СИСТЕМА ПЕРЕДАЧИ ПРИВАТНОЙ ИНФОРМАЦИИ НА ОСНