УДК 004.056.5

ЦИФРОВОЕ СКРЕМБЛИРОВАНИЕ КАК СПОСОБ ЗАЩИТЫ РЕЧЕВОГО СИГНАЛА

Константинов Д.А.

Студент,

ФГАОУ ВО «Севастопольский государственный университет»,

Севастополь, Россия

Мирянова А.Д.

Студент,

ФГАОУ ВО «Севастопольский государственный университет»,

Севастополь, Россия

Мирянова В.Н.

Кандидат технических наук, доцент

ФГАОУ ВО «Севастопольский государственный университет»,

Севастополь, Россия

Аннотация

Скремблирование может быть использовано в инфокоммуникационных системах с целью защиты передаваемой информации от несанкционированного доступа, например, для шифровки речевого сигнала путем преобразования его в случайную последовательность битов. Скремблирование используется обычно, если не требуется высокая криптостойкость. Существуют цифровые и аналоговые способы закрытия речи. В системах цифровой связи дискретизированный речевой сигнал преобразуется в соответствии с выбранным алгоритмом шифрования. Для передачи и хранения речевой информации, а также уменьшения объема или скорости передачи, применяют различные методы сжатия передаваемого сообщения, в том числе вокодеры. В статье приводится сравнительный анализ вокодеров.

Ключевые слова: информационная безопасность, вокодер, дешифрование,

дискретизация речи, защита информации, скремблер, скремблирование, цифровая связь, шифрование.

DIGITAL SCRAMBLING AS A METHOD OF SPEECH SIGNAL PROTECTION

Konstantinov D.A.

student,

Sevastopol State University,

Sevastopol, Russia

Mirianova A.D.

student

Sevastopol State University,

Sevastopol, Russia

Mirianova V.N.

Ph.D , Associate Professor,

Sevastopol State University,

Sevastopol, Russia

Abstract

Scrambling can be used in infocommunication systems to protect transmitted information from unauthorized access, for example, to encrypt a speech signal by converting it into a random sequence of bits. Scrambling is usually used when high security is not required. There are digital and analog ways to close speech. In digital communication systems, the sampled speech signal is converted in accordance with the selected encryption algorithm. Various methods of compressing the transmitted message are used for transmit and store speech information, as well as reduce the volume or transmission rate, including vocoders. The article provides a comparative analysis of vocoders.

Keywords: information security, decryption, speech sampling, information security,

scrambler, scrambling, digital communications, encryption.

При цифровой передаче информации скремблер (от англ. to scramble – перемешивать, шифровать) можно определить, как алгоритм, шифрующий цифровой поток информации так, что на выходе получается последовательность, обладающая свойствами случайной: появление нуля и единицы равновероятно [1]. С одной стороны, это позволяет четко выделить тактовую частоту и постоянную мощность передаваемого сигнала, что и повышает надежность синхронизации; с другой стороны — обеспечить информационную безопасность передаваемого сигнала. Такое преобразование не изменяет скорость передачи, а также является обратимым, то есть данные можно восстановить обратным алгоритмом.

Идея разработки устройств цифрового закрытия речи состоит в сохранении характеристик, которые больше всего влияют на разборчивость сообщения. Однако, для передачи и хранения речевой информации, а также уменьшения объема или скорости передачи, применяют различные методы сжатия передаваемого сообщения.

Речевой сигнал обладает определенной избыточностью, которая не влияет на смысловое содержание сообщения. Сжатие частично уменьшает избыточность, не затрагивая разборчивость и качество восприятия речи. Но лишает особых признаков, необходимых для экспертной идентификации.

Алгоритмы сжатия речи могут быть реализованы как аппаратными, так и программными методами. Их делят на *вокодеры* (от англ. Voice и Coder) и *липредеры* (от англ. Linear и Predictor).

Вокодер – это устройство кодирования, учитывающее статистические свойства речевого сигнала. Вокодеры делят по принципу действия на два класса: речеэлементные и параметрические.

