискретизации, следовательно, частота дискретизации – величина, обратная периоду дискретизации:

$$f_d \le \frac{1}{T}, \tag{1.1}$$

где T – период дискретизации, с.

Формула (1.2) описывает цифровой сигнал как совокупность значений *n*-х отсчетов:

$$\vec{x} = (x_1, .., x_n, .., x_N)^T \tag{1.2}$$

где $\vec{x}$ - отрезок речевого сигнала; $(\ )^T$ - знак транспонирования обозначает, что данные представлены в виде столбца.

Сигнал, подверженный дискретизации во времени и квантованию по уровню называется *цифровым*. Данный сигнал можно описать квантованной последовательностью $x_{un}(T)$, отсчеты которой принимают значения уровней квантования в каждый момент времени *T*.

Также необходимо упомянуть *теорему Котельникова*, согласно которой, исходный сигнал возможно однозначно восстановить, если частота дискретизации будет как минимум в два раза превышать верхнюю частоту, (наибольшую в спектре сигнала). Иными словами, аналоговый сигнал, имеющий ограниченный спектр полностью определяется последовательностью своих отсчетов, взятых с интервалом:

$$T \le \frac{1}{2 f_в}, \tag{1.3}$$

где $f_в$ – верхняя частота конечного спектра, Гц

Под *спектром* сигнала подразумевается распределение энергии сигнала по его частоте. При увеличении частоты дискретизации, увеличивается спектр дискретного сигнала. Также, следует обозначить величину, равную половине частоты дискретизации и называемую *Частотой Найквиста.*

Дискретные сигналы следует рассматривать в области *основного диапазона частот*: $[0; f_d / 2]$. Таким образом, можно ввести понятие *нормированной круговой* частоты:

$$\omega = \frac{2\pi}{T} = 2\pi \cdot f \,, \tag{1.4}$$

где ω - круговая частота, нормированная к π, Гц.

Также следует ввести понятие единичного отсчета, равного одному единичному импульсу и определяемому следующим образом:

$$\delta(n) = \begin{cases} 1, n = 0 \\ 0, n \neq 0 \end{cases}. \tag{1.1}$$

При этом, последовательность единичного скачка представлена в виде:

$$u(n) = \begin{cases} 1, n \geq 0; \\ 0, n < 0. \end{cases} \tag{1.6}$$

При анализе сигнала целесообразно раскладывать его на синусоидальные составляющие (гармоники). Данные синусойды проходят через линейные системы не изменяя при этом своей формы (изменяются при этом амплитуда либо фаза). Таким образом, можно показать, что синусоиды являются «собственными функциями» линейных систем.

Преобразование Фурье (FFT) [19, 23]– это метод анализа сигналов основанный на разложении функций на синусные и косинусные составляющие, описываемое выражением:

$$x\left(e^{j\omega t}\right) = \sum_{n=0}^{\infty} x(t) \cdot e^{j\omega t} \,, \tag{1.7}$$

где $x(t)$ - вещественная или же комплексная функция – оригинал; $X(j\omega)$ - Фурье – образ функции; $x(t)$ - результат Фурье – преобразования.

Сигнал может быть представлен в амплитудно – временной и амплитудно – частотной областях, и в зависимости от того, каким образом необходимо использовать реализацию, применяют *Прямое и обратное преобразования Фурье* [19, 25].

Прямое преобразование определяется формулой:

$$X(j\omega) = \int_0^{\infty} x(t) \cdot e^{j\omega t} dt . \quad (1.8)$$

Обратное преобразование Фурье определяется следующим образом:

$$X(j\omega) = \int_0^{\infty} x(t) \cdot e^{j\omega t} dt , \quad (1.9)$$

$$x(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} X(j\omega) \cdot e^{j\omega t} d\omega , \quad (1.10)$$

где $x(t)$ - вещественная или же комплексная функция – оригинал; $X(j\omega)$ - Фурье – образ функции; $x(t)$ - результат Фурье – преобразования.

Наиболее широкое применение среди спектральных преобразований дискретных сигналов конечной длительности, содержащих *N* отсчетов получило *Дискретное преобразование Фурье* [20, 282] с использованием базисных функций, количество отсчетов которых совпадает с количеством отчетов исследуемого сигнала. Базисную систему в данном преобразовании составляют ортогональные дискретные экспоненциальные функции:

$$\varphi_k(nT) = e^{jk\Omega nT} = e^{\frac{2\pi}{N} \cdot k \cdot n} = W_N^{-k \cdot n} , \quad (1.11)$$

где *n* – номер отсчета дискретного сигнала; *n=[0; N-1]*; k – номер спектральной составляющей дискретного сигнала *k=[0; N-1];* где W_n - поворачивающий множитель ДПФ.

$$W_n = e^{-j\frac{2\pi}{N}}, \tag{1.12}$$

$$\Omega = \frac{2\pi}{N \cdot T}, \tag{1.13}$$

где Ω - основная частота ДПФ.

Положим, дискретный сигнал является периодическим:

$$x(nT) = x[(n + m \cdot N) \cdot T]; m=0, 1, 2\ldots. \tag{1.14}$$

Для перехода сигнала из временной области в спектральную используется *прямое дискретное преобразование Фурье ПДПФ* [20, 285]:

$$X(jk\Omega) = \sum_{n=0}^{N-1} x_n(T) \cdot e^{-j\frac{2\pi}{N} \cdot k \cdot n} = \sum_{n=0}^{N-1} x_n(T) \cdot W_N^{k \cdot n} = \sum_{n=0}^{N-1} x_n(T) \cdot e^{-jk\Omega nT}. \tag{1.15}$$

Последовательность $X(jk\Omega)$ является периодической (период в N отсчетов):

$$X(jk\Omega) = X[j(k + l \cdot N) \cdot \Omega]. \; l=1, 2, \ldots \tag{1.16}$$

Частота дискретизации комплексного спектра $X(jk\Omega)$:

$$\omega_o = N \cdot \Omega. \tag{1.17}$$

Для осуществления обратной процедуры – перехода сигнала из спектральной области во временную применяется *обратное дискретное преобразование Фурье ОДПФ* [20, 286]:

$$x(nT)=\frac{1}{N}\sum_{k=0}^{N-1}X(jk\Omega)\cdot e^{-j\frac{2\pi}{N}\cdot k\cdot n}=\frac{1}{N}\sum_{k=0}^{N-1}X(jk\Omega)\cdot W_N^{-k\cdot n}=\frac{1}{N}\sum_{k=0}^{N-1}X(jk\Omega)\cdot e^{jk\Omega nT}\ . \qquad (1.18)$$

Данное выражение можно пояснить следующим образом: периодический сигнал $x_n(T)$ с периодом в N отсчетов можно представить в виде суммы N соответствующих комплексных дискретных экспонент, действительные части которых представляют собой косинусойды с амплитудами $|X(0)|,|X(j\cdot 1\cdot\Omega)|,|X(j\cdot 2\cdot\Omega)|,\ldots|X(j\cdot(N-1)\cdot\Omega)|$, угловыми частотами $0,\Omega,2\Omega,(N-1)\Omega$ и начальными фазами $\arg X(0),\arg X(j\cdot 1\cdot\Omega)\ldots\arg X(j\cdot(N-1)\cdot\Omega)$.

1.3 Векторное представление речевого сигнала

Для обработки, преобразования речевого сигнала применяются различные технические области программирования. Учитывая тот факт, что программный код способен воспринять речевой сигнал в виде массива мнгновенных значений сигнала определенной длительности, необходимо рассмотреть сигнал как вектор некоторого бесконечного пространства

Любая совокупность n линейно независимых векторов n – мерного пространства, в котором каждый вектор единственным образом может быть представлен в виде линейной комбинации векторов данной совокупности называется его *базисом*.

Гильбертово пространство – нормированное векторное пространство, бесконечномерное Евклидово пространство.

Пространство также можно назвать *метрическим*, если в его области существует *метрика* – расстояние между элементами пространства (*векторами*).

Важную роль среди линейных метрических пространств играют *нормированные пространства,* в которых каждому вектору $\vec{S}(t)$ соответствует его длина, т. е. *норма* $\left\|\vec{S}\right\|$.

Норма для вещественных аналоговых сигналов:

$$\left\|\vec{S}\right\| = \sqrt{\int_{-\infty}^{+\infty} s^2(t)dt}\,. \qquad (1.19)$$

Норма для комплексных сигналов:

$$\left\|\vec{S}\right\| = \sqrt{\int_{-\infty}^{+\infty} s(t)\cdot s^*(t)dt} \qquad (1.20)$$

Энергия сигнала есть квадрат его нормы. Данная величина определяется выражением:

$$E_S = \left\|\vec{S}\right\|^2 = \int_{-\infty}^{+\infty} s^2(t)dt \qquad (1.21)$$

Взаимная энергия двух сигналов $\vec{S}_i$ и $\vec{S}_j$ определяется их скалярным произведением:

$$E_{ij} = 2\int_{-\infty}^{+\infty} s_i \cdot s_j dt \qquad (1.22)$$

причем, если равенство (1.22) принимает значение 0, т. е. сигналы обладают нулевой взаимной энергией, то они являются *ортогональными*.

Если в пространстве сигналов с конечной энергией существует бесконечное множество взаимоортогональных функций $\{\psi_i\}$, норма которых равна 1, базис является *ортонормированным.*

Классической системой ортонормированных кусочно – постоянных функций меандрового типа, определенных на интервале [0,1] является *система функций Хаара* [6, 1].

При спектральной обработке сигнала удобно использовать ненормированный базис Хаара ввиду отсутствия многозначности функций. В данном случае, значения элементов базиса будут соответствовать 0, либо же ±1.

Ортогональность данного базиса доказывает выражение:

$$\int_{o}^{1} h(k,z)h(p,z)dz = 0 \qquad (1.23)$$

при $k \neq p$. $h(k,z)$ – функции базиса Хаара.

На рисунке 2 представлен базис Хаара из восьми функций:

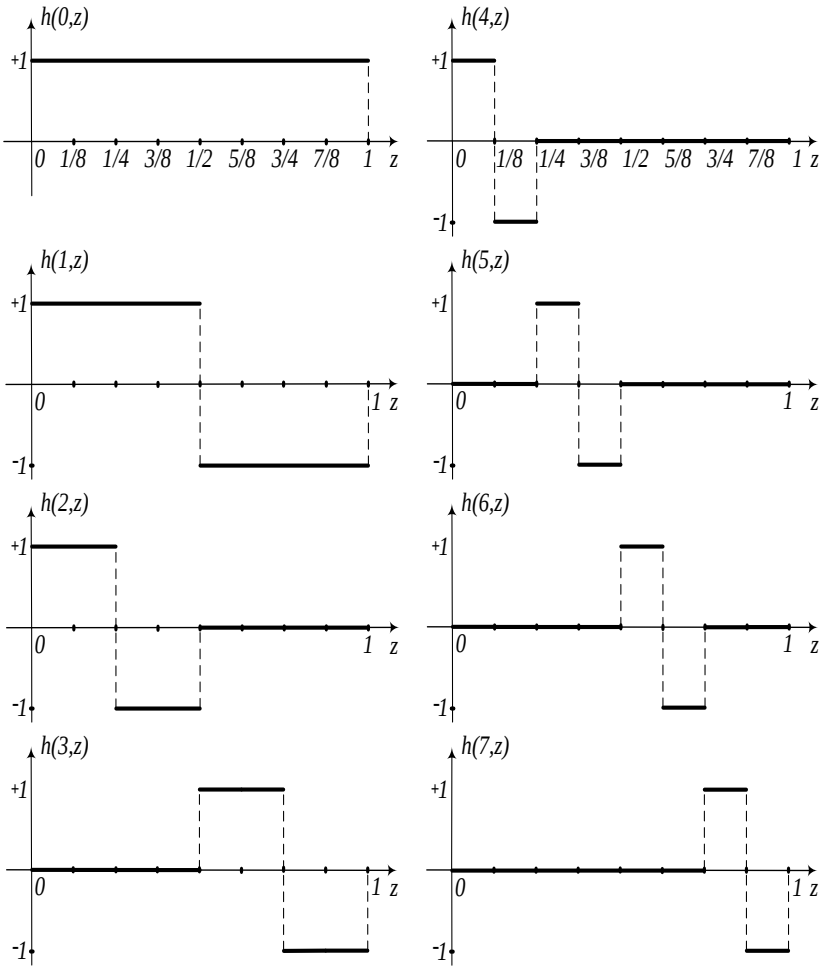

Рисунок 1.2 – Система функций Хаара для *N=8*

Однако система функций Хаара является не оптимальной для кодирования информации по причине недостаточной простоты функций – т. е. конечности набора значений.

В данном случае, преимуществом обладает *Система Радемахера*, построенная на основе системы Хаара методом сложения и нормировки функций Хаара, имеющих идентичный нижний индекс.

Функция Радемахера с номером *k* определяется:

$$R_k = sign\left(\sin 2^k \cdot \pi \cdot t\right), t \in [0,1] \tag{1.24}$$

причем для знака аргумента выполняется условие:

$$sign(x) = \begin{cases} 1, x > 0; \\ -1, x < 0 \end{cases} \tag{1.25}$$

Итак, функция определена на отрезке от 0 до 1.

Функция R_0 *(k=0)* является постулированной, поскольку она равна 1 на всей области определения. Последующая функция R_1 *(k=1)* определяется по формуле (1.26):

$$R_1 = sign\left(\sin 2^1 \cdot \pi \cdot t\right) = \sin 2 \cdot \pi \cdot t, t \in [0,1] \tag{1.26}$$

За время, когда t изменяется от 0 до 1, аргумент синуса меняется от 0 до 2π, то есть преодолевает всю окружность(Рисунок 1.3).

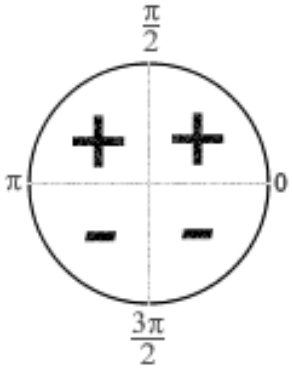

Рисунок 1.2 – Окружность синусоидальной функции

Учитывая, что выше *Ox* значения функции синус положительные, а ниже – отрицательные, формируется функция Радемахера, в которой первая половина принадлежит +1, а вторая -1(Рисунок 1.4):

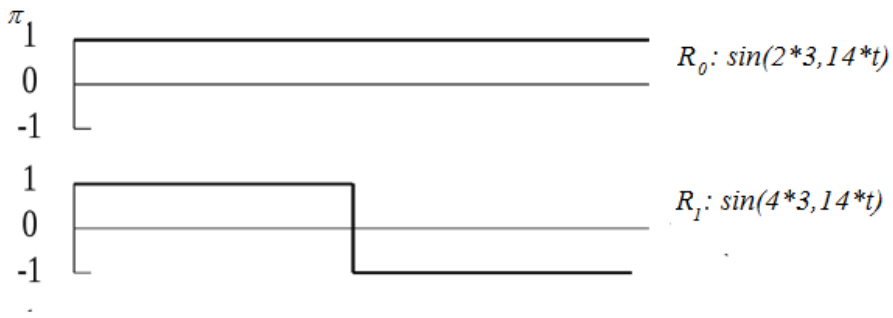

Рисунок 1.4 – Нулевая и первая функции Радемахера

На рисунке 1.5 представлены первые 4 функции Радемахера:

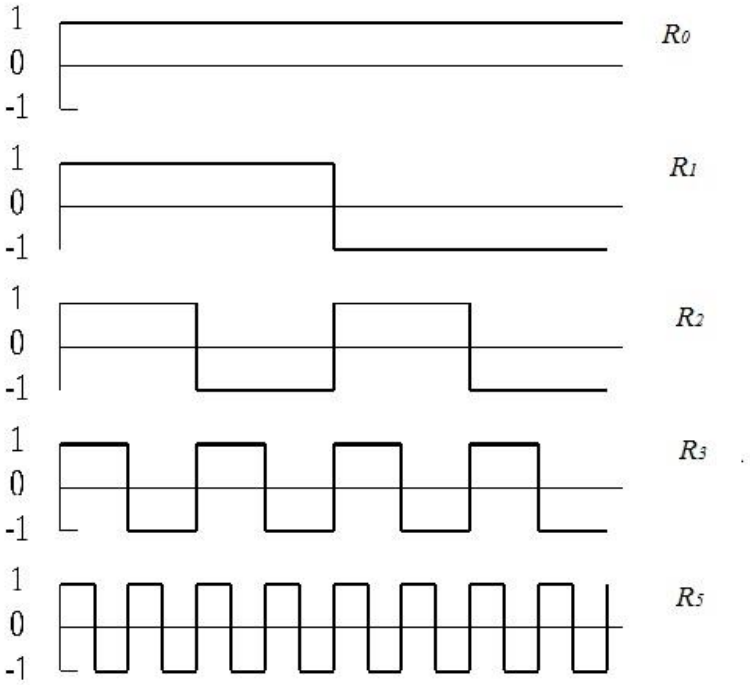

Рисунок 1.3 – Функции Радемахера

Видно, что по мере увеличение номера функции, увеличивается количество меандровых волн, принадлежащих отрезку [0, 1]. Иными словами, Чем больше индекс рассматриваемой функции, тем более детально просматриваются особенности построения некоторой функции в базисе, составленном из данных функций. Очевидно, что все эти функции

взаимоортогональны, поскольку, если взять скалярное произведение любых двух функций из данного базиса, то в результате взятия интеграла получится одинаковое количество +1 и -1, которые скомпенсируют друг друга.

С помощью функций Радемахера можно построить *ортонормированную систему Уолша*.

Система Уолша – система взаимоортогональных ортонормированных функций, принимающих значения ±1 в области $\left[-\frac{T}{2}:\frac{T}{2}\right]$.

Свойства ортогональности позволяют осуществлять оптимальное кодирование в речевом сигнале.

Базис Уолша обладает свойствами ортогональности и мультипликативности:

1) Ортогональность: $wal(n,\theta)\cdot wal(k,\theta)=0$, $k\neq n$

2) Мультипликативность: $wal(n,\theta)\cdot wal(k,\theta)=wal(i,\theta)$, где $i=n\oplus k$.

