

приводит к изменению разборчивости, а понижение, наоборот, существенно её снижает. Этот результат имеет важное практическое значение, так как позволяет применить данную технологию формирования и обработки клипированной речи в существующих цифровых системах передачи речи.

#### Список использованных источников

1. Козленко Н.И. Помехоустойчивость дискретной передачи непрерывных сообщений.- М.: Радиотехника, 2003г.-352 с.: ил.
2. Бухвинер В.Е. Управляемое компандирование звуковых сигналов.- М.: Связь, 1978.-208 с.: ил.
3. Ричард Лайонс. Цифровая обработка сигналов: Второе издание. Пер с англ.-М.: ООО «Бином-Пресс», 2009.- 656 с.:ил.
4. Цифровая обработка сигналов в LabVIEW: учеб. пособие / под ред. В. П. Федосова. - М.: ДМК Пресс, 2007.- 456 с.

## ОБ ИСПОЛЬЗОВАНИИ АППАРАТНО-ПРОГРАММНОГО МОДЕЛИ В ИССЛЕДОВАНИИ СТЕГАНОГРАФИЧЕСКОГО МЕТОДА РАСШИРЕНИЯ СПЕКТРА

**Гурьянова О.И.**

г. Белгород, ФГАОУ ВО «Белгородский государственный национальный  
исследовательский университет»,  
02.04.01 – «Математика и компьютерные науки»

**Азизова Д.Г.**

г. Белгород, ФГАОУ ВО «Белгородский государственный национальный  
исследовательский университет»,  
09.04.03 – «Прикладная информатика»

**Аннотация.** В статье рассматривается аппаратно-программная модель стеганографического метода расширения спектра, разработанная для среды National Instruments. Модель позволяет исследовать восприятие синтезированного аудио-сигнала, позволяющего в реальном режиме времени оценивать скрытность кодируемой информации. В модели имеется возможность изменения параметров кодирования: кодируемого символа, величины энергии, места кодирования.

Методы стеганографии имеют широкое применение и используются для систем скрытой связи, для кодирования скрыты меток и т.д. [1]. Так же известно, что стеганографическая система является разрушенной если обнаружен факт кодирования [2]. Как показало множество экспериментов [3] использование мер и оценок не всегда позволяет оценить скрытность закодированной информации. Наиболее правильным и естественным способом оценки скрытности, является прослушивание синтезированного сигнала, являющегося результатом результата стеганографического кодирования. В качестве меры внедрения целесообразно использовать значение энергии сигнала:

$$\|\vec{x}\|^2 = \sum_{i=1}^N x_i^2, \quad (1)$$

где  $x_i$  – мгновенное значение амплитуды аудио-сигнала.

При этом стоит отметить, что для звуков имеющих разную природу, в частности сигналов, являющихся результатом регистрации речи порог определяющий скрытность будет различным. В этом случае интерес представляет эмпирический поиск порога для конкретного звука, который может быть использован в дальнейшем для построения психоакустической модели.

Работа посвящена использованию визуальной среды National Instruments LabView, применяемой для оценки скрытности в реальном режиме времени, информации закодированной стеганографическим методом расширения спектра [3]

$$\vec{\tilde{x}} = \vec{x} + K \cdot e \cdot \vec{u}, \quad (2)$$

где  $\vec{x}$  – исходный отрезок данных;  $\vec{u}$  – отрезок, соответствующий псевдослучайной последовательности (ПСП);  $K$  – весовой коэффициент;  $e$  – кодовое отображение двоичного бита контрольной информации,  $e \in \{-1, 1\}$ .

В работах [3, 4] его предлагается выбирать весовой коэффициент  $K$  равным [4]:

$$K = h \cdot \frac{\langle \tilde{x}, \tilde{u} \rangle}{\sqrt{\|\tilde{u}\|^2 \cdot \|\tilde{x}\|^2}}, \quad (3)$$

где  $h$  – коэффициент, регулируемый в реальном режиме времени.

Декодирование бита контрольной информации из данных происходит путем определения знака скалярного произведения отрезка данных и псевдослучайной последовательности:

$$\tilde{e} = \text{sign}(\langle \tilde{x}, \tilde{u} \rangle), \quad (4)$$

где  $\text{sign}()$  – операция выделения знака.

Создание программного обеспечения для решения поставленной задачи осуществлялось в среде программирования NI LabVIEW 8.6 [5]. Структурная схема аппаратно-программной модели стеганографического метода расширения спектра, представлена на рис. 1.