Речеэлементные вокодеры на передающем конце распознают, какие элементы речи произнесены, а на приёмном конце эти элементы воссоздаются

по правилам речеобразования или извлекаются из памяти устройства. В таких вокодерах решают задачу распознавания элементов речи.

В *параметрических* вокодерах с речевого сигнала выделяют два типа параметров и по этим параметрам в декодере синтезируют речь:

- параметры, которые характеризуют источник речевых колебаний – частота основного тона, изменение во времени, моменты появления и исчезновения основного тона шумового сигнала;
- параметры, которые характеризуют огибающую спектра речевого сигнала.

В декодере по заданным параметрам генерируются основной тон, шум, а затем пропускаются через гребенку полосовых фильтров для восстановления огибающей спектра речевого сигнала.

По принципу определения параметров фильтровой функции различают вокодеры:

- полосные (канальные);
- формантные;
- ортогональные;
- липредеры (вокодеры с линейным предсказанием).

В *полосных* вокодерах спектр речи делится на 7 – 20 полос (каналов) аналоговыми или цифровыми полосовыми фильтрами. Большее число каналов в вокодере дает большую натуральность и разборчивость.

Полосной вокодер состоит из двух частей: анализирующая (передающая сторона) и синтезирующая (принимающая сторона) (рис. 1). Полосовые фильтры перекрывают диапазон неравномерно, что существенно для восприятия речи. На выходе фильтра колебания детектируются и проходят через фильтр нижних частот (ФНЧ). Выходные данные в разной степени представляются огибающей спектра речи. Параметры, характеризующие источник возбуждения, получаются с помощью обнаружения тон-шум, определяющего, является ли звук звонким или глухим [3, 4].

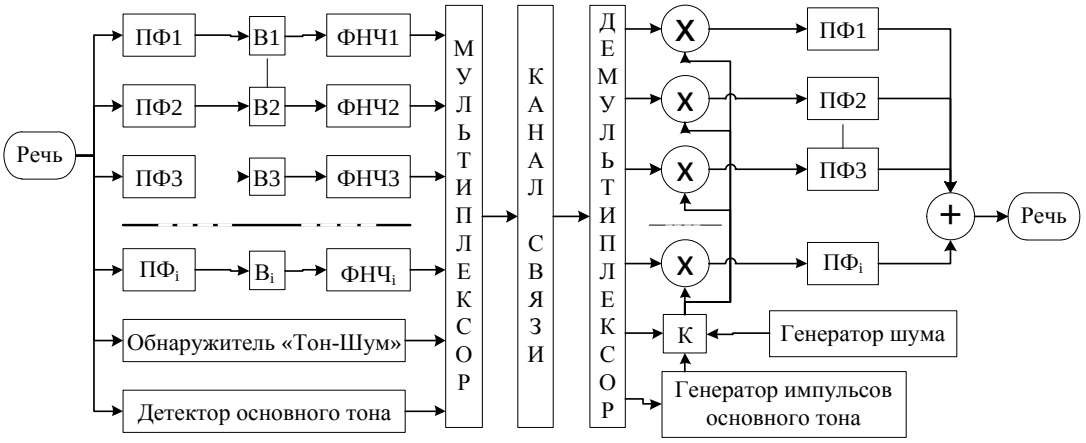

Рис. 1 – Блок-схема полосного вокодера [3]

Канальные сигналы, сигнал тон-шум и значение высоты основного тона кодируются и передаются приемнику по каналу связи. Если передача происходит без ошибок, то задача приемника состоит в восстановлении речи на основе переданных параметров. Источник возбуждения либо генератор импульсов, либо генератор шума. В зависимости от сигнала тон-шум один из них подключается к гребенке фильтров, идентичных фильтрам анализатора, и возбуждает их. Детектированные сигналы огибающей спектра используются для модуляции колебаний на выходах соответствующих полосовых фильтров. Для создания звуковой мощности каждой из частотных полос. Синтезированный речевой сигнал получается после суммирования всех промодулированных полосовых колебаний.