Данная система определяется формулой:

$$wal_n(t)=R_{n+1}(t)\cdot R_{n+1}(t)\cdot\ldots\cdot R_{k+1}(t), t\in[0,1] \qquad (1.26)$$

где $R_{n+1}(t)$, *[i=1,k]* – функции системы Радемахера.

Попарную ортогональность функций системы Уолша в Гильбертовом пространстве можно доказать следующим образом. Положим, используются различные номера *n* и *l*, причем:

$$\begin{aligned} n &= 2^{v1}+2^{v2}+\ldots+2^{vp}, 0\le v_1<v_2<\ldots<v_p;\\ l &= 2^{\eta 1}+2^{\eta 2}+\ldots+2^{\eta q}, 0\le \eta_1<\eta_2<\ldots<\eta_q. \end{aligned} \qquad (1.27)$$

Склалярное произведение находится следующим образом:

$$(w_n,w_l)=\int_0^1 w_n(x)\cdot w_l(x)dx=\int_0^1 (r_{v1+1}(x)..r_{vp+1}(x))\cdot(r_{\eta 1+1}(x)...r_{\eta q+1}(x))dx \qquad (1.28)$$

где $x\in[0,1]$, r_v – функция Радемахера.

Из произведения $(r_{v1+1}(x)...r_{vp+1}(x))\cdot(r_{\eta 1+1}(x)...r_{\eta q+1}(x))$ в подынтегральном выражении необходимо удалить пары с одинаковым индексом:

$$(r_{v1+1}(x)...r_{vp+1}(x))\cdot(r_{\eta 1+1}(x)...r_{\eta q+1}(x)) = r_{j1}(x)r_{j2}...r_{jk}(x), \quad (1.29)$$

где $1 \le j_1 < j_2 < ... < j_k$ (равенство выполняется почти всюду на отрезке [0,1].

Согласно определению системы Радемахера, произведение функций с меньшими индексами $r_{j1}(x)r_{j2(x)}\ldots r_{jk-1}(x)$ это кусочно – постоянная функция, элементы которой равны *+1* и *-1*, а каждый интервал постоянства $E_i=(a_i,b_i)$ разбивается функцией $r_{jk}(x)$ с более высоким индексом на четное количество интервалов равной длины, причем функция попеременно принимает значения *+1* и *-1* . Поэтому для любого интервала $E_i=(a_i,b_i)$ постоянства функции $r_{j1}(x)r_{j2(x)}\ldots r_{jk-1}(x)$, получается:

$$\int_{Ei}(r_{j1}(x)r_{j2}(x)...r_{jk-1}(x))r_{jk}(x)dx = \pm 1\int_{Ei} r_{jk}(x)dx = 0. \quad (1.30)$$

В результате, просуммировав эти равенства по всем интервалам постоянства, получается:

$$\int_0^1 r_{j1}(x)r_{j2}(x)...r_{jk}(x)dx = \sum_i \int_{Ei}(r_{j1}(x)r_{j2}(x)...r_{jk-1}(x))r_{jk}(x)dx = 0. \quad (1.31)$$

Из равенства следует, что для всех $n \ne l$:

$$(wal_n, wal_l) = \int_0^1 wal_n(x)wal_l(x)dx = \int_0^1 r_{j1}(x)r_{j2}(x)...r_{jk}(x)dx = 0. \quad (1.32)$$

Исходя из того, что квадрат любой функции Радемахера равен 1 почти всюду на отрезке [0,1]:

$$wal_n^2(x) = r_{v1+1}^2(x) r_{v2+1}^2(x)$$
$$r_{vp+1}^2(x) = 1 \qquad (1.33)$$

значит для всех *n=0, 1, 2…*норма:

$$\| wal_n \| = \sqrt{\int_0^1 wal_n^2(x)dx = 1.} \qquad (1.34)$$

Итак, система функций Уолша $\{wal_n(x)\} \in [0,\infty)$ является ортонормированным базисом на отрезке [0,1], а система Радемахера есть подмножество системы Уолша.

В процессе исследования всреде Matlab был сформирован ортогональный базис $\vec{u}_n$, но необходимо убедиться, что его элементы не искажены, для этого необходимо задать взаимопротивоположные гипотезы и осуществить проверку.

Гипотеза H_0 – базис $\vec{u}_n$ ортогонален;

Альтернативная гипотеза H_1 - базис $\vec{u}_n$ не ортогонален.

На данном этапе необходимо проверить гипотезу H_0. Ортогональность данного базиса наблюдается в особенности его построения. В этом можно убедиться, проверив аналитически условие ортогональности для каждой пары вектор – столбцов данного базиса. В данном случае, матрицу $\vec{u}_n$ составляет набор из 9 функций (9 вектор – столбцов): $\langle \vec{u}_1, \vec{u}_1 \rangle, \langle \vec{u}_2, \vec{u}_2 \rangle ... \langle \vec{u}_9, \vec{u}_9 \rangle$. Предлагается попарно выделять элементы базиса и находить их скалярное произведение. Таким образом, если скалярное произведение всех векторных пар будет равно машинному нулю, ортогональность базиса с использованием основного условия данного критерия будет доказана.

При этом, необходимо учитывать некоторые свойства, ввиду которых, не все пары будут включены в расчет.

Во – первых, используя свойство скалярного произведение вектора самого на себя, при котором результат может быть не только равен 1, но и быть больше на величину δ , необходимо исключить пары, имеющие одинаковый индекс номера:

$$\langle \vec{u}_i, \vec{u}_i \rangle = \|\vec{u}_i\|^2 = 1 \cdot \delta, \tag{1.35}$$

где $\|\vec{u}_i\|^2$ - энергия функции, δ - величина сдвига.

Во – вторых, используя свойство коммуникативности, при котором, от перестановки множителей результат один и тот же, следует исключить пары с идентичными индексами противоположных элементов:

$$\langle \vec{u}_i, \vec{u}_j \rangle = \langle \vec{u}_j, \vec{u}_i \rangle \tag{1.36}$$

Таким образом, зная понятия и свойства наиболее оптимальных с точки зрения обработки сигналов базисов, можно выбрать наиболее оптимальную систему для кодирования информационного сообщения в речевой сигнал.

2 МЕТОДЫ СКРЫТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Современные возможности сферы цифровой обработки сигналов позволяют не только производить качественную и количественную оценку аудиоконтента , но и рассмотреть его как среду для скрытия и шифрования в нём каких либо данных. Эти процессы детально отражены во взаимодействующих науках: криптография и стеганография.

Криптография – это наука, изучающая процесс преобразования информации за счет её шифрования с целью её сокрытия от несанкционированного доступа злоумышленника (криптоаналитика) и других неавторизованных лиц.

Сам факт скрытия информации ещё не является полноценным гарантом её защиты, поскольку он дает понять злоумышленнику, что в передаваемом сообщении содержатся данные, имеющие какую-либо ценность. Для решения данной проблемы существует понятие стеганографии:

Стеганография – наука, изучающая методы скрытия самого факта наличия секретных данных при их передаче, обработке и хранении.

Существует три основных направления применения стеганографии:

1. Скрытие факта передачи информации;
2. Скрытие самой информации при её передаче;
3. Аутентификация пользователя.

Скрытная передача информации заключается в проблеме, при получении информации *криптоаналитиком* [22], человеком, который осуществляет попытки несанкционированного доступа к передаваемой информации.

Для осуществления кодирования, обеспечивающего скрытность передачи информации, необходимо воспользоваться одним из методов *цифровой стеганографии*[5]. В различных источниках [3, 5, 10] данное понятие стеганографического кодирования трактуется как процесс, при котором в одни битовые последовательности, имеющие аналоговую природу, надежно и незаметно встраиваются другие последовательности бит.

Существуют различные способы применения цифровой стеганографии:

- Встраивание информации с целью ее скрытой передачи;
- Внедрение ЦВЗ (ЦВЗ – цифровой знак);
- Внедрение заголовков;
- Внедрение идентификационных номеров.

Алгоритмы внедрения секретной информации также можно следующие группы:

алгоритмы, работающие непосредственно с цифровым сигналом (например, метод LSB);

наложение скрытой информации (текстовой или мультимедийной) поверх оригинала. (актуален при внедрении ЦВЗ);

использование особенностей форматов файлов.

Для стеганографического кодирования речевых данных наиболее приемлемы следующие методы:

Метод наименьшего значащего бита (LSB - Least Significant Bit). Основная идея: произвести замену последних значащих бит в контейнере речевого сигнала на биты скрываемого сообщения. Недостаток данного метода заключается в ограниченной устойчивости к различным видам атак, а значит, данные методы разумно реализовывать лишь при отсутствии шума в канале связи.

Эхо-методы. Основная идея реализуется с использованем эхо-сигналов, которым соответствует свое значение задержки, начальной амплитуды и степени затухания. Чтобы закодировать битовую последовательность, необходимо задействовать интервалы между эхо-сигналами. В свою очередь, интервалы не равномерны. Чтобы сделать искажения, вызванные кодированием незаметными для слуховой системы, необходимо установить некоторый порог слияния эхо и сигнала. Преимуществом метода является стойкость к атакам, взаимодействующим с фазой и амплитудой. Недостатком является возможная недостоверность считываемости, т. е. ошибочное принятие 0 за 1 и наоборот.

Суть *фазового кодирования* заключается в том, чтобы заменить исходный звуковой элемент на скрытое сообщение, в качестве которого выступает относительная фаза. Это один из наиболее эффективных методов цифровой стеганографии.

Сетевая стеганография. Метод основан на том, что стегоконтейнером являютя протоколы модели OSI (взаимодействия открытых систем). Информация передается по скрытому каналу, при этом изменяется структура передачи пакета в сетевом протоколе. Типичный пример сетевой стеганографии основан на изменении свойств одного из сетевых протоколов, а также использование взаимосвязи между двумя или более различными протоколами для улучшения надежности секретности передачи сообщения.

Метод расширенного спектра. Основная идея заключается во внедрении в контейнер случайной последовательности, а затем процесс её детектирования с помощью согласованного фильтра. Таким образом, в контейнер можно встраивать несколько сообщений так, что они не будут создавать друг другу помех.

Проанализировав все перечисленные методы, было выявлено, что эхо - методы и методы фазового кодирования не подходят для проведения эксперимента по причине малой ёмкости и недостаточной стойкости эхо – сигнала. Использование метода расширения спектра позволяет скрывать и передавать информацию не по биту, а в виде потока данных, следовательно, этот метод весьма оптимален для выполнения эксперимента.

2.1 Анализ метода расширения спектра

Наиболее эффективным способом защита аудиоконтента от несанкционированного доступа является встраивание в сигнал специальной цифровой метки, которую нельзя идентифицировать без специального ключа

либо программного обеспечения. Данная метка называется *цифровым водяным знаком (ЦВЗ)*.

Алгоритмы, применяемые для аудиосигналов, реализуются и функционируют с учетом некоторых свойств слухового аппарата и самого звукового сигнала. Слуховая система человека функционирует в широком динамическом диапазоне, поэтому, помимо информативных данных, слушатель проявляет высокую чувствительность к аддитивному флотационному шуму, иными словами, к *белому шуму*. Несмотря на способность слышать и распознавать звуки широкого динамического диапазона, система слуха характеризуется достаточно малым разностным диапазоном. Ввиду этого, звуки, произнесенные с большей громкостью маскируют наименее слышимые.

Метод расширения спектра функционирует во временной области сигнала и используется для шифрования информационного потока. Скрываемые данные при этом оказываются рассредоточенными в пределах всего спектра частот. Таким образом, в случае воздействия помех сигнал всё-равно будет передан.

Расширение спектра прямой последовательностью (РСПП) – метод, при котором информационный сигнал расширяется за счет его умножения на *элементарную посылку* – псевдослучайную последовательность (ПСП), имеющую максимальную длину и модулированную известной частотой.

Сообщение - это секретная информация, наличие которой необходимо скрыть.

Контейнером называется несекретная информация, которую можно использовать для скрытия в ней сообщения.

По наличию или отсутствию содержимой стеганоинформации контейнеры подразделяются на:

Контейнер – оригинал «c», т. е. пустой, не содержащий стеганоинформации;

Контейнер – результат (*Стегоконтейнер*) «c\» - заполненный и содержащий скрытую информацию m.

Следует отметить, что для качественной передачи необходимо, чтобы контейнер – результат нельзя было визуально отличить от контейнера – оригинала.

Сигнал – контейнер является дискретным, благодаря чему имеется возможность правильного определения границ ПСП с целью фазовой синхронизации. Для шифрования и дешифрования информации при РСПП используется единый ключ – псевдослучайный (белый) шум.

Идея данного метода заключается в следующем: сообщение (сигнал, содержащий какие-либо данные) умножается на сигнал несущей и на ПСП, спектр которой весьма широк. Вследствие этого, спектр данных расишряется в пределах диапазона частотной полосы. Полученные данные ослабляются и в качестве аддитивного шума прибавляются к исходному сигналу.

На рисунке 6 представлена структурная схема кодека с применением расширения спектра:

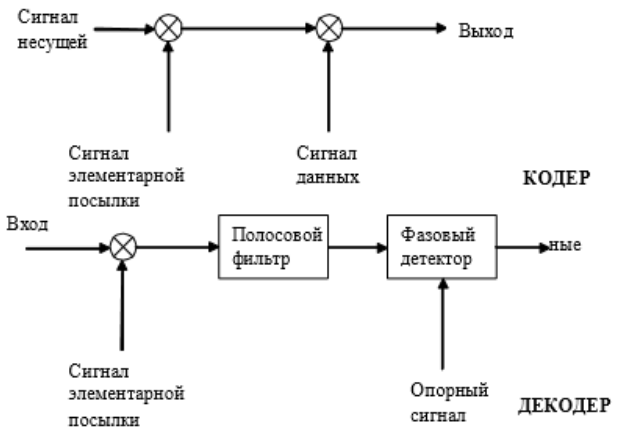

Рисунок 2.1 – Структурная схема кодека с расширением спектра

Синтез информации при данном методе с шифрованием прямой последовательностью, показан на рисунке 7:

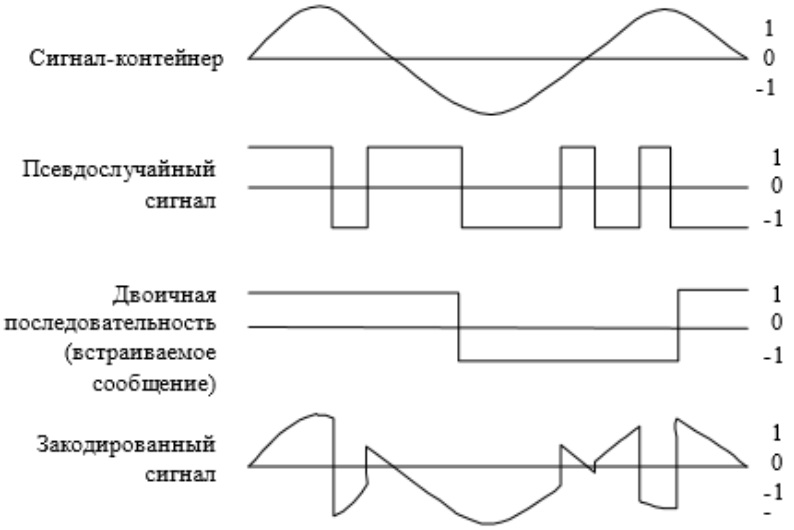

Рисунок 2.2 – Изменение сигнала при кодировании с расширением спектра

Как видно из рисунка 2.2, фаза сигнала с ПСП чередуется с фазой, которая промодулированна последовательностью ±1. Таким образом можно сказать, что речь идет о двоичной фазовой манипуляции. При извлечении фазовые значения ϕ_0 и $\phi_0 + \pi$ представлены битовыми значениями 1 и 0, с помощью которых была закодирована последовательность битовых данных.

Для реализации кодирования необходимо учитывать некоторые положения:

- ПС ключ есть последовательность (M) с максимально возможным и равномерно рассредоточенным набором комбинаций;

- Сигнал синхронизирован;

- Аналитик при приеме владеет следующей информацией: поток ключей, границы расширенных данных, частота следования ПСП, скорость передачи данных и вид несущей.

Реализация программного алгоритма метода РСПП:

1. Ввод начальных данных: речевой материал, имеющий длину I бит и сообщения, подлежащего скрытию, длиной L_M бит.

Для того, чтобы скрыть сообщение размерностью L_M бит в речевой сигнал-контейнер, необходимо сегментировать контейнер на L_M отрезков, длина которых прописывается в программном коде, как:

SegLen= Math.Floor(I);

где *Math.Floor()* – округление до целого числа в меньшую сторону [10].

В каждый сегмент пощмещается 1 бит информации.

2. ПСП с минимальной длиной seglen элементов, представленная значениями ± 1 генерируется для каждого информационного бита. длиной. Генератором ПСП возможно назначить регистр сдвига с линейной обратной связью (РСЛОС) [10] *Регистр сдвига* есть битовая последовательность разрядов *r*. Их количество *d* соответствует длине регистра сдвига. Сумма по модулю 2 определенных битов регистра есть *обратная связь*.

В теории, d-битовый РСЛОС может находиться в каком-либо внутреннем состоянии из из $2^d - 1$ (период генерирования ПСП).

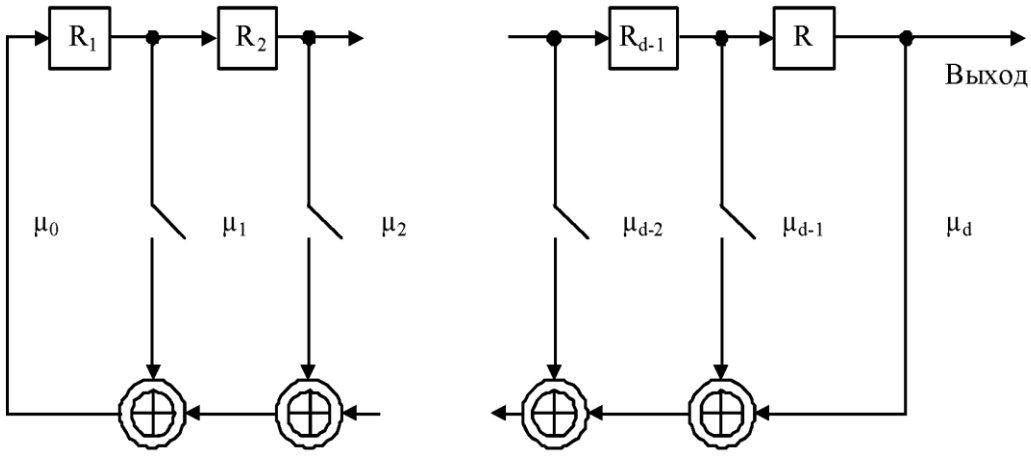

Рисунок 2.3 - Обобщенная схема работы регистра сдвига с линейной обратной связью

При этом наблюдается последовательность:

$$p(x) = \mu_0 x^0 + \mu_1 x^1 + ... + \mu_d x^d, \quad (2.1)$$

где μ_i *(i = 0, 1, …, d)* - весовые коэффициенты полинома степени d.