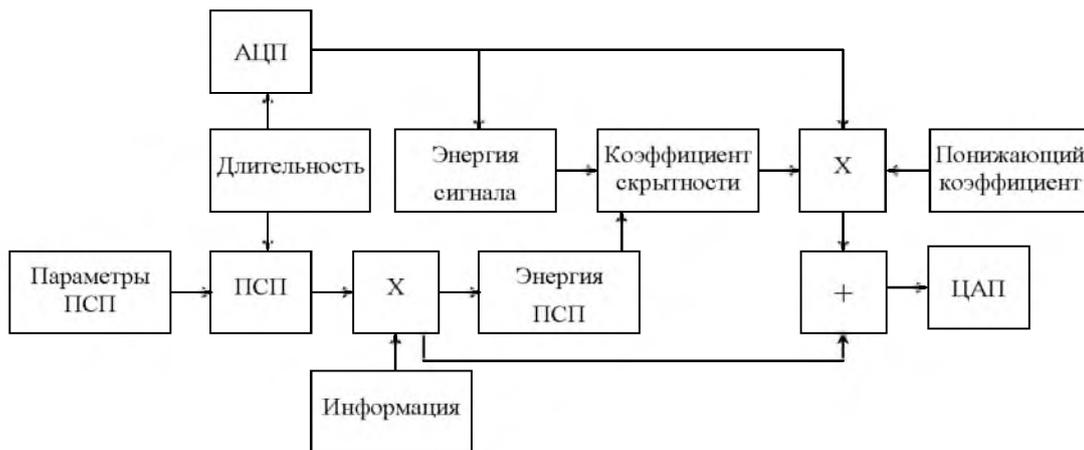


Рисунок 1 – Структурная схема стеганографического метода расширения спектра

На рисунке 1 представлены: «АЦП» – аналого-цифровой преобразователь, осуществляющий загрузку сигнала; «X» - перемножитель; «+» – блок осуществляющий суммирование; «ЦАП» – цифро-аналоговый преобразователь, осуществляющий выгрузку сигнала (его воспроизведение).

Объект исследования – метод расширения спектра имеет настройки, путем задания коэффициента скрытности зависящий от энергии сигнала и энергии ПСП, принцип задания основан на равенстве (3) [4]. Понижающий/повышающий коэффициент, регулируемый в режиме реального времени позволяет контролировать скрытность «Gain» (рис.2).

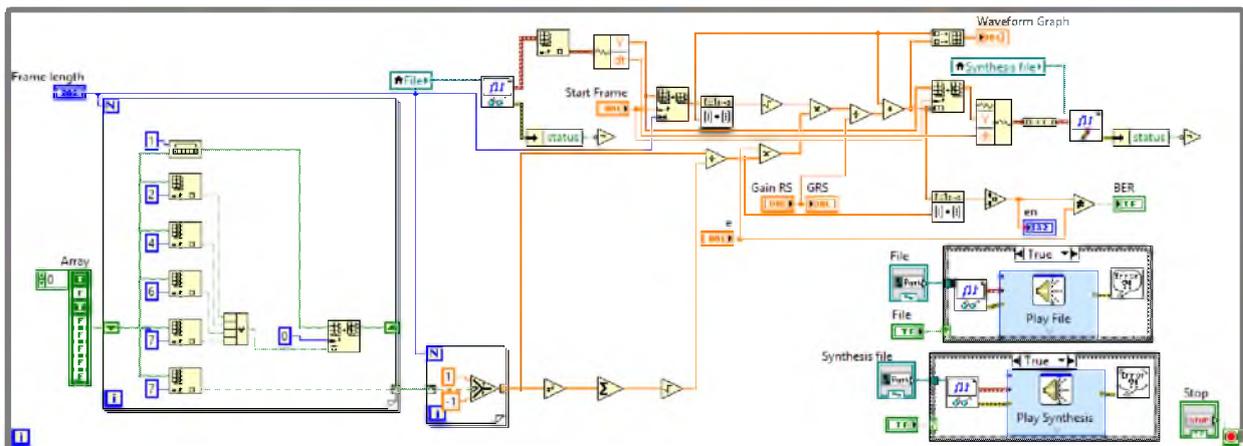


Рисунок 2 – Блок-схема моделирования стеганографического метода расширения спектра

Также разработанная программная поддержка (рис. 3), позволяет кроме анализа однозначности извлечения, прослушать результат стеганографического кодирования и визуально оценить возникающие искажения.