В *формантных* вокодерах огибающая спектра речи описывается комбинацией формант (резонансных частот голосового тракта). Основные параметры формант — центральная частота, амплитуда и ширина спектра.

Принцип построения формантного вокодера (рис. 2) похож на принцип естественного речеобразования и приема речи. Речевой тракт представляет совокупность резонаторов, которые изменяются в процессе речи. А формантный вокодер выделяет из речевого сигнала основные сигналы-параметры, которые в приемнике воздействуют на резонансные контуры и воспроизводят требуемую огибающую спектра.

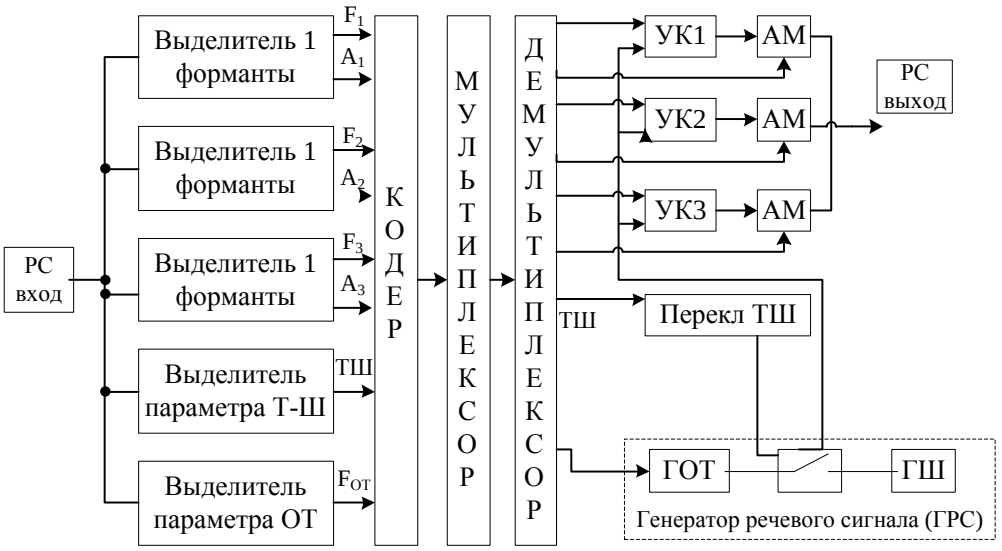

Рис. 2 – Структурная схема формантного вокодера [5]

Передающая сторона в анализаторе вокодера выделяет структурные сигналы-параметры для первых трех формант и интонационные параметры. Для оценки амплитуды форманты используется её усредненный уровень, который получают с помощью полосовых фильтров, выпрямителей и ФНЧ. Формантные частоты находят при помощи метода фильтрации. Синтезатор формантного вокодера состоит из трех управляемых резонансных контуров (УК) с плавной перестройкой их частоты под приходящий параметр. Модуляторы взаимодействуют резонансные и колебательные процессы в зависимости от уровня соответствующего сигнала-параметра.

В *ортогональных* вокодерах (рис. 3) огибающая мгновенного спектра разлагается на составные части в ряд по выбранной системе ортогональных базисных функций. Рассчитанные коэффициенты этого ряда передаются на приемную сторону.