При этом, состояние $\mu_i = 1$ *означает*, что ключ замкнут, а состояние $\mu_i = 0$ говорит о том, что ключ разомкнут.

Необходимое количество разрядов регистра вычисляется как $Math.Ceiling(\log_2 SegLen))$, где *Math.Ceiling()* – оператор округления в большую сторону.

Наименьший значащий бит состояния регистра определяет конечную последовательность. На выходе получается последовательность 0 и 1, преобразованная в последовательность ±1.

3. Производится встраивание информационных бит в сигнал-контейнер. Символы сообщения преобразовываются в вектор значений ±1, после чего контейнер равномерно сегментируется, причем одному биту соответствует один сегмент. С помощью сгенерированной ПСП полученные биты накладываются на сегменты пустого контейнера за счет преобразования каждого 16-битного отсчета в сегменте. Энергию ЦВЗ задает параметр *alpha*, который варьируется в зависимости от условий стойкости ЦВЗ. Оптимальное значение данного параметра составляет примерно 0,01 (1 % искажения пустого контейнера). Далее преобразованныые сегменты суммируются в один вектор, причем после встраивания крайнего информационного бита длина вектора увеличивается за счет не преобразованных элементов пустого контейнера, соответствуя длине исходного сигнала. По завершению встраивания ЦВЗ стегоконтейнер объединяется с непреобразованным каналом и загружается в файл формата WAV.

4. Последним шагом является декодирование, т. е. извлечение информационных данных. Аналитик на приемной стороне должен иметь оригинальный аудиофайл, знать численное значение *SegLen*,+. При считывании ЦВЗ из стегоконтейнера применяется ПСП, использууемая для кодирования. Разница между исходным и синтезированным сигналом посегментно анализируется, причем берется усредненное значение сегмента, в результате чего определяются закодированные значения (1, если знак разницы сигналов положительный или 0, если отрицательный).

Среди достоинств вышеуказанного метода стоит отметить высокий показатель скрытности и устойчивость к модификации, однако емкость речевых данных используется не достаточно эффективно.

2.2 Анализ модифицированного метода расширения спектра и алгоритмов его реализующих

Метод расширения спектра [22, 26] довольно часто применяется при обработке речевых сигналов, его можно описать выражением:

$$\tilde{\vec{y}} = \vec{y} + k \cdot e \cdot \vec{u} - \alpha \cdot e \cdot \vec{u}\ ;\ \alpha = \langle \vec{y}, \vec{u} \rangle, \quad (2.2)$$

где $\vec{y}$ – исходный отрезок (речевой материал); $\tilde{\vec{y}}$ – отрезок содержащий стеганографически закодированную информацию (стегоконтейнер); $\vec{u}$ - псевдослучайная последовательность (ПСП); α – множитель определяющий взаимную энергию ПСП и исходного отрезка; k – коэффициент определяющий скрытность и стойкость стеганографически кодируемой информации; e – ортонормальное представление кодируемого бита информации:

$$e = 2b - 1, \quad (2.3)$$

где b – кодируемый бит.

Декодирование информации из стегоконтейнера происходит посредством определения знака скалярного произведения отрезка речевых данных содержащих информацию и ПСП:

$$\tilde{e} = sign\left(\langle \tilde{\vec{y}}, \vec{u} \rangle\right), \quad (2.4)$$

где $sign(\ )$ – операция выделения знака; $\tilde{e}$ – ортонормальное представление декодируемого бита информации.

$$\tilde{b} = (\tilde{e} + 1)/2, \qquad (2.5)$$

где $\tilde{e}$ – бит декодируемой информации.

Для повышения емкости в качестве ПСП последовательности предлагается использовать ортогональный базис, энергия каждой функции которого равна единице:

$$\|\vec{u}_i\|^2 = 1; \; i = 1,2,...9. \qquad (2.6)$$

На рисунке 2.4 – 2.5 представлены сигналы, принадлежащие одному из ортогональных базисов полученных на основе функций Радемахера.

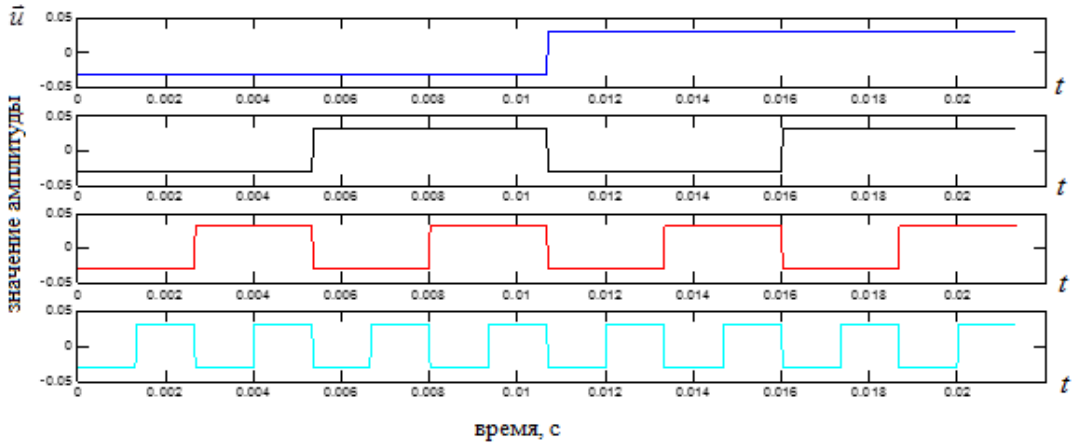

Рисунок 2.4 - Ортогональный базис Радемахера (функция *rad₁, rad₂, rad₃, rad₄*)

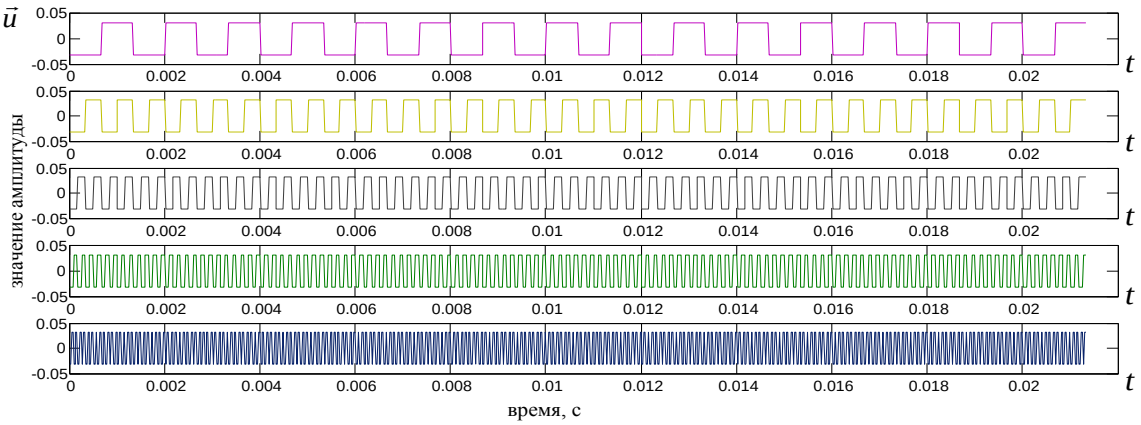

Рисунок 2.5 - Ортогональный базис Радемахера (функция *rad₅, rad₆, rad₇, rad₈, rad₉*)

Для кодирования используется ортонормальный базис, содержащий ортогональные друг другу функции $\vec{u}$ и представляется в виде матрицы **U** размерности $[M \times N]$:

$$\mathbf{U} = (\vec{u}_1, ..., \vec{u}_m, ..., \vec{u}_M);\ \vec{u}_m = rad_m;\ rad_m(i) = sign(\sin(2^m \cdot 2\pi \cdot i)),\ i = 1, \ldots, N, \quad (2.7)$$

где M – количество строк матрицы **U**, зависящее от объема скрываемого сообщения $\vec{x}$:

$$\vec{x} = (x_1, ..., x_i, ..., x_M)^T, \quad (2.8)$$

где $\vec{x}$ – отрезок данных соответствующий цифровому представлению речевого сигнала (речевое сообщение).

Учитывая вышеописанные подходы модель (2.2), для осуществления скрытной передачи речевого сообщения в речевых данных, примет вид:

$$\tilde{\vec{y}} = \vec{y} - \beta \cdot \vec{w} + k \cdot (\vec{x} \cdot \mathbf{U});\ \vec{w} = \sum_{i=1}^{M} \vec{u}_i;\ \beta = \langle \vec{y}, \vec{w} \rangle, \quad (2.9)$$

где $\vec{w}$ – сигнально-кодовая конструкция отображающая речевое сообщение, длительностью M отчетов.

Для декодирования речевого сообщения, необходимо для каждого отчета выполнить свертку вида:

$$\tilde{x}_i = \left\langle \tilde{\vec{y}}, \vec{u}_i \right\rangle;\ i = 1,2,..., M;\ \tilde{\vec{x}} = (\tilde{x}_1, ..., \tilde{x}_i, ..., \tilde{x}_M)^T, \quad (2.10)$$

где $\tilde{\vec{x}}$ – декодированный отрезок данных соответствующий цифровому представлению переданного речевого сигнала (речевое сообщение).

Речевой сигнал, записанный с частотой дискретизации Fs был разбит на равное количество отрезков, соответствующих *i-й букве (i=1,…,Z)* и имеющих

определённую длительность T в секундах. В программном коде отсчеты в секундах необходимо вводить.

Количество отсчетов одного окна:

$$N = F_s \cdot T\,. \tag{2.11}$$

Следовательно, в Z*й* отрезок, содержащий N отсчетов, можно закодировать количество бит, определяемое по формуле:

$$n = \log_2 N\,. \tag{2.12}$$

При частоте дискретизации Fs и известном количестве отсчетов, приходящихся на Z*й* отрезок, можно также определить количество отрезков для анализа и кодирования информации:

$$Z = \frac{F_s}{N}. \tag{2.13}$$

Таким образом, если в 1сек можно поместить *n* отсчетов, то в весь РС помещается количество отсчетов, определяемое следующим образом:

$$L = Z \cdot n\,. \tag{2.14}$$

Каждая буква слова, подверженная шифрованию, имеет размерность примерно 100-300 отсчетов. В данных условиях, с целью полного скрытия необходимой информации (РС, слово – фрагмент предложения) необходимо записать её с частотой дискретизации Fs=8кГц. Это позволит поместить по одной букве, имеющей размерность, примерно, 100 – 300 отсчетов, в каждый контейнер $\vec{y}$.

Предполагается, что в качестве контейнера $\vec{y}$ для скрытия данных берется РС с частотой дискретизации Fs=48 кГц. Для осуществления кодирования был сформирован ортогональный базис, представленный на Рисунке 2.4 – 2.5.

Словестный алгоритм формирования базиса Радемахера

Ввод**:** *T, Fs;*

Вывод: $\vec{u}_n$.

1. Начало;
2. Ввести длительность отрезка T;
3. Рассчитать количество отсчетов для одного окна: *N=fix(Fs*T);*
4. Рассчитать длительность прямоугольного импульса *dN=N/2*;
5. Задать начальное количество базисных функций (столбцов) *J=0*;
6. Задать условие: *dN>1/Fs*
7. Задать количество строк: *I= -1*;
8. Увеличить количество базисных функций: *J=J+1*;
9. Задать элемент начальной размерности: *n=1*;
10. Задать условие: *n<N*;
11. Найти количество строк *I* как элементов базиса *u*, от *n* до *J* с шагом *n+dN-1: u(n:n+dN-1,J)=I*;
12. Осуществить смену знака для *I*: *I=-1*I*;
13. Переприсвоить n на отрезок длительности *dN* больше: *n=n+dN*;
14. Осуществить проверку условия: *dN>1/Fs*:
    - если *dN>1/Fs*, вернуться к п. 8;
    - если *dN<1/Fs*, завершить цикл и перейти к п. 13;
15. Осуществить разбиение фронта прямоугольного импульса *dN=dN/2*;
16. Осуществить проверку условия: *dN>1/Fs*:
    - если *dN>1/Fs*, вернуться к п. 5;
    - если *dN<1/Fs*, завершить цикл и перейти к п. 15;
17. Осуществить цикл: нормировку базиса к 1 для каждого столбца: *j=1:J;*

18. Просуммировать квадрат каждого столбца матрицы (базисной функции) *u*, найдя тем самым энергию матрицы *Eu*: *Eu=sum(u(:,j).^2);*

19. Сформировать нормированную базисную функцию un как частное каждого *j*го столбца матрицы u и корня из *Eu*: *un(:,j)=u(:,j)/sqrt(Eu)* ;

20. Вывод базисной функции u;

21. Вывод нормированной базисной функции un;

22. Конец.

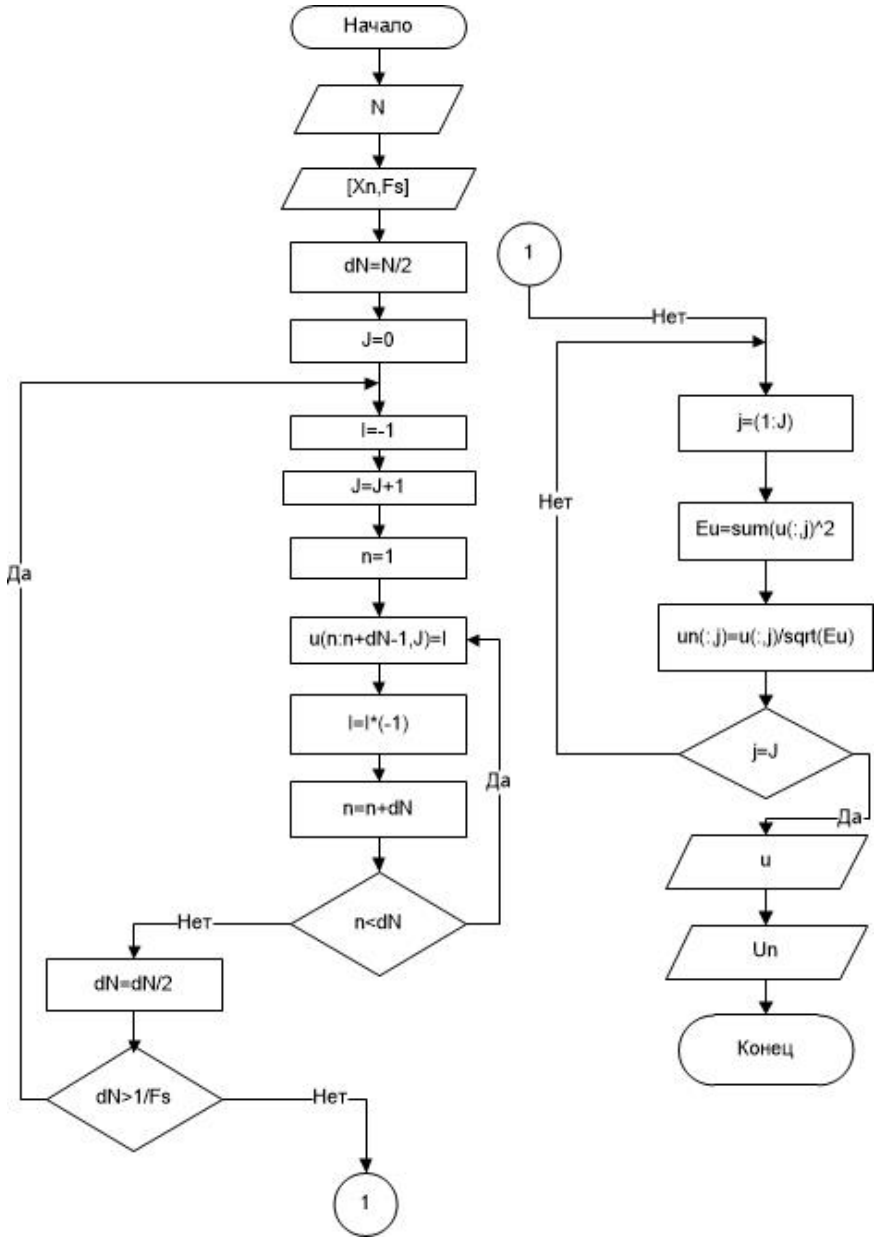

Рисунок 2.6 – Блок-схема формирования ортогонального базиса

Ортогональный базис для кодирования сформирован. Далее необходимо скрыть в контейнере $\vec{y}$ аудиосигнал, $\vec{x}$.

Положим, каждый внедренный символ имеет номер *m*. Значит, зная количество анализируемых окон *Z* и границы каждого необходимого окна можно закодировать информацию путём последовательного сложения каждого необходимого окна и скалярного произведения коэффициента внедрения на элемент скрываемого РС $\vec{x}$ и транспонированную функцию ортогонального базиса $\vec{u} = (u_1, ..., \vec{u}_i, ..., \vec{u}_N)$ (элемента вектор - столбца). При этом, необходимо подобрать такое значение коэффициента внедрения *K*, при котором искажения стегоконтейнера будут минимальны. Данная величина является *порогом кодирования*. Кодирование производится в соответствии с формулой (2.9)

В результате данной операции формируется стегоконтейнер $\tilde{\vec{y}}$, состоящий из Z окон, длительностью *(v(z):v(z)+N-1)*.

Словесный алгоритм кодирования:

Ввод: *T*, *K*, [*V*], *Z*, *Wfile*, *fs*, *Xfile*, *Fs*;

Вывод: $\vec{c}$, *Fs*.

1. Начало
2. Ввести длительность сигнла *T*;
3. Задать коэффициент внедрения *K*;
4. Загрузить файл [*V*]– массив нижних границ анализируемых окон предложения x_n;
5. Задать количество анализируемых отрезков *Z*;
6. Загрузить звуковой файл *Wfile* – информация, которую необходимо скрыть, *fs=8000 Гц*;
7. Загрузить звуковой файл - контейнер *Xfile, Fs=48000 Гц*;
8. Назначить счетчик *m=0* - номер внедренного символа;
9. Назначить звук *Xn* файлом – контейнером: *C=Xn*;

10. Назначить счетчик: *z=1:Z* – перебор отрезков с шагом 1;

11. Из контейнера выделить необходимый отрезок *x*: *x=Xn(v(z):v(z)+N-1)*;

12. Назначить счетчик *j=1:J* – перебор вектор – столбцов базисной нормированной матрицы $\overline{un_j}$ с шагом 1;

13. Увеличить счетчик: *m=m+1*;

14. Осуществить кодирование: *x=x+K*W(m)*un(:,j)'*;

15. Осуществить проверку условия: *j=J* :

- если *j<J*, вернуться к п. 11;
- если *j=J* завершить цикл и перейти к п. 15;

16. Присвоить x отрезок контейнера: *C(v(z):v(z)+N-1)=x*;

17. Осуществить проверку условия: *z=Z* :

- если *z<Z*, вернуться к п. 9;
- если *z=Z* завершить цикл и перейти к п. 17;

18. Вывести воспроизводимый стегоконтейнер $\vec{C}$;

19. Конец.

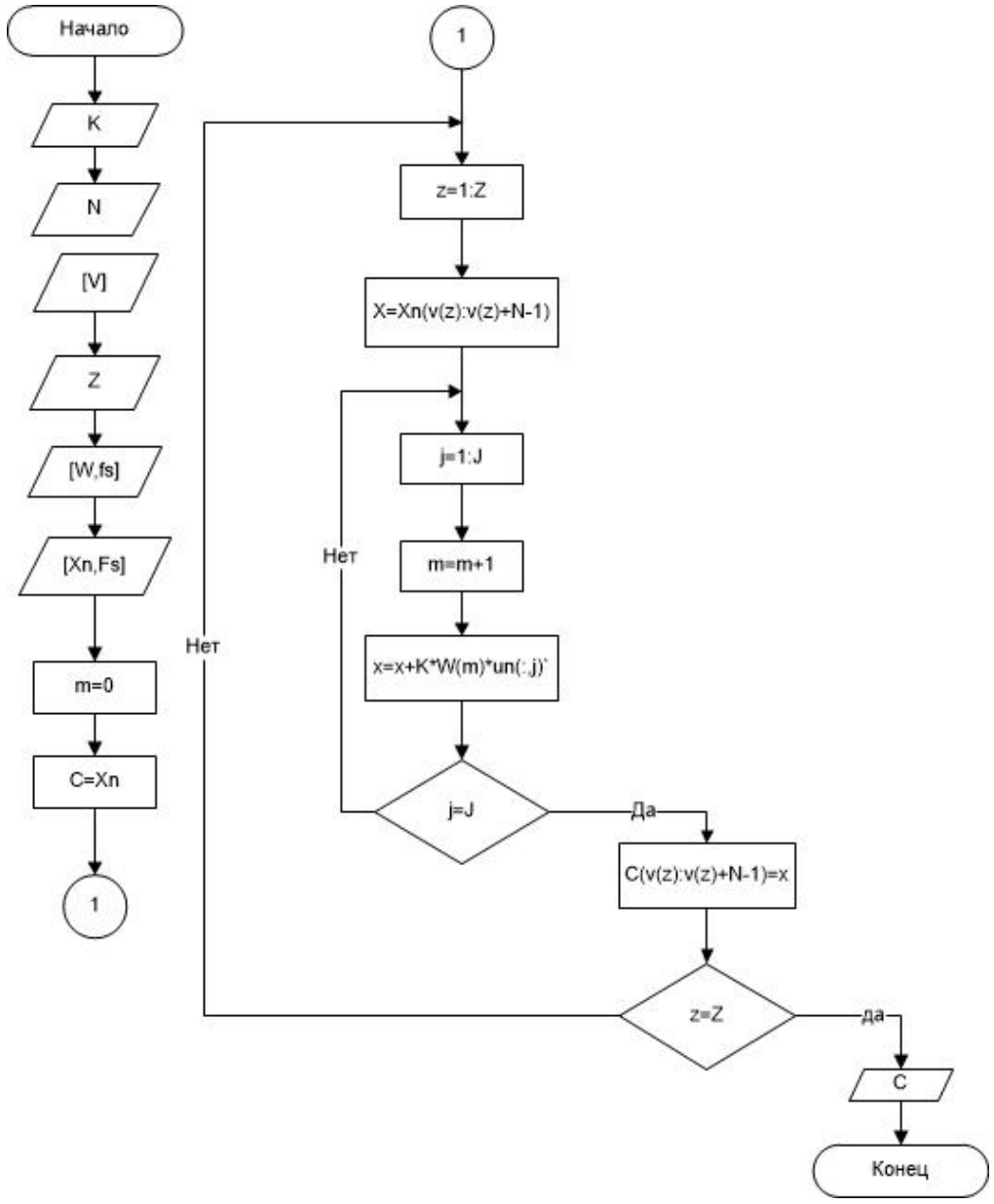

Рисунок 2.7 – Блок-схема кодирования речевого сообщения в РС

С целью корректного проведения эксперимента было реализовано декодирование скрываемой информации. Данный этап позволяет оценить, насколько искажается передаваемое сообщение $\vec{w}$ под воздействием изменения различных параметров сигнала.

Декодирование осуществляется следующим образом:

Предположим, что скрываемое сообщение имеет определенное количество значений. Каждому значению сигнала соответствует скрытый символ *mn*. Следовательно, информацию, которая содержится в отрезке стегоконтейнера,

длиной от *v(z)* до *v(z)+N-1*, можно извлечь, скалярно умножив данный отрезок на транспонированный элемент базисной функции, нормированный к единице (2.10).

Словесный алгоритм декодирования:

Ввод: *T*, $\vec{c}$, *Fs*, [*V*];

Вывод: $\vec{w}_n$, *fs*.

1. Начало;
2. Задать длительность анализируемого отрезка T;
3. Считать стегоконтейнер $\vec{c}$, полученный при кодировании с частотой дискретизации *Fs=8000 Гц*;
4. Загрузить файл [*V*] – массив нижних границ анализируемых отрезков предложения x_n;
5. Определить количество анализируемых отрезков *Z*, исходя из размерности [*V*];
6. Считать сформированную ранее матрицу un;
7. Считать *J* - количество вектор – столбцов нормированой матрицы ;
8. Задать начальное количество скрытых символов *mn=0*;
9. Назначить счетчик: *z=1:Z* – перебор отрезков с шагом 1;
10. Выделить отрезок *s* из стегоконтейнера *C*: *s = C(v(z):v(z)+N-1)* ;
11. Назначить счетчик *J=1:J*;
12. Увеличить номер скрытого символа: *mn=mn+1* ;
13. Осуществить декодирование: $wn(mn)$*=un(:,j)'*s;*
14. Осуществить проверку условия: *j=J* :

- если *j<J*, вернуться к п. 12;
- если *j=J* завершить цикл и перейти к п. 16;

15. Осуществить проверку условия: *z=Z* :

- если *z<Z*, вернуться к п. 10;
- если *z=Z* завершить цикл и перейти к п. 17;

16. Вывести декодированную информацию *wn*
17. Конец.

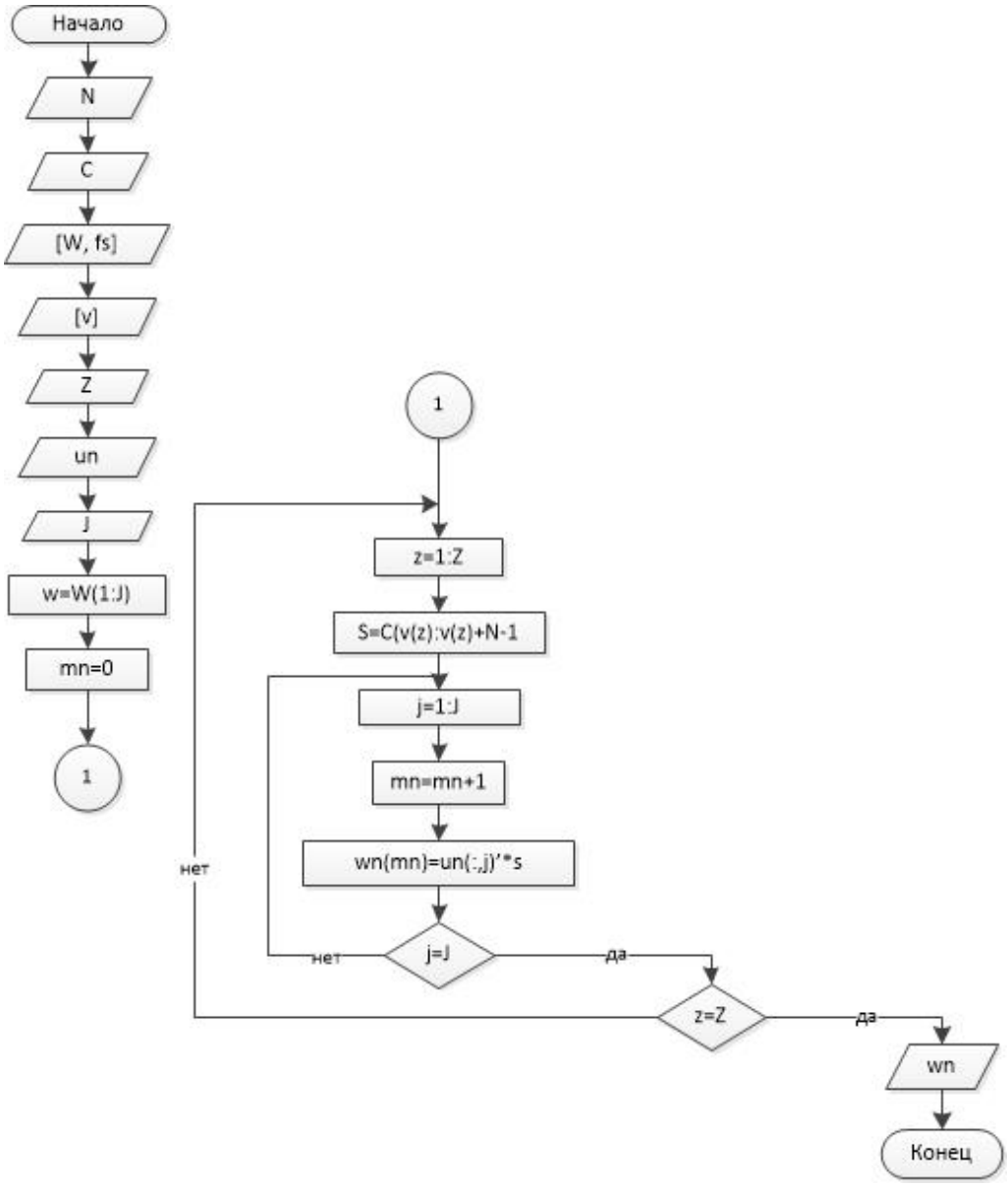

Рисунок 2.8 – Блок-схема декодирования речевого сообщения из РС

В данном разделе была реализована модификация метода расширения спектра посредством использования элементов ортогонального базиса Радемахера, позволяющего скрыть в одном отрезке речевого сигнала не 1 бит информации, а поток данных (примерно 9 бит).

3 ОЦЕНКА СКРЫТНОСТИ РЕЧЕВОГО СООБЩЕНИЯ

3.1 Качественная оценка искажений, вызываемых кодированием сообщения в речевых данных

Для проведения исследования в соответствии с выбранным методом использовались следующие компоненты:

1) Три РС $\vec{y}$, записанные с частотой дискретизации f_d = 48 кГц, разрядностью 16 бит. Параметр частоты дискретизации достаточно велик (соответствует студийной записи речевого материала ГОСТ), что позволит увеличить емкость скрываемой информации.

2) Длительность речевых сигналов $\vec{y}_i$:

N_1=202046, N_2=154437, N_3=163412 отсчетов при выбранной частоте дискретизации;

3) РС, используемый в качестве скрываемого сообщения $\vec{x}$ (побуквенно) с частотой дискретизации f_d=8 кГц, разрядностью кодовой последовательности 16 бит.

4) Длительность РС, используемого в качестве скрываемого сообщения $\vec{x}$: N_C=25734 отсчетов при выбранной частоте дискретизации.

В ходе выполнения данного эксперимента были отобраны 3 предложения, содержащие преимущественно:

1. Взрывные согласные;

2. Звонкие согласные;

3. Шипящие согласные.

Данная процедура проводилась для того, чтобы скрыть информацию в этих согласных и исследовать качество полученных аудиосигналов. Ниже представлены реализации временных осциллограмм выбранных предложений. Выделен необходимый набор звуков, обозначены границы начала данных звуков.

Предложение 1 $\vec{y}_1$ длительностью 4.209 с. с частотй дискретизации 48кГц содержит взрывные звуки и соответствует фразе: «Ру***к***ово***д***и***т***ель ***п***о***т***ре***б***овал ***п***ре***к***ра***т***и***ть*** ***п***осад***к***у».

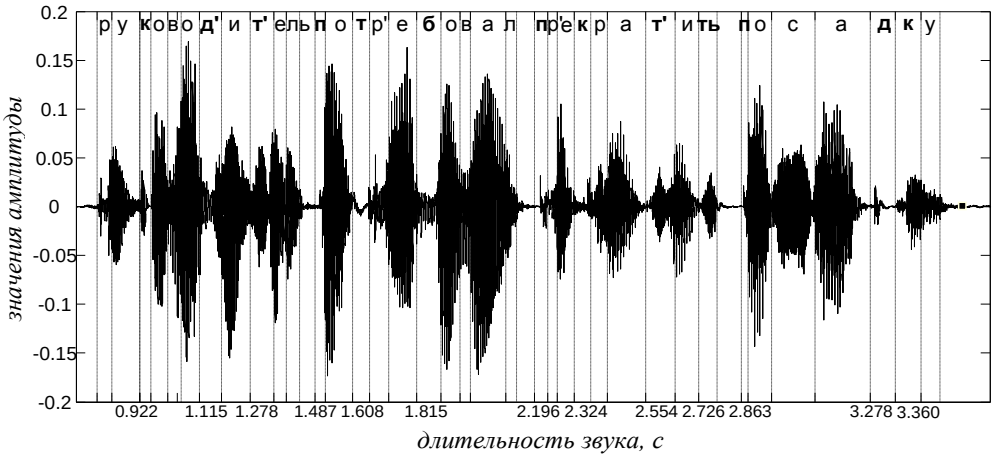

Рисунок 3.1 - Временная осциллограмма предложения 1

Предложение 2 $\vec{y}_2$ длительностью 3.217 с. с частотй дискретизации 48кГц содержит звонкие звуки и соответствует фразе: «***Г******е******р***ои ***в******ер******н******у******л***ись ***д***о***м***ой с по***б******е******д***ой».

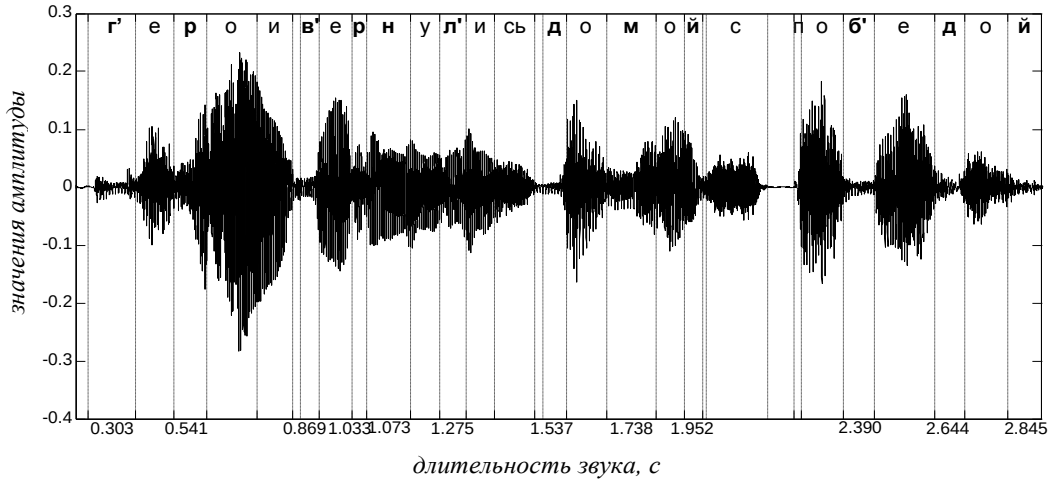

Рисунок 3.2 - Временная осциллограмма предложения 2

Предложение 3 $\vec{y}_3$ длительностью 3.404с. с частотй дискретизации 48кГц содержит щипящие звуки и соответствует фразе: «Де***ж***урный принес оде***ж***ную ***щ***етку».

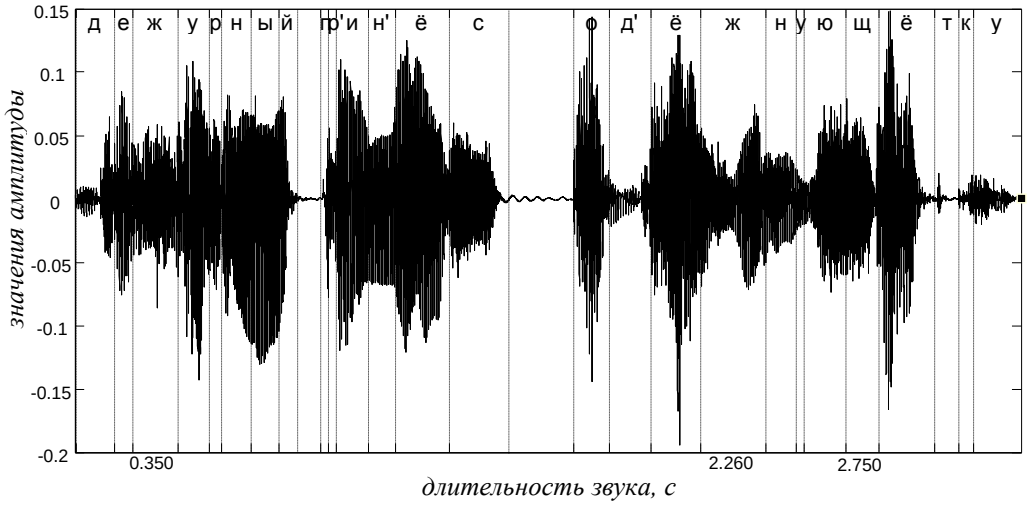

Рисунок 3.3 - Временная осциллограмма предложения 3

Далее из каждого предложения были выделены границы звуков и определена их длительность в отсчетах и секундах. Эти данные представлены в таблицах (1 – 3) приложения А.

В качестве скрываемого сообщения был использован фрагмент предложения «Фильм снимали целый год». Длительность предложения 3.216 с. (3191 отсчет) Длительность отобранного фрагмента $\vec{x}$, соответствующего слову *«год»* - 0.398 с при частоте дискретизации 8кГц.

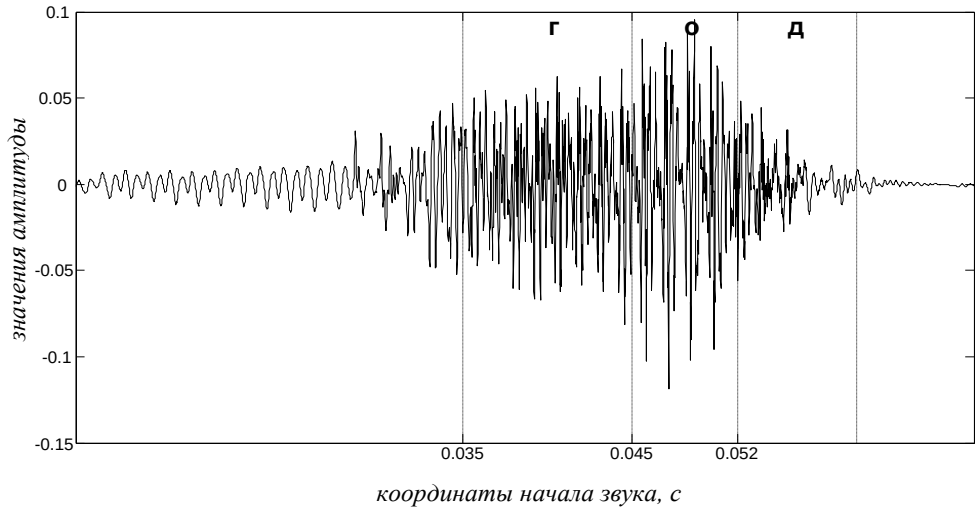

Рисунок 3.4 - Временная осциллограмма скрываемого слова

Также были определены координаты начала, конца звуков и их длительность:

Таблица 3.1 – Диапазоны звуков скрываемого РС

Буквы	**Звуки**	**Нижняя граница**	**Верхняя граница**	**Длительность, отсчеты**	**Длительность, сек**
1	**2**	**3**	**4**	**5**	**6**
г	[*г*]	1659(0.035)	1941	282	0.035
о	[*о*]	2168(0.045)	2442	274	0.034
д	[*т*]	2484(0.052)	2661	177	0.022

В результате скрытия отрезка речевого сигнала в сигналах – контейнерах при различном значении порога кодирования были получены стегоконтейнеры, представленные на рисунках 3.5 – 3.13. На рисунках 3.5 – 3.7 представлены стегоконтейнеры, полученные при скрытии информации в предложение 1:

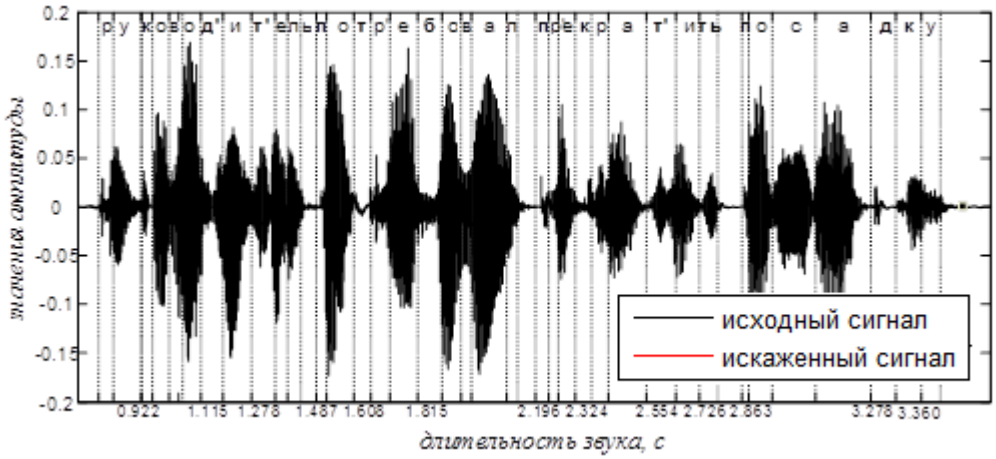

Рисунок 3.5 - Временная осциллограмма предложения 1 при K=0,1

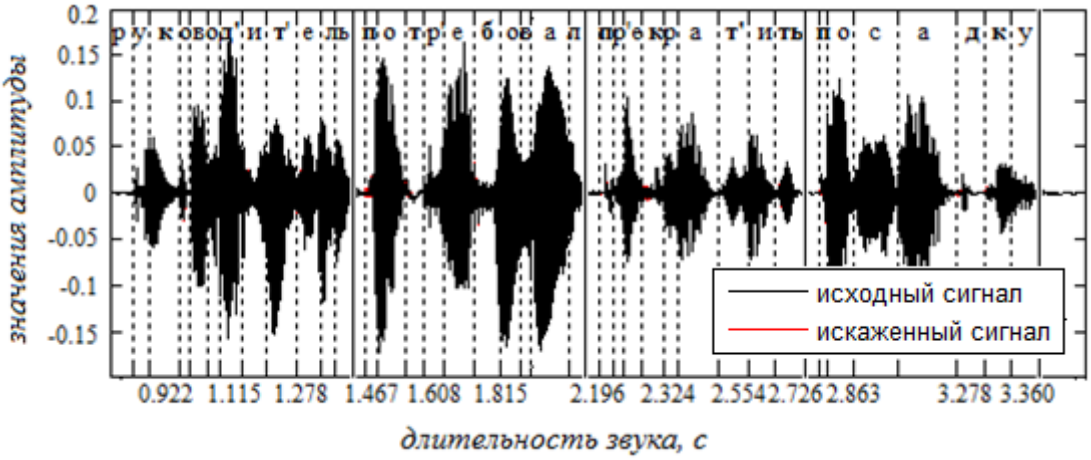

Рисунок 3.6 - Временная осциллограмма предложения 1 при K=0,5

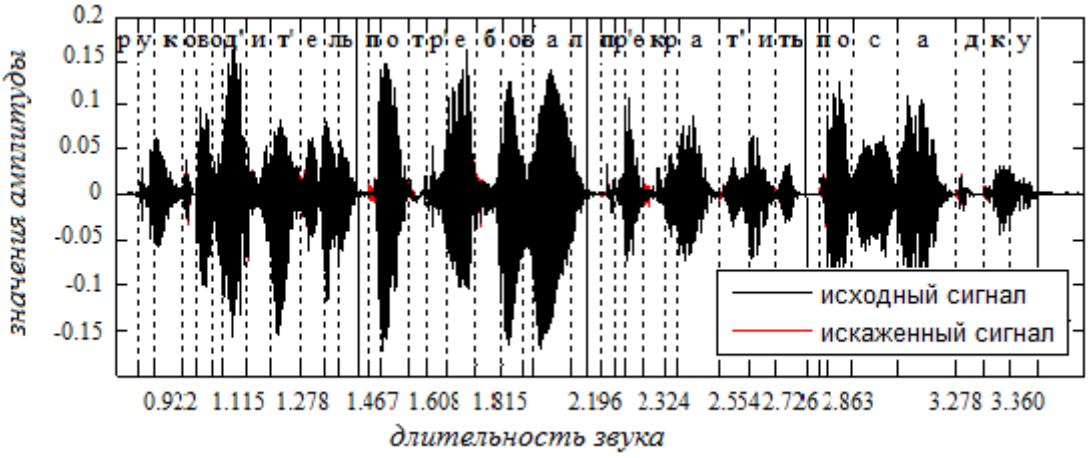

Рисунок 3.7 - Временная осциллограмма предложения 1 при K=1

Рисунки 3.8 – 3.10 иллюстрируют стегоконтейнеры, полученные при скрытии информации в предложение 2:

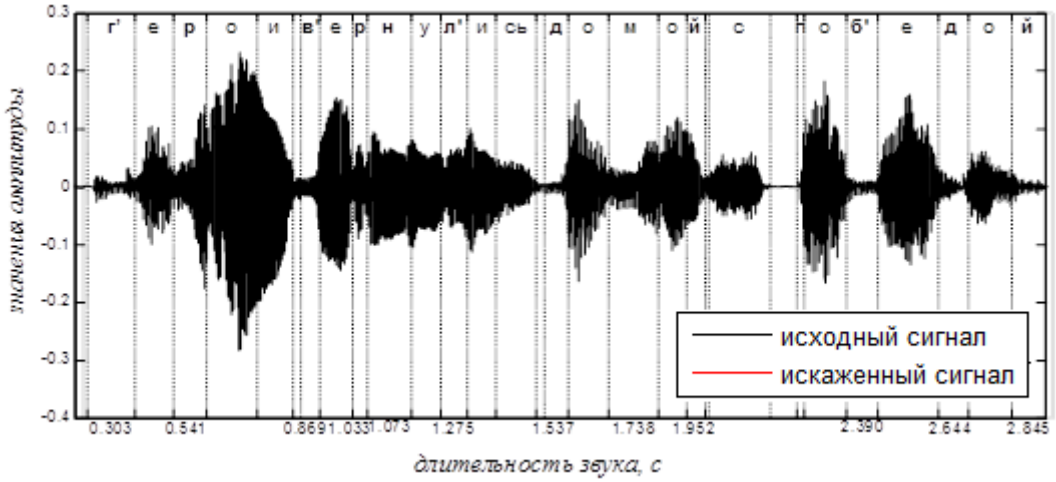

Рисунок 3.8 - Временная осциллограмма предложения 2 при K=0,1

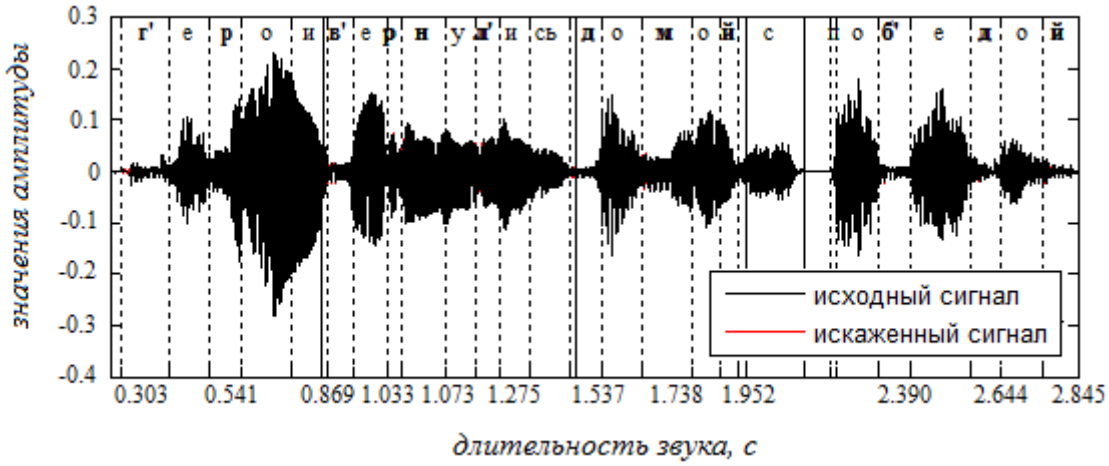

Рисунок 3.9 - Временная осциллограмма предложения 2 при K=0,5

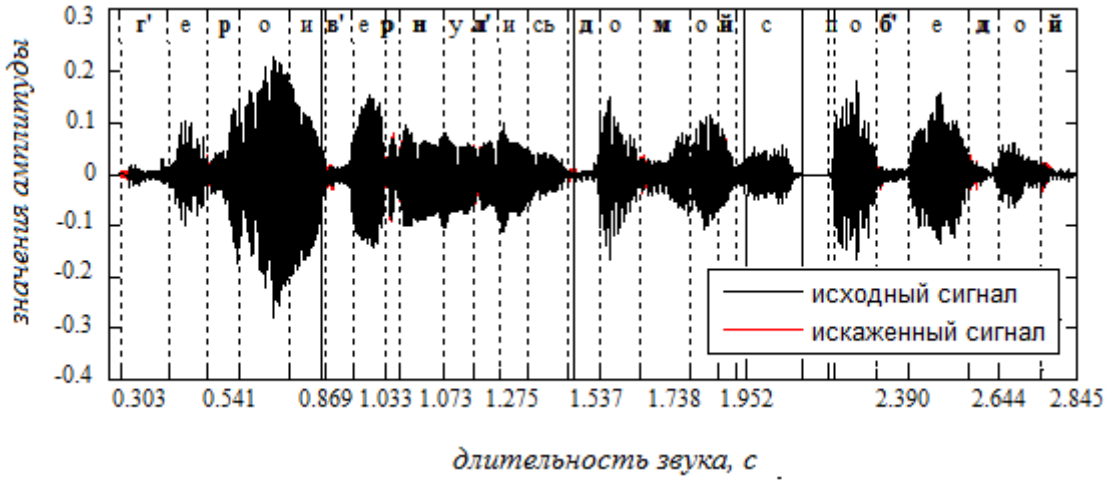

Рисунок 3.10 - Временная осциллограмма предложения 2 при K=1

Осциллограммы предложений-стегоконтейнеров, полученных при скрытии информации в предложение 3 представлены на рисунках 3.11 – 3.13:

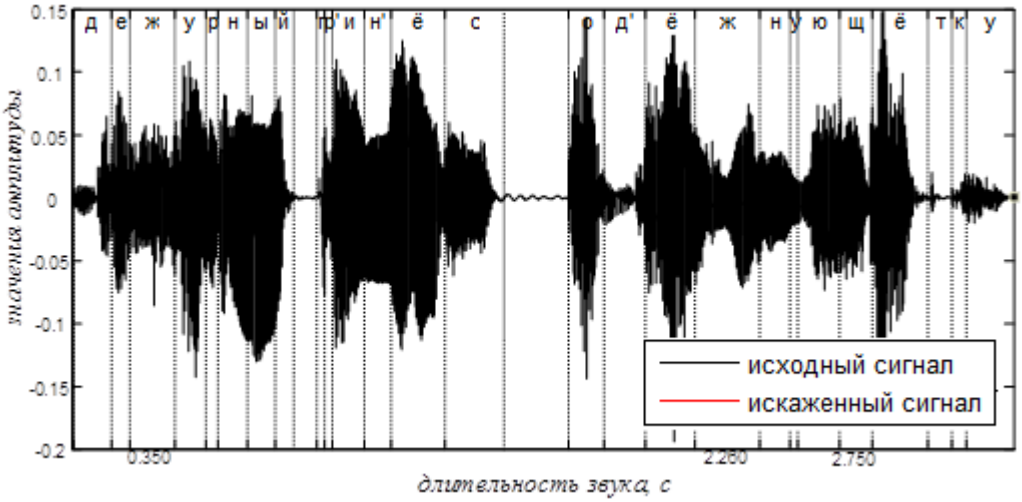

Рисунок 3.11 - Временная осциллограмма предложения 3 при K=0,1

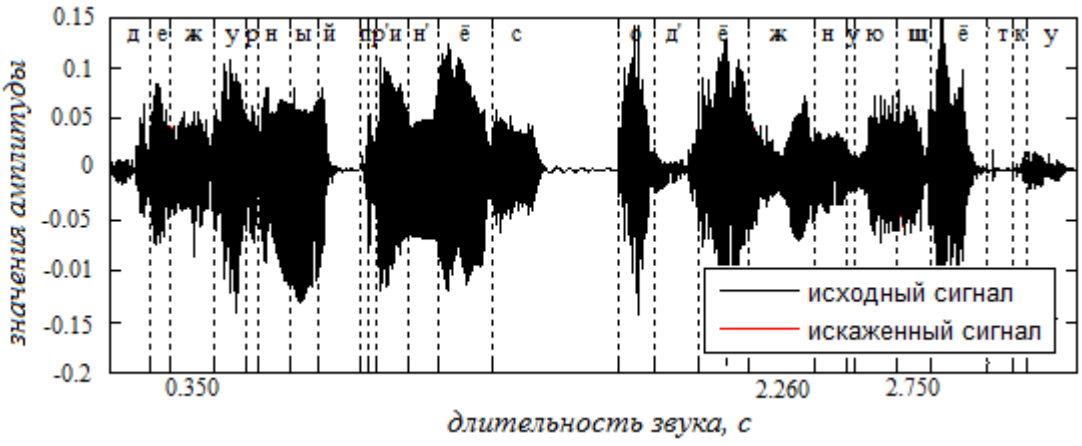

Рисунок 3.12 - Временная осциллограмма предложения 3 при K=0,5

Рисунок 3.13 - Временная осциллограмма предложения 3 при K=1

Как видно из рисунков 3.5 – 3.13, при увеличении коэффициента скрытности, видимые на осциллограмме искажения проявляются с большей степенью, таким образом, увеличение видимых искажений напрямую зависит от коэффициента *K*, регулирующего порог кодирования. Наиболее очевидные сигнальные искажения при единичном значении коэффициента *K* проявились в предложении 1, причём из всех 13 взрывных звуков с закодированным в них сигналом, наиболее четко проявили искажения звуки: [*n*], [*m*], [*к*], [*m'*]. Это может быть вызвано особенностью распределения долей энергии в данных интервалах. В предложении 2 искажения проявились во всех исследуемых звуках, но с меньшей степенью заметности, что вызвано более интенсивным распределением энергии в частотах данного набора звуков. Наименее заметно искажения проявились в шипящих звуках предложения 3. Это вызвано способностью шумоподобного вида шипящего звука маскировать возникшие при кодировании искажения.