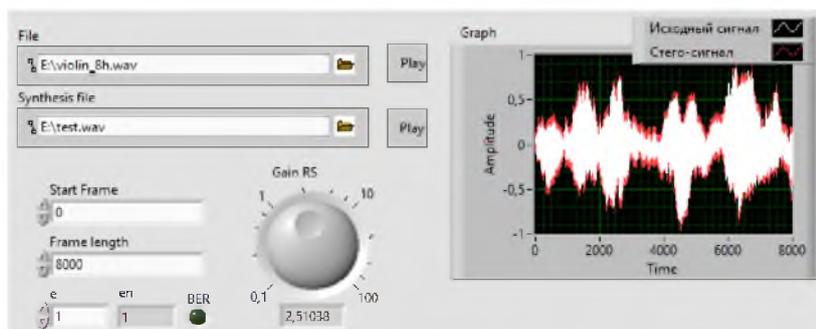


Рисунок 3 – Результат кодирования и вызванные изменения

Созданная программная поддержка, позволяет ускорить процесс создания психоакустической модели, по сравнению со средой MatLab. Это возможно в связи с возможностью изменений в реальном режиме времени. Разработанная программная поддержка, может быть применена для анализа и обучения методов стеганографии.

#### Список использованных источников

1. Конахович Г.Ф. 2006. Компьютерная стеганография. Теория и практика Г.Ф. Конахович, А.Ю. Пузыренко. – Киев, «МК-Пресс». С.288.
2. Грибунин В.Г. 2002. Цифровая стеганография. Аспекты защиты / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. - М., Солон-Пресс. С.261.
3. Жиликов Е. Г., Лихолоб П. Г., Медведева А. А., Прохоренко Е. Н. Исследование чувствительности некоторых мер качества скрытия информации в речевых сигналах // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. – 2016. – Т. 9, № 230. – С. 174-179.
4. Жиликов Е. Г., Пашинцев В. П., Белов С. П., Лихолоб П. Г. О методе скрытного кодирования контрольной информации в речевые данные // Инфокоммуникационные технологии. – 2015. – Т. 13, № 3. – С. 325--333.
5. Lykholob, P.G. Research of sensitivity of some measures of quality assessment of hidden information in the audio content [Текст] // Medvedeva, A.A. Likhogodina, E.S. Mishina, O.O. RESEARCH RESULT. Information technologies. №4. v.1. 2016. pp.21-25 URL: [http://tr.bsu.edu.ru/media/information/2016/4/3\\_it.pdf](http://tr.bsu.edu.ru/media/information/2016/4/3_it.pdf) DOI: 10.18413/2518-1092-2016-1-4-21-24
6. <http://www.ni.com/pxi/> – раздел на сайте National Instruments

## АНАЛИЗ КОНЦЕПЦИИ ПОСТРОЕНИЯ ЕДИНОЙ ТОЧКИ ДОСТУПА В СЕТИ INTERNET НА БАЗЕ КОМПЬЮТЕРНОЙ СЕТИ RSNET

Ельцова Н.С.

г. Орел, ФГБОУ ВО Орловский государственный университет имени И.С. Тургенева,  
11.03.02 – «Инфокоммуникационные технологии и системы связи»

**Аннотация.** Данная статья посвящена RSNet (Russian State Network) – разрабатываемому в России выделенному безопасному сегменту интернета, созданному с целью его применения федеральными органами государственной власти, и имеющему усиленные меры безопасности.

Детальное изучение процессов развития информационных технологий позволяет сделать вывод о наличии множества открытий, позволивших сделать современную связь и информационные ресурсы неотъемлемой частью человеческого существования.

Для современного этапа развития общества характерно еще и наличие его прочной связи с развитой информационной структурой, вследствие чего информация приобретает политическое, экономическое и материальное выражение. Информационный ресурс в настоящее время выступает в роли основных источников экономической и военной мощи государства, поэтому все более актуальный характер приобретает задача обеспечения информационной безопасности Российской Федерации как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач. В рамках их решения разрабатывается специально выделенный безопасный сегмент Интернета, предназначенный для федеральных органов государственной власти и имеющий усиленные меры безопасности – RSNet (Russian State Network). [1]

Данная сеть послужила следующим шагом в развитии сети RGIN - сегмента сети Интернет для органов государственной власти Российской Федерации (Russian Government Internet Network). Сеть RSNet