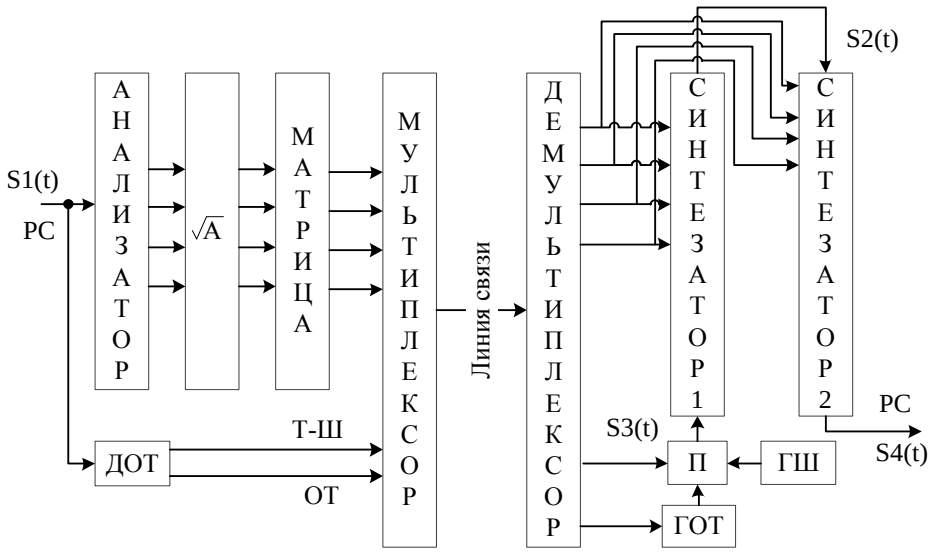

Рис. 3 – Блок-схема ортогонального вокодера [5]

На приемной стороне сигнал-параметры управляют двумя синтезаторами линейного типа. На вход линии задержки первого синтезатора подается сигнал от источника речевых колебаний, т. е. от генератора основного тона или генератора шума, а на вход линии задержки второго синтезатора подается сигнал с выхода первого синтезатора. В результате этой операции огибающей спектра, получаемая спектральная огибающая становится близкой к исходной как по формантным кривым, так и вследствие устранения ложных формант. Экспериментально доказано, что в данном случае разборчивость лучше по сравнению с линейным вокодером.

При создании ортогональных вокодеров определяют систему ортогональных функций, такую, чтобы число значащих слагаемых ряда, в который раскладывается речевой сигнал, было минимальным.

Вокодеры с *линейным предсказанием* речи получили наибольшее распространение среди систем цифрового кодирования с последующим шифрованием. Область применения – низкоскоростная передача речи и ее хранение.

В соответствии с рис. 4 вокодер состоит из передатчика, канала связи и приемника. В передатчике вычисляются коэффициенты линейного

предсказания и параметры основного тона и шумовой составляющей речи, которые передаются по каналу связи. В приемнике вычисленные коэффициенты и параметры используются для синтезирования речевого сигнала.

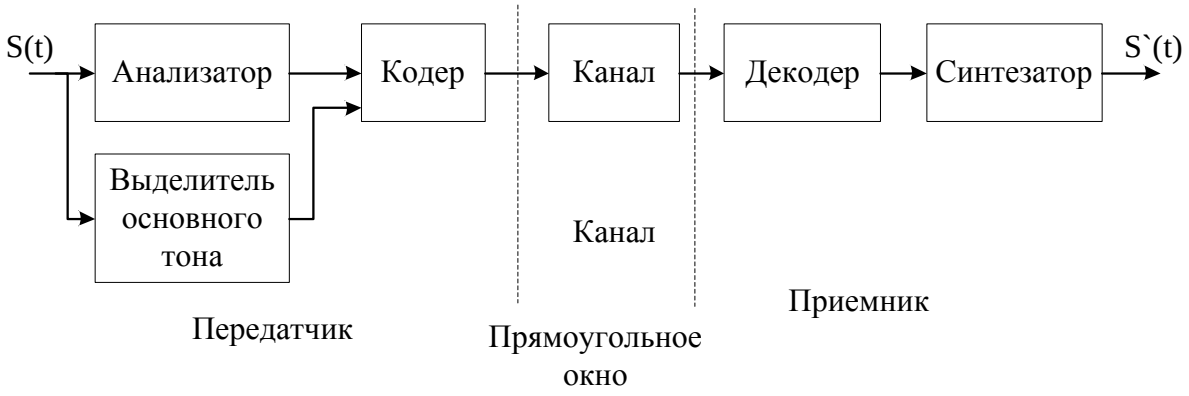

Рис. 4 – Структурная схема вокодера с линейным предсказанием [5]

На практике возникает сложность реализации схем вокодер с линейным предсказанием. Во-первых, речевой сигнал содержит два вида внутренних корреляционных связей, с кратковременной и долговременной избыточностью. Поэтому используются два предсказателя. Кратковременный предсказатель учитывает кратковременную избыточность и связан с корреляциями между близко расположенными отсчетами сигнала. Долговременный предсказатель определяет тонкую структуру и связан с корреляцией двух отрезков сигнала между собой.