Помимо особенностей распределения долей энергии в звуках русской речи и индивидуальных свойств исследуемых звуков, важное значение имеет количество анализируемых окон и длина исследуемого отрезка. В программной реализации анализ проводился на отрезке длиной в *N*=1024 отсчета, временная длительность при частоте дискретизации 48 кГц составила 0,22 с. Количество

анализируемых окон R=45 определялось из отношения частоты дискретизации к длине одного отрезка в отсчетах.

В звуковом спектре при диапазоне слышимости человеком 20 Гц – 20 кГц существуют следующие показатели:

1. Звуки с диапазоном слышимости: от 20Гц – 20 кГц:
   - низкочастотные звуки: до 500 Гц;
   - среднечастотные звуки: 0.5 – 10 кГц;
   - высокочастотные звуки: более 10 кГц;
2. Инфразвуки: до 20 Гц;
3. Ультразвуки: от 2 кГц и выше;

К диапазону среднечастотных звуков: 1 – 5 кГц слуховая система наиболее чувствительна, а при более низкочастотных или же высокочастотных звуках чувствительность уменьшается, в результате чего слуховой аппарат теряет слышимость низкочастотных звуков в диапазоне (20 – 60) дБ, но способен слышать звуки , энергия которых приближенак 0 дБ из среднечастотного диапазона. То есть, звуки с одной и той же энергией. Имеется в виду, что звуки среднечастотного диапазона можно принять за громкие, а звуки, принадлежащие низкочастотному диапазону считать тихим или же вовсе не слышать их.

На данном этапе была реализовано восприятие на слух речевых сигналов – стегоконтейнеров. Для оценки были назначены три проинструктированных эксперта – оценщика различной возрастной категории. Каждому оценщику предлагалось прослушать три речевых сигнала с закодированной аудиоинформацией. Для каждого предложения информация скрывалась в различном наборе звуков: во взрывных, звонких и шипящих согласных.

Далее была составлена анкета для аудиальной оценки исходного РС и РС с искажениями, вызванными скрытием в нём аудиоданных с различными значениями порога кодирования.

По результатам опроса были выявлены следующие результаты:

1. Слышимость.

Наибольшее количество искажений при различных значениях порога кодирования было замечено в предложении со скрытием в звонких согласных.

2. Абсолютное отсутствие искажений, воспринимаемых на слух:

В предложении 3 слушатели не заметили искажений при прослушивании материала.

3. Значение порога кодирования.

Во всех трех предложениях, по мере увеличения порога кодирование, количество слышимых искажений так же возрастает.

Таблица 3.2 - Количество воспринятых на слух искажений при различном значении порога кодирования

	Количество воспринятых искажений		
	K=0,1	**K=0,5**	**K=1**
1	**2**	**3**	**4**
Предложение 1	6	15	16
Предложение 2	6	9	21
Предложение 3	0	0	0

По результатам качественной оценки было выявлено, что нецелесообразно скрывать информацию в звонких согласных, так как в спектре данного набора звуков наиболее просматриваемы внесенные искажения. Это может быть связано с особенностью распределения энергии в звонких звуках. Также было выявлено, что оптимальным набором для встраивания скрытой информации является набор шипящих, ввиду того, что их реализация близка к шумоподобной, также проявляемомой как следствие кодирования. За счет слияния этих компонентов, искажения маскируются. Ещё одним заключением является выбор оптимального порога кодирования, который должен варьироваться от 0,1 до 0,3.

На рисунках 3.14 – 3.16 представлены исходные и искаженные кодированием звуки, а так же их спектры.

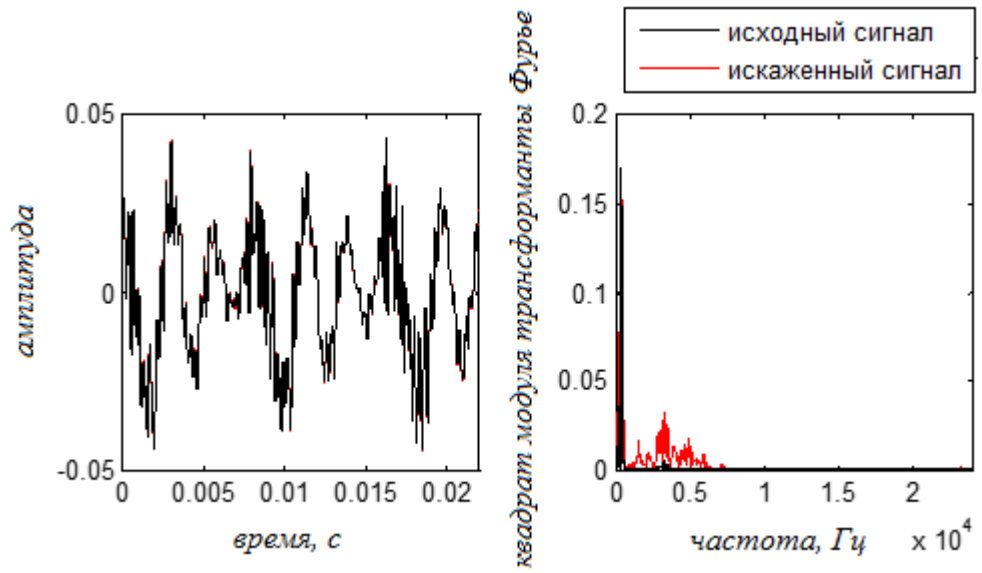

Рисунок 3.14 – Временная осциллограмма и спектр звука «*ж*» при значении коэффициента внедрения K=0.1

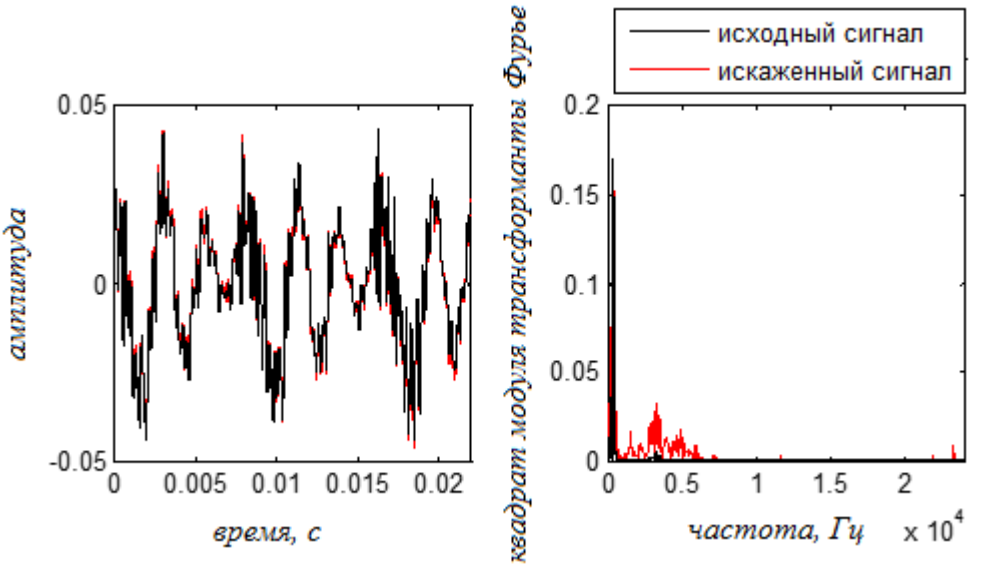

Рисунок 3.15 – Временная осциллограмма и спектр звука «*ж*» при значении коэффициента внедрения K=0.5

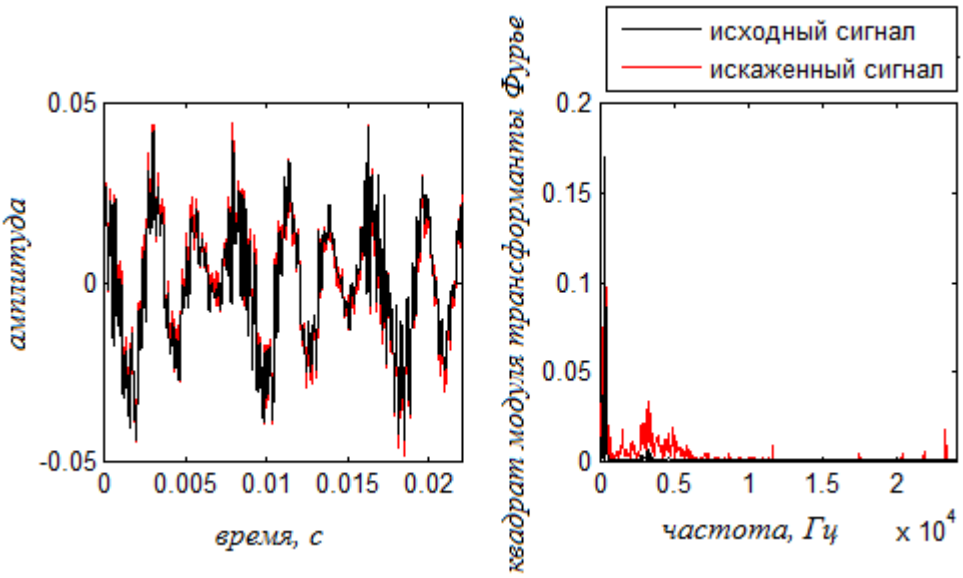

Рисунок 3.16 – Временная осциллограмма и спектр звука «*ж*» при значении коэффициента внедрения K=0.1

3.2 Количественная оценка искажений, вызываемых кодированием сообщения в речевых данных

В данном разделе были определить параметры исходного РС и сигналов – сегоконтейнеров при различном значении порога кодирования. Данная оценка очень важна, так как необходимо убедиться, что синтезированный сигнал качественно и количественно не отличается от исходного. Степень искажений, вносимых в сигнал при кодировании в него информации, можно пронаблюдать, определив следующие параметры:

Отношение сигнал/шум, параметр, определяющий суммарные мощности как шума, так и сигнала на всей его длительности :

$$ОСШ = 10\lg\frac{\sum_{i=1}^{N} x^2(i)}{\sum_{i=1}^{N}(x(i)-y(i))^2}, \qquad (3.2)$$

где N – общее количество отсчетов в РС; $x(i)$ и $y(i)$ - отсчеты исходного и искаженного (синтезированного) сигналов с номером i.

В процессе исследования может возникнуть необходимость вычисления отношения сигнал/шум на отдельных сегментах речевого сигнала. В этом случае удобно пользоваться формулой 3.3:

$$ОСШ_{сег} = \frac{10}{M}\sum_{m=0}^{M-1}\lg\sum_{N_m}^{N_m+N-1}\frac{x^2(i)}{(x(i)-y(i))^2}, \quad (3.3)$$

где M - количество сегментов в РС; N - длина сегмента; $x(i)$ и $y(i)$ - отсчеты исходного и искаженного (синтезированного) сигналов с номером i, вычесленные на m-м сегменте.

Среднеквадратическая ошибка[23, 2] позволяет анализировать сигнал во временной области, определяя различие энергии отрезков сигналов*:*

$$СКО = \sum_{n=1}^{N}(x_n - \tilde{x}_n)^2, \quad (3.4)$$

где x_n – амплитуды исходного отрезка данных; $\tilde{x}_n$ –амплитуда отрезка данных, содержащего дополнительную информацию; N – количество отсчетов анализируемых сигнальных отрезков.

Однако при использовании данной оценки, энергия самого сигнала не учитывается, поэтому стоит ввести оценку, обладающую аналогичным поведением при определении СКО, *нормированную среднеквадратическую ошибку* [23, 2]*:*

$$НСКО = \frac{\sum_{n=1}^{N}(x_n - \tilde{x}_n)^2}{\sum_{n=1}^{N}x_n^2}, \quad (3.5)$$

где x_n - исходный сигнал; $\tilde{x}_n$ – синтезированный сигнал;

Степень взаимосвязи между исходным и синтезированным речевыми сигналами определяется их *корреляцией*:

$$r = \frac{\sum_{n=1}^{N}(x_n - \bar{x}_n)(\tilde{x}_n - \bar{\tilde{x}}_n)}{\sqrt{\sum_{n=1}^{N}(x_n - \bar{x}_n)^2(\tilde{x}_n - \bar{\tilde{x}}_n)^2}}, \quad (3.6)$$

где x_n – исходный сигнал; $\tilde{x}_n$ – синтезированный сигнал; $\bar{x}_n$ и $\bar{\tilde{x}}_n$ – выборочное среднее исходного и синтезированного сигнала, определяемое формулой:

$$\bar{\tilde{x}}_n = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (3.7)$$

Все вышеперечисленные оценки позволяют сравнить исходный и синтезированный отрезки речевого сигнала в процессе кодирования, функционируя при этом во временной области.

Таблица 3.2 - Представлены результаты количественной оценки звуков – стегоконтейнеров

	Предложение 1: звук «*к*»			**Предложение 2: звук «*д*»**			**Предложение 3: звук «*ж*»**		
	К=0,1	**К=0,5**	**К=1**	**К=0,1**	**К=0,5**	**К=1**	**К=0,1**	**К=0,5**	**К=1**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
ОСШ	66.383	38.423	26.380	45.522	17.585	5.542	72.074	44.132	32.097
СКО	$5.684*10^{-5}$	0.001	0.006	$8.232*10^{-5}$	0.002	0.008	$7.766*10^{-5}$	0.002	0.008
ε	$4.796*10^{-4}$	0.012	0.048	0.005	0.132	0.528	$2.491*10^{-4}$	0.006	0.025
r	0.999	0.994	0.977	0.997	0.937	0.785	0.999	0.997	0.988

По результатам количественной оценки было выявлено, что наиболее оптимальным является скрытие речевого сигнала в шипящих звуках-контейнерах с использованием порога кодирования в диапазоне от 0,1 до 0,5. Как видно, при данных критериях уровень зашумленности велик, но синтезированный сигнал практически идентичен исходному.

Величина среднеквадратической ошибки в данном случае приближена к нулю при минимальном коэффициенте внедрения, но по мере его увеличения, СКО незначительно возрастает. Тем не менее, допустимая степень идентичности исходного и синтезированного сигнала сохраняется. Также видно, что при увеличении интенсивности кодирования, отношение сингал/шум уменьшается, что свидетельствует об увеличении искажений. Корреляция при исследовании каждого набора звуков и при всех вариациях коэффициента K не опускается ниже 0,97, следовательно, сохраняется достаточная схожесть между сигналами.

4 ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Основная задача научно-исследовательской работы заключалась в разработке алгоритма скрытной передачи речевого сигнала, в результате чего был получен необходимый продукт, а также проведено исследование искажений при различной интенсивности порога кодирования. По мере выполнения работы возникал ряд определенных экономических затрат.

4.1 Планирование работ по исследованию

Для реализации работы были задействованы следующие сотрудники:

- младший научный сотрудник, выполняющий сбор и обработку необходимой информации, теоретическое описание и изложение математической модели исследования, разработку расчетных и функциональных алгоритмов, соответствующих выбранной теме.

- старший научный сотрудник, контролирующий и проверяющий работу в процессе её реализации.

- экономист, оценивающий экономические затраты на исследования.

Расчет трудоемкости и временных затрат представлен в таблице 4.1.

Таблица 4.1 - Планирование работ по исследованию

Этапы выполнения работы	**Исполнитель**	**Трудоемкость, час**	**Продолжительность, дней**
1	**2**	**3**	**4**
1.Подготовительный			
1.1.Поиск информации	Младший научный сотрудник	120	15

Окончание таблицы 4.1

Этапы выполнения работы	**Исполнитель**	**Трудоемкость, час**	**Продолжительность, дней**
1	**2**	**3**	**4**
1.2.Формирование направления исследования	Старший научный сотрудник	120	15
1.3.Определение объема исследовательских работ	Младший научный сотрудник	40	5
1.4.Формирование исследовательской работы	Младший научный сотрудник	8	1
1.5.Обработка и анализ информации	Младший научный сотрудник	64	8
Итого:	472	59	44
2.Основной (экономический анализ)			
2.1.Обоснование актуальности исследовательской работы	Старший научный сотрудник	24	3
2.2.Реализация работы	Младший научный сотрудник	320	40
Итого:		344	43
3.Заключительный			
3.1.Экономическое обоснование результатов исследования	Экономист	40	5
3.2. Оформление и утверждение документации	Младший научный сотрудник	40	5
Итого:		80	10

В результате планирования было определено штатное количество сотрудников, задействованных в работе, а также была рассчитана почасовая и ежедневная трудоемкость исследования. Было выявлено, что наибольшая временная нагрузка на всех этапах выполнения работы приходится на младшего научного сотрудника, а наиболее продолжительным по времени является подготовительный этап, поскольку необходимо собрать достаточное количество информации, соответствующей теме исследования.

4.2 Расчет расходов на оплату труда

Распределение расходов на оплату труда по разработке алгоритма скрытной передаче речевого сигнала представлен в таблице 4.2.

Таблица 4.2 - Распределение расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**
1	**2**	**3**
Младший научный сотрудник	592	17000
Старший научный сотрудник	144	31000
Экономист	40	15000
Итого:	776	63000

Часовая тарифная ставка ($Ч_{ТС}$) определяется формулой:

$$Ч_{TC} = \frac{P}{F_{мес}}\ , \qquad (4.1)$$

где $F_{мес}$ – фонд рабочего времени месяца, составляет 176 часов (22 рабочих дня, 8 часов в день); Р – оклад сотрудника, руб.

Для младшего научного сотрудника часовая тарифная ставка составит:

$$Ч_{TC1} = \frac{17000}{176} = 96{,}59\ руб/час.$$

Для старшего научного сотрудника часовая тарифная ставка составит:

$$Ч_{TC2} = \frac{31000}{176} = 176{,}14\ руб/час.$$

Часовая тарифная ставка экономиста:

$$Ч_{ТСЗ} = \frac{15000}{176} = 85,23 \, руб / час.$$

Таким образом, общая часовая тарифная ставка составит:

$$Ч_{ТС} = 96,591 + 176,136 + 85,227 = 357,95 \, руб / час.$$

Расход на оплату труда ($Р_{ОТ}$) находится следующим образом:

$$P_{ОТ} = Ч_{ТС} * T_{сум}, \quad (4.2)$$

где $Т_{СУМ}$ – суммарная трудоемкость каждого из исполнителей, час.

Расход на оплату труда младшего научного сотрудника:

$$P_{ОТ1} = 95,591 \cdot 592 = 56589,87 \, руб.$$

Расход на оплату труда старшего научного сотрудника:

$$P_{ОТ2} = 176,136 \cdot 144 = 25363,58 \, руб.$$

Расход на оплату труда экономиста:

$$P_{ОТЗ} = 85,227 \cdot 40 = 3409,08 \, руб.$$

Общий расход на оплату труда:

$$P_{ОТ} = 56589,872 + 25363,584 + 3409,080 = 85362,54 \, руб.$$

Результаты расчетов сведены в таблицу 4.3:

Таблица 4.3 - Расчет расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**	**Чтс, руб/час**	**Рот, руб**
1	**2**	**3**	**4**	**5**
Младший научный сотрудник	592	17000	96,59	56589,87
Старший научный сотрудник	144	31000	176,14	25363,58
Экономист	40	15000	85,23	3409,08
Итого:	776	63000	357,95	85362,54

Согласно расчетам трудоемкость исследования составила 776 часов, итоговый оклад оценивается в 63000 рублей, общая часовая ставка равна 357,954 *руб/час*, а суммарный расход на оплату труда составляет 85362,54 рубля.

4.3 Расчет продолжительности исследования

Длительность проводимой работы составит:

$$T_{иссл} = T_{сум} / T_{РД} \quad (4.3)$$

где $T_{СУМ}$ = 776 часов - суммарная трудоемкость исследования; $T_{РД}$ = 8 часов – продолжительность рабочего дня.

$$T_{ИССЛ} = 776/8 = 97 \text{ дней.}$$

Без учета выходных и праздничных дней продолжительность работы составляет 97 дней.

4.4 Расчет стоимости расходных материалов

В данном разделе рассчитываются расходы на приобретение материалов для печати, канцелярских товаров, различных бумажных материалов необходимых для проведения исследования, нанесения необходимых письменных заметок, печати и оформления документации. Расчет стоимости расходных материалов приведен в таблице 4.4:

Таблица 4.4 - Стоимость расходных материалов.

Наименование расходных материалов	**Цена за единицу, руб.**	**Количество, шт.**	**Сумма, руб.**
1	**2**	**3**	**4**
Бумага	180	2	360
Канцтовары	200	1	200
Расходные материалы для принтера (картридж)	3800	1	3800
Ватман	10	10	100
Итого:	4180	14	4460

Выявлено, что расход на приобретение используемых материалов составляет 4460 рублей.

4.5 Расчет сметы расходов на исследование.

В категорию расчетов расходов на исследования включаются премиальные выплаты, районный коэффициент и страховые взносы. Данные

показатели зависят от величины расхода на оплату труда. По итогам расчета была составлена смета, в которой обозначены расходы на реализацию исследования.

Премиальные выплаты рассчитываются по формуле:

$$ПВ = Р_{ОТ} К_{ПВ} \quad (4.4)$$

где $К_{ПВ}$ - коэффициент премиальных выплат - 20 %, в случае если премии не предусмотрены $К_{ПВ}$=1.

Сумма премиальных выплат составит:

$$ПВ = 85362,54 \cdot 0,2 = 17072,51 руб.$$

Дополнительные затраты на проведение исследования можно определить как::

$$З_{ДОП} = Р_{ОТ} К \quad (4.5)$$

где К - коэффициент дополнительных затрат (К=14%).

$$З_{ДОП} = Р_{ОТ} \cdot 14\%.$$

$$З_{ДОП} = 85362,54 \cdot 0,14 = 11950,76 руб.$$

В случае, если работа осуществляется в неблагоприятных условиях, необходимо сделать доплату к основной заработной плате. Величину доплаты характеризует районный коэффициент, определяемый формулой:

$$РК = Р_{ОТ} К_{РВ} \quad (4.6)$$

где $К_{РВ}$ – коэффициент районных выплат, для примера составляет 15 % от суммы.

$$РК = 85362,54 \cdot 0,15 = 12804,39 руб.$$

Общие расходы на оплату труда вычисляются по формуле:

$$P_{общ} = P_{ОТ} + ПВ + РК + З_{ДОП} \quad (4.6)$$

где $Р_{ОТ}$ - основная заработная плата; ПВ - премиальные выплаты; $З_{ДОП}$ - дополнительные затраты; РК - районный коэффициент.

$$P_{общ} = 85362{,}54 + 17072{,}51 + 12804{,}39 + 11950{,}76 = 127190{,}20\,руб.$$

Итоговая сумма стоимости расходных материалов по статье расходных материалов:

$$\Sigma\ Р_{РМ} = 4460 \text{ руб.}$$

Страховые взносы рассчитываются по формуле:

$$СВ = P_{ОТ}\,0{,}3 \quad (4.7)$$

$$СВ = 85362{,}536 \cdot 0{,}3 = 25608{,}60\,руб.$$

На использование компьютера предусмотрены амортизационные исчисления, составляющие 25% от его стоимости и вычисляемые по формуле:

$$АО = С_{ПК}\,0{,}25 \quad (4.8)$$

$$СВ = 23000 \cdot 0{,}25 = 5750\,руб.$$

Расходы на использование Интернета берутся из расчета месячной абонентской платы для предприятия. Пусть:

$$Р_{ИНТ} = 800\ руб.$$

Административно-хозяйственые расходы составляют 50% от основной заработной платы ($Р_{ОТ}$).

$$P_{AX} = P_{OT} \cdot 0{,}5. \tag{4.9}$$

$$P_{AX} = 85362{,}54 \cdot 0{,}5 = 42681{,}27 \, руб.$$

Результирующие расходы были сведены в таблицу. Смета расходов на разработку и проведение исследования представлена в таблице 4.5.

Таблица 4.5 - Смета расходов на разработку и проведение исследования

Наименование статей расходов	**Сумма, руб.**	**Удельный вес статей, %**
1	**2**	**3**
1.Стоимость расходных материалов	4460	2,16
2. Расходы на оплату труда 2.1. Основная заработная плата	127190,20 85362,54	 41,34
2.2. Дополнительные затраты	11950,76	5,79
2.3. Премиальные выплаты	17072,51	8,268
2.4 Районный коэффициент	12804,39	6,2
3. Единый социальный налог	25608,60	12,4
4. Амортизационные исчисления на использование компьютера	5750	2,785
5. Расходы на использование Интернет	800	0,388
6.Административно-хозяйственные расходы	42681,27	20,67
Итого:	206490,07	100

В результате экономической оценки исследования были определены затраты на разработку и реализацию исследования:

- продолжительность исследовательских работ составила 97 дней;

- сметы расходов на исследование – 206490,07 рублей с учетом отчислений и единого социального налога.

ЗАКЛЮЧЕНИЕ

В реализованной работе были рассмотрены основные стеганографические методы, позволяющие осуществлять скрытную передачу информации. Проанализировав преимущества и недостатки было выявлено, что наиболее оптимальным с точки зрения емкости скрываемой информации, маскировки и сложности реализации является алгоритм, основанный на методе расширения спектра. Данный метод был модифицирован за счет замены псевдослучайной последовательноси как ключа на ортонормированный базис, в результате чего появилась возможность скрывать поток данных, а не 1 бит информации в сегменте. Использование ортонормированного базиса вместо ПСП, позволяет более эффективно с позиции объема кодируемой информации использовать речевой материал для скрытной передачи сообщения.

Стеганографическое кодирование имеет ряд этапов. Первый включает в себя кодирование сообщения в ортонормальном базисе. Второй осуществляет адаптивную фильтрацию, для того чтобы декодирование сообщения обладало более высокой достоверностью и не было подвержено искажениям. Третий этап непосредственное кодирование с адаптивным коэффициентом. Как показали эксперименты скрытность можно обеспечить за счет использования в качестве коэффициентов отражающих значение энергии исходного отрезка.

В процессе исследовательской работы была выполнена основная цель, так как разработанный алгоритм способствует модификации методов скрытого внедрения информации в звуковые файлы. Для достижения поставленной цели был проведен мониторинг изменений качества звука и восприятия искажений при скрытном кодировании информации модифицированным методом расширения спектра.

Поэтапно был реализован ряд задач. В результате анализа метода расширения спектра и его модификации был разработан алгоритм скрытного кодирования и декодирования речевого сообщения в речевые данные, причем в

качестве ПСП был использован ортогональный базис Радемахера, что позволило увеличить скрытность.

Проанализировав речевой материал, содержащий преимущественно взрывные, звонкие и шипящие согласные было выявлено, что наиболее оптимальным сигналом для скрытия в него информационного сообщения является предложение, содержащее шипящие звуки ввиду минимального наличия визуальных искажений на осциллограмме. Результаты качественной оценки также направлены на оптимальность предложения с шипящими звуками, так как слияние шумоподобных составляющих звука и искажения способны взаимомаскироваться.

При количественной оценке были определены величины отношения сигнаол шум, среднеквадратической и нормированной среднеквадратической ошибки, корреляции. Было выявлено, что наиболее оптимальным является скрытие речевого сигнала в шипящих звуках-контейнерах с использованием порога кодирования в диапазоне от 0,1 до 0,5.

Разработанные алгоритмы стеганографического кодирования и декодирования речевого сообщения в речевые данные были реализованы в среде программирования Matlab в соответствии с приведенными словесными алгоритмами. Программный код позволил за короткое время получить достоверные результаты расчетов с использованием общеизвестных и разработанных формул.

В результате экономической оценки исследования удалось оценить продолжительность исследовательских работ – 97 дней и сумму расходов на исследование – 206490,07 рублей с учетом отчислений и единого социального налога.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Yong Xiang Spread Spectrum-Based High Embedding Capacity Watermarking Method for Audio Signals [электронный ресурс] / Yong Xiang, Iynkaran Natgunanathan, Yue Rong, , Song Guo // IEEE.ACM TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING. 23(12). 2015. pp. 2228 – 2237 URL: https://www.researchgate.net/publication/281930141_Spread_Spectrum-Based_High_Embedding_Capacity_Watermarking_Method_for_Audio_Signals?C (дата обращения: 04.05.2016)

2. Ahmed Hussain Ali A Review on Audio Steganography Techniques [электронный ресурс] / Mohd Rosmadi Mokhtar, LoayEdwar George // Research Journal of Applied Sciences, Engineering and Technology. 12(2). 2016. pp. 154-162 URL:https://www.researchgate.net/publication/292361595_A_Review_on_Audio_Steganography_Techniques (дата обращения: 05.05.2016)

3. Таравков, А.В. Разработка алгоритма синхронизации для внедрения цифрового водяного знака в потоковое видео [Электронный ресурс]/ Григорьев А.С., Баженов Р.И.// Современная техника и технологии. № 11. 2014. URL: https://d.docs.live.net/99ddf781f115b8ed/Литература%20к%20диплому/3.html (дата обращения 18.04.2016)

4. Zhenghui Liu A security watermark scheme used for digital speech forensics [электронный ресурс] / Jiwu Huang, Xingming Sun, Chuanda Qi // Springer Science+Business Media New York. 10.1007/s11042-016-3533-9. 2016. pp 1-21.URL:
https://www.researchgate.net/publication/301576015_A_security_watermark_scheme_used_for_digital_speech_forensics (дата обращения 25.04.2016)

5. Коробейников, А.Г. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра [Электронный ресурс] / А.Г. Даурских, Н.В. Павлова // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. № 1(59). 2009. URL: http://cyberleninka.ru/article/n/vstraivanie-tsifrovyh-

vodyanyh-znakov-v-audiosignal-metodom-rasshireniya-spektra (дата обращения 27.04.2016)

6. Сюзев, В.В. Основы спектрального анализа в базисах Хаара [Электронный ресурс] // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия «Приборостроение». № 2. 2011. URL: http://cyberleninka.ru/article/n/spektralnyy-analiz-v-bazisah-funktsiy-haara (дата обращения 29.04.2016)

7. Сергиенко А.Б. Цифровая связь: Учеб. пособие. СПб / А.Б. Сергиенко – Изд – во: С32 СПбГЭТУ «ЛЭТИ», 2012. 164с.

8. Nedeljko Cvejic. Spread spectrum audio watermarking using frequency hopping and attack characterization [Электронный ресурс] / Nedeljko Cvejic, Tapio Seppanen// Signal Processing 84. 2004. pp 207 – 213. URL: http://www.mediateam.oulu.fi/publications/pdf/465.pdf (дата обращения 04.05.2016)

9. Saito S. A digital watermarking for audio data using band division based on QMF bank [Электронный ресурс] / S. Saito, T. Furukawa, K. Konishi // IEEE International Conference on Acoustics, Speech, and Signal Processing. 2002. – V. 4. pp 3473-3476. URL: http://books.google.ru/books?id (дата обращения 05.05.2016)

10. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Текст] / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: «МК-Пресс», 2006 - 288с.

11. Boney, L. Digital watermarks for audio signals Tewfic [Электронный ресурс] / A.H., Hamdy A.K. // Department of Electrical engineering, University of Minnesota. DOI: 10.1109/MMCS.1996.535015. 1996. URL: https://www.researchgate.net/publication/3639217_Digital_watermarks_for_audio_signals (дата обращения 11.05.2016)

12. Рабинер, Л.Р. Цифровая обработка речевых сигналов = Digital processing of speech signals: для инженеров, специализирующихся в данной области, а также для студентов вузов соответствующих специальностей / Л.Р. Рабинер, Р.В. Шафер; Пер. с англ./ Под ред. М.В. Назарова и Ю.Н. Прохорова - М.: Радио и связь, 1981. - 496 с., ил.

13. Кирякова, Г.С. Системы искусственного интеллекта: Учеб. пособие / Г.С. Кирякова. Красноярск: ИПЦ КГТУ. 2005. 168 с.

14. Чесебиев, И.А. Компьютерное распознавание и порождение речи [Текст] / И.А. Чесебиев. Спорт и культура-2000, 2008. 128 с.

15. Ле, Н. В. Предварительная обработка речевых сигналов для системы распознавания речи [Электронный ресурс] / Н. В. Ле, Д. П. Панченко // Молодой ученый. — 2011. — №5. Т.1. — С. 74-76. URL: http://www.moluch.ru/archive/28/3171/ (Дата обращения 18.04.2016)

16. Горшков, Ю.Г. Обработка речевых сигналов на основе вейвлетов [Электронный ресурс] // T-Comm. 2015. №2. С. 46 – 53. URL: http://cyberleninka.ru/article/n/obrabotka-rechevyh-signalov-na-osnove-veyvletov (дата обращения: 18.05.2016).

17. Белов, С.П. Метод частотно – временного анализа сигналов [Электронный ресурс] / С.П. Белов, Е.И. Прохоренко, А.С Белов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2009. №1 (56). URL: http://cyberleninka.ru/article/n/metod-chastotno-vremennogo-analiza-signalov-1 (дата обращения: 20.05.2016).

18. Жиляков, Е.Г. Алгоритмы обнаружения основного тона речевых сигналов [Электронный ресурс] / Е.Г Жиляков, А.А. Фирсова, Н.А. Чеканов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2012. №1-1 (120). URL: http://cyberleninka.ru/article/n/algoritmy-obnaruzheniya-osnovnogo-tona-rechevyh-signalov (дата обращения: 18.05.2016).

19. Рыболовлев, А.А. Основы цифровой фильтрации: Пособие / А.А. Рыболовлев, А.А. Афанасьев. – Орел: Академия ФАПСИ. 2013. – 121 с.

20. Солонина, А.И. Основы цифровой обработки сигналов: Учеб. Пособие / А.И. Солонина, Д.А. Улахович, С.М. Арбузов, Е.Б. Соловьева / Изд-е 2-е испр. и перераб. – Санкт – Петербург: БХВ Петербург. – 2005. 768 с.: ил.

21. Трахтман, А.М. Основы теории дискретных сигналов на конечных интервалах [Текст] / А.М. Трахтман, В.А. Трахтман. М, «Сов. радио». 1975. 208 с.

22. Zhengguang Xu. Channel Capacity Analysis of the Multiple Orthogonal Sequence Spread Spectrum Watermarking in Audio Signals [Электронный ресурс] / Zhengguang Xu, Chenghuan Ao, and Benxiong Huang // IEEE SIGNAL PROCESSING LETTERS. 2016. 23(1). pp. 20-24 URL: https://www.researchgate.net/publication/283805432_Channel_Capacity_Analysis_of_the_Multiple_Orthogonal_Sequence_Spread_Spectrum_Watermarking_in_Audio_Signals (Дата обращения 26.04.2016)

23. Илюшин, М.В. Обоснование объективного критерия качества звучания синтезированного широкополосного речевого сигнала / М.В. Илюшин , О.О. Басов, А.В. Радаев, А.В. Степанов // Рязань, Вестник РГРТУ. 2010. 4(34).

24. Белов, С.П. О методе скрытного кодирования контрольной информации в речевые данные [Текст]/ С.П. Белов, Е.Г. Жиляков, П.Г. Лихолоб, В.П. Пашинцев // Инфокоммуникационные технологии. Саратов. Поволжский государственный университет телекоммуникаций и информатики, № 13(3). 2015. С. 325-333.

25. Жиляков, Е.Г. Определение возможного объёма внедряемой информации при скрытой передаче меток в речевых данных [Текст]/ Е.Г. Жиляков, П.Г. Лихолоб, С.Н. Девицына // Научные ведомости Белгородского государственного университета № 13 (132). выпуск 23/1, серия История. Политология. Экономика. Информатика. – Белгород: ГиК – 2012г. С. 222-226.

26. Жиляков, Е.Г. Об использовании распределения долей энергии по частотным диапазонам в задачах защиты речевых данных [Текст]/ А.В. Болдышев, Е.Г. Жиляков, П.Г. Лихолоб, Е.И. Прохоренко, А.А. Фирсова // Цифровая обработка сигналов и её применение – DSPA-2013. – М.: РНТОРЭС. Вып. XV, т. 1. 2013. – С. 198.

27. Крыжевич, Л.С. Стеганографические методы сокрытия данных в звуковых файлах на основе всплесковых преобразований // Л.С. Крыжевич, Д.А.

Белобородов // Auditorium: электронный научный журнал Курского государственного университета. – Курск: № 2, 2014г. «Аудиториум» электронный научный журнал http://auditorium.kursksu.ru. URL: http://auditorium.kursksu.ru/index.php?page=6&new=2 (Дата обращения 26.04.2016)

ПРИЛОЖЕНИЕ А

Таблица А.1 – Диапазоны звуков предложения 1

Буквы	Звуки	Начальная граница	Конечная граница	Длительность, отсчеты	Длительность, сек
1	**2**	**3**	**4**	**5**	**6**
р	[*р*]	37694	39488	1794	0.937
у	[*у*]	40007	43632	4330	0.076
к	**[*к*]**	**44264**	**45320**	**1056**	**0.022**
о	[*а*]	46044	48580	2536	0.053
в	[*в*]	48581	50064	1670	0.035
о	[*а*]	50122	53755	3633	0.076
д	**[*д'*]**	**53537**	**56120**	**2583**	**0.054**
и	[*и*]	56929	60673	3834	0.080
т	**[*т'*]**	**61344**	**64924**	**3580**	**0.075**
е	[*и*]	65031	66515	1484	0.031
ль	[*л'*]	66948	69546	2598	0.054
пауза					
п	**[*п*]**	**71381**	**72907**	**1526**	**0.032**
о	[*а*]	73009	75916	2907	0.061
т	**[*т*]**	**77191**	**79657**	**2466**	**0.051**
р	[*р'*]	79813	82472	2659	0.055
е	[*е*]	82781	86925	4144	0.086
б	**[*б*]**	**87111**	**90574**	**3463**	**0.072**
о	[*а*]	90945	93543	2598	0.054
в	[*в*]	93914	95460	1546	0.032
а	[*а*]	95522	100346	4824	0.101
л	[*л*]	100964	103562	2598	0.054
пауза					
п	**[*п*]**	**105424**	**105950**	**526**	**0.011**
р	[*р'*]	107458	108757	1299	0.027
е	[*и*]	108943	110984	2041	0.043
к	**[*к*]**	**111552**	**113254**	**1702**	**0.035**
р	[*р*]	114880	116303	1423	0.030
а	[*а*]	116674	120694	4020	0.084
т	**[*т'*]**	**122586**	**127106**	**4520**	**0.094**
и	[*и*]	127188	130466	3278	0.068
ть	**[*т'*]**	**130862**	**134853**	**3991**	**0.083**
пауза					
п	**[*п*]**	**137436**	**138375**	**939**	**0.020**
о	[*а*]	138506	141660	3154	0.066
с	[*с*]	142155	148401	6246	0.130
а	[*а*]	148773	154462	5689	0.119
д	**[*т*]**	**157333**	**159622**	**2289**	**0.048**
к	**[*к*]**	**161266**	**163085**	**1819**	**0.038**
у	[*у*]	165224	168502	3278	0.068

Таблица А.2 – Диапазоны звуков предложения 2

Буквы	Звуки	Начальная граница	Конечная граница	Длительность, отсчеты	Длительность, сек
1	2	3	4	5	6
г	***[г']***	**14558**	**20264**	**5706**	**0.119**
е	[*и*]	20874	24961	4087	0.085
р	***[р]***	**25969**	**28723**	**2754**	**0.057**
о	[*о*]	30306	34141	3855	0.080
и	[*и*]	36970	41120	4150	0.087
пауза					
в	***[в']***	**41708**	**44659**	**2951**	**0.061**
е	[*и*]	45270	49231	3961	0.083
р	***[р]***	**49577**	**53315**	**3738**	**0.078**
н	***[н]***	**51494**	**56461**	**4967**	**0.104**
у	[*у*]	57342	61177	3835	0.080
л	***[л']***	**61185**	**64332**	**3147**	**0.066**
и	[*и*]	64698	68408	3710	0.077
сь	[*с'*]	68470	73689	5219	0.109
пауза					
д	***[д]***	**73776**	**77514**	**3738**	**0.078**
о	[*а*]	78090	82743	4653	0.097
м	***[м]***	**83416**	**87350**	**3934**	**0.082**
о	[*о*]	89911	93683	3772	0.079
й	***[й']***	**93683**	**95569**	**1886**	**0.039**
пауза					
с	[*с*]	96135	103743	7608	0.159
пауза					
п	[*п*]	108270	109150	880	0.018
о	[*а*]	109150	114935	5785	0.121
б	***[б']***	**114697**	**120008**	**5311**	**0.111**
е	[*е*]	118896	126881	7985	0.167
д	***[д]***	**126894**	**131026**	**4132**	**0.086**
о	[*а*]	130842	134300	3458	0.072
й	***[й']***	**136564**	**140147**	**3583**	**0.075**

Таблица А.3 – Диапазоны звуков предложения 3

Буквы	Звуки	Начальная граница	Конечная граница	Длительность, отсчеты	Длительность, сек
1	2	3	4	5	6
д	[*д'*]	7372	13427	6055	0.126
е	[*и*]	13577	16473	2896	0.060
ж	***[ж]***	**16653**	**23939**	**7286**	**0.152**
у	[*у*]	23845	28922	5077	0.106

Окончание таблицы А.3

Буквы	Звуки	Начальная граница	Конечная граница	Длительность, отсчеты	Длительность, сек
1	**2**	**3**	**4**	**5**	**6**
р	[*р*]	28960	30314	1354	0.028
н	[*н*]	30915	34902	3987	0.083
ы	[*ы*]	35692	40168	4476	0.093
й	[*й’*]	40168	43289	3121	0.065
пауза					
п	[*п*]	46937	48179	1242	0.026
р	[*р’*]	48254	49532	1278	0.027
и	[*и*]	49495	54196	4701	0.098
н	[*н’*]	54685	58559	3874	0.081
ё	[*о*]	59123	67247	8124	0.169
с	[*с*]	67736	75747	8011	0.167
пауза					
о	[*а*]	87895	92784	4889	0.102
д	[*д’*]	93687	100908	7221	0.150
ё	[*о*]	100382	108392	8010	0.167
ж	**[*ж*]**	**108456**	**112411**	**3955**	**0.082**
н	[*н*]	118999	123174	4175	0.087
у	[*у*]	123914	124979	1065	0.022
ю	[*йу*]	125178	126842	1664	0.035
пауза					
щ	**[*ш’*]**	**131979**	**137183**	**5204**	**0.108**
ё	[*о*]	137287	144605	7318	0.153
т	[*т*]	146268	147998	1730	0.036
к	[*к*]	150227	152603	2376	0.050
у	[*у*]	152610	159227	6617	0.138

ПРИЛОЖЕНИЕ Б

«Слуховое восприятие искажений речевого сигнала, вызванных кодированием»

Вам предлагается прослушать 3 предложения качества студийной записи (48 кГц), воспроизводимые в оригинале и при наличии искажений в определенном наборе звуков. Необходимо оценить уровень слышимости данных икажений. Каждое предложение будет воспроизведено несколько раз с изменением параметра кодирования *K*.В зависимости от его величины, будет меняться слышимость искажений в речевом сигнале.

Оценка эксперта №1.

Во взрывные звуки предложения 1 был закодирован звук «*г*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.1 – восприятие искажений в предложении 1 экспертом №1

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	4	5
р	Искажений нет			
у	Искажений нет			
к	Искажения есть		+	+
о	Искажений нет			
в	Искажений нет			
о	Искажений нет			

Продолжение таблицы Б.1

Буквы	Наличие искажений по факту	Слышимость искажений (К=0.1)	Слышимость искажений (К=0.5)	Слышимость искажений (К=1)
1	**2**	**3**	**4**	**5**
д	Искажения есть		+	
и	Искажений нет			
т	Искажения есть	+		
е	Искажений нет			
ль	Искажений нет			
пауза	Искажений нет			
п	Искажения есть		+	+
о	Искажений нет			
т	Искажения есть			+
р	Искажений нет			
е	Искажений нет			
б	Искажения есть			
о	Искажений нет			
в	Искажений нет			
а	Искажений нет			
л	Искажений нет			
пауза	Искажений нет			
п	Искажения есть	+	+	
р	Искажений нет			
е	Искажений нет			
к	Искажения есть			
р	Искажений нет			
а	Искажений нет			
т	Искажения есть			+
и	Искажений нет			
ть	Искажения есть		+	
пауза	Искажений нет			
п	Искажения есть	+	+	+

Окончание таблицы Б.1

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**4**	**5**
о	Искажений нет			
с	Искажений нет			
а	Искажений нет			
д	Искажения есть			+
к	Искажения есть			
у	Искажений нет			

В звонкие звуки предложения 2 был закодирован звук «*о*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.2 – восприятие искажений в предложении 2 экспертом №1

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**4**	**5**
г	Искажения есть	+	+	+
е	Искажений нет			
р	Искажения есть			
о	Искажений нет			
и	Искажений нет			
пауза	Искажений нет			
в	Искажения есть			+
е	Искажений нет			
р	Искажения есть			+

Окончание таблицы Б.2

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**4**	**5**
н	Искажения есть			+
у	Искажений нет			
л	Искажения есть			
и	Искажений нет			
сь	Искажений нет			
пауза	Искажений нет			
д	Искажения есть			+
о	Искажений нет			
м	Искажения есть			
о	Искажений нет			
й	Искажения есть			+
пауза	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			
п	Искажений нет			
о	Искажений нет			
б	Искажения есть	+	+	+
е	Искажений нет			
д	Искажения есть		+	+
о	Искажений нет			
й	Искажения есть		+	+

В шипящие звуки предложения 3 был закодирован звук «*д*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.3 – восприятие искажений в предложении 3 экспертом №1

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	4	5
д	Искажений нет			
е	Искажений нет			
ж	Искажения есть			
у	Искажений нет			
р	Искажений нет			
н	Искажений нет			
ы	Искажений нет			
й	Искажений нет			
пауза	Искажений нет			
п	Искажений нет			
р	Искажений нет			
и	Искажений нет			
н	Искажений нет			
ё	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			
о	Искажений нет			
д	Искажений нет			
ё	Искажений нет			
ж	Искажения есть			
н	Искажений нет			
у	Искажений нет			
ю	Искажений нет			
пауза	Искажений нет			
щ	Искажения есть			
ё	Искажений нет			
т	Искажений нет			
к	Искажений нет			
у	Искажений нет			

«Слуховое восприятие искажений речевого сигнала, вызванных кодированием»

Вам предлагается прослушать 3 предложения качества студийной записи (48 кГц), воспроизводимые в оригинале и при наличии искажений в определенном наборе звуков. Необходимо оценить уровень слышимости данных искажений. Каждое предложение будет воспроизведено несколько раз с изменением параметра кодирования *K*.В зависимости от его величины, будет меняться слышимость искажений в речевом сигнале.

Оценка эксперта №2.

Во взрывные звуки предложения 1 был закодирован звук «*г*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.4 – восприятие искажений в предложении 1 экспертом №2

Буквы	**Наличие искажений по факту**	**Слышимость искажений (K=0.1)**	**Слышимость искажений (K=0.5)**	**Слышимость искажений (K=1)**
1	**2**	**3**	**4**	**5**
р	Искажений нет			
у	Искажений нет			
к	Искажения есть			
о	Искажений нет			
в	Искажений нет			
о	Искажений нет			
д	Искажения есть		+	+
и	Искажений нет			
т	Искажения есть		+	

Продолжение таблицы Б.4

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**4**	**5**
е	Искажений нет			
ль	Искажений нет			
пауза	Искажений нет			
п	Искажения есть			
о	Искажений нет			
т	Искажения есть	+	+	+
р	Искажений нет			
е	Искажений нет			
б	Искажения есть			
о	Искажений нет			
в	Искажений нет			
а	Искажений нет			
л	Искажений нет			
пауза	Искажений нет			
п	Искажения есть	+	+	
р	Искажений нет			
е	Искажений нет			
к	Искажения есть			+
р	Искажений нет			
а	Искажений нет			
т	Искажения есть	+	+	+
и	Искажений нет			
ть	Искажения есть			
пауза	Искажений нет			
п	Искажения есть			
о	Искажений нет			
с	Искажений нет			
а	Искажений нет			

Окончание таблицы Б.4

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	4	5
д	Искажения есть			+
к	Искажения есть			
у	Искажений нет			

В звонкие звуки предложения 2 был закодирован звук «*о*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.5 – восприятие искажений в предложении 2 экспертом №2

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	4	5
г	Искажения есть	+	+	
е	Искажений нет			
р	Искажения есть			+
о	Искажений нет			
и	Искажений нет			
пауза	Искажений нет			
в	Искажения есть			
е	Искажений нет			
р	Искажения есть			+
н	Искажения есть			

Продолжение таблицы Б.5

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**4**	**5**
у	Искажений нет			
л	Искажения есть			+
и	Искажений нет			
сь	Искажений нет			
пауза	Искажений нет			
д	Искажения есть			
о	Искажений нет			
м	Искажения есть			
о	Искажений нет			
й	Искажения есть			
пауза	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			
п	Искажений нет			
о	Искажений нет			
б	Искажения есть	+	+	+
е	Искажений нет			
д	Искажения есть		+	+
о	Искажений нет			
й	Искажения есть		+	+

В шипящие звуки предложения 3 был закодирован звук «*д*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.6 – восприятие искажений в предложении 3 экспертом №2

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	3	3
д	Искажений нет			
е	Искажений нет			
ж	Искажения есть			
у	Искажений нет			
р	Искажений нет			
н	Искажений нет			
ы	Искажений нет			
й	Искажений нет			
пауза	Искажений нет			
п	Искажений нет			
р	Искажений нет			
и	Искажений нет			
н	Искажений нет			
ё	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			
о	Искажений нет			
д	Искажений нет			
ё	Искажений нет			
ж	Искажения есть			
н	Искажений нет			
у	Искажений нет			
ю	Искажений нет			
пауза	Искажений нет			
щ	Искажения есть			
ё	Искажений нет			
т	Искажений нет			
к	Искажений нет			
у	Искажений нет			

«Слуховое восприятие искажений речевого сигнала, вызванных кодированием»

Вам предлагается прослушать 3 предложения качества студийной записи (48 кГц), воспроизводимые в оригинале и при наличии искажений в определенном наборе звуков. Необходимо оценить уровень слышимости данных искажений. Каждое предложение будет воспроизведено несколько раз с изменением параметра кодирования *K*.В зависимости от его величины, будет меняться слышимость искажений в речевом сигнале.

Оценка эксперта №3.

Во взрывные звуки предложения 1 был закодирован звук «*г*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.7 – восприятие искажений в предложении 1 экспертом №3

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	4	5
р	Искажений нет			
у	Искажений нет			
к	Искажения есть			
о	Искажений нет			
в	Искажений нет			
о	Искажений нет			
д	Искажения есть		+	+
и	Искажений нет			
т	Искажения есть		+	
е	Искажений нет			
ль	Искажений нет			

Окончание таблицы Б.7

Буквы	Наличие искажений по факту	Слышимость искажений (К=0.1)	Слышимость искажений (К=0.5)	Слышимость искажений (К=1)
1	2	3	4	5
пауза	Искажений нет			
п	Искажения есть			
о	Искажений нет			
т	Искажения есть	+	+	+
р	Искажений нет			
е	Искажений нет			
б	Искажения есть			
о	Искажений нет			
в	Искажений нет			
а	Искажений нет			
л	Искажений нет			
пауза	Искажений нет			
п	Искажения есть	+	+	
р	Искажений нет			
е	Искажений нет			
к	Искажения есть			+
р	Искажений нет			
а	Искажений нет			
т	Искажения есть	+	+	+
и	Искажений нет			
ть	Искажения есть			
пауза	Искажений нет			
п	Искажения есть			
о	Искажений нет			
с	Искажений нет			
а	Искажений нет			
д	Искажения есть			+
к	Искажения есть			
у	Искажений нет			

В звонкие звуки предложения 2 был закодирован звук «*о*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.8 – восприятие искажений в предложении 2 экспертом №3

Буквы	**Наличие искажений по факту**	**Слышимость искажений (K=0.1)**	**Слышимость искажений (K=0.5)**	**Слышимость искажений (K=1)**
1	**2**	**3**	**3**	**3**
г	Искажения есть	+	+	
е	Искажений нет			
р	Искажения есть			+
о	Искажений нет			
и	Искажений нет			
пауза	Искажений нет			
в	Искажения есть			
е	Искажений нет			
р	Искажения есть			+
н	Искажения есть			
у	Искажений нет			
л	Искажения есть			+
и	Искажений нет			
сь	Искажений нет			
пауза	Искажений нет			
д	Искажения есть			
о	Искажений нет			
м	Искажения есть			
о	Искажений нет			
й	Искажения есть			
пауза	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			

Окончание таблицы Б.8

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**3**	**3**
п	Искажений нет			
о	Искажений нет			
б	Искажения есть	+	+	+
е	Искажений нет			
д	Искажения есть		+	+
о	Искажений нет			
й	Искажения есть		+	+

В шипящие звуки предложения 3 был закодирован звук «*д*». В речевом сигнале закодированный звук проявляется как шум в виде «потрескивания». В случае, если вы услышали данный шум в звуках, выделенных оранжевым цветом, поставьте в графе «слышимость искажений (K=…)» знак «+».

Таблица Б.9 – восприятие искажений в предложении 3 экспертом №3

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	**2**	**3**	**3**	**3**
д	Искажений нет			
е	Искажений нет			
ж	Искажения есть			
у	Искажений нет			
р	Искажений нет			
н	Искажений нет			
ы	Искажений нет			
й	Искажений нет			
пауза	Искажений нет			
п	Искажений нет			

Окончание таблицы Б.9

Буквы	Наличие искажений по факту	Слышимость искажений (K=0.1)	Слышимость искажений (K=0.5)	Слышимость искажений (K=1)
1	2	3	3	3
р	Искажений нет			
и	Искажений нет			
н	Искажений нет			
ё	Искажений нет			
с	Искажений нет			
пауза	Искажений нет			
о	Искажений нет			
д	Искажений нет			
ё	Искажений нет			
ж	Искажения есть			
н	Искажений нет			
у	Искажений нет			
ю	Искажений нет			
пауза	Искажений нет			
щ	Искажения есть			
ё	Искажений нет			
т	Искажений нет			
к	Искажений нет			
у	Искажений нет			