Сочетание двух предсказателей с разными характеристиками позволяет устранить остаточную избыточность и приблизить остаток предсказания к белому шуму.

Во-вторых, использование остатка предсказания в качестве сигнала возбуждения неэффективно. Для кодирования требуется слишком большое число бит. Поэтому на практике применяются более экономичные методы формирования сигнала возбуждения.

Рассмотренные вокодеры обеспечивают сжатие сигнала до 1200 – 4800

Бит/с, позволяя восстановить частоту основного тона с дискретностью в несколько герц и с невысокой точностью огибающую спектра сигнала с периодом изменения 16 – 40 мс, при этом даже при достаточно высокой разборчивости речи теряются многие индивидуальные особенности диктора.

Среди разработанных алгоритмов кодирования и декодирования в настоящее время заметно выделяются вокодеры с линейным предсказанием (липредеры). В отличие от формантных вокодеров зависимость этих методов от данных о механизмах речеобразования отступает на второй план. Липредеры находят широкое применение. Некоторые липредеры позволяют снизить скорость передачи речи до 1200 бит/сек при хороших характеристиках переданного речевого сигнала.

Итак, для передачи сигнала по цифровому каналу связи, необходимо провести дискретизацию по времени. В таком виде он преобразуется в соответствии с выбранным алгоритмом шифрования. Для сохранения характеристик, влияющих на разборчивость сообщения, требуется сжать речевой сигнал при передаче вокодером.

Вокодеры позволяют устранить избыточность речевого сообщения. Полосные вокодеры являются системой анализа синтеза речи. Точное определение параметров основного тона и сигнала тон/шум усложняет их реализацию. Без точных параметров характеристик сигналов разборчивость сообщения на выходе вокодера является низкой.

Вокодеры с линейным предсказанием используются для низкоскоростной передачи речи и ее хранения. Совокупность параметров выбирается с учетом удобства для кодирования и передачи.

Библиографический список:

1. Тумбинская, М.В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М.В. Тумбинская, М.В. Петровский. — Санкт-Петербург: Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст: электронный // Лань : электронно-библиотечная система. — URL:

https://e.lanbook.com/book/207095.

2. Сергиенко А. Б. Цифровая обработка сигналов: учеб. пособие. — 3-е изд. — СПб.: БХВ-Петербург, 2011. — 768 с.

3. Панько, С. П. Радиотехнические системы специального назначения. Системы связи : учебник / С. П. Панько, Е. Н. Гарин, В. В. Сухотин. — Красноярск : СФУ, 2019. — 340 с. — ISBN 978-5-7638-4014-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/128729.

4. Голиков А.М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: Учебное пособие/А.М. Голиков. — СПб.: Изд-во «Лань», 2018. — 452с.

5. Рабинер, Л. Р. Цифровая обработка речевых сигналов: учебник / Л. Рабинер, Р. В. Шафер; пер. с англ. под ред. М. В. Назарова, Ю. Н. Прохорова - М: Радио и связь, 1981. – 496 с.

6. Подвальный С.Л. Обзор методов и алгоритмов сжатия речевой информации в системах цифровой радиосвязи/ А.Д. Рощупкин // Вестник ВГТУ. — 2017. — №2. — URL: https://cyberleninka.ru/article/n/obzor-metodov-i-algoritmov-szhatiya-rechevoy-informatsii-v-sistemah-tsifrovoy-radiosvyazi.

7. Большов О.А. Пороговые сигналы при предельном ограничении речи //Спецтехника и связь. — 2010. — №2-3. — URL: https://cyberleninka.ru/article/n/porogovye-signaly-pri-predelnom-ogranichenii-rechi

Оригинальность 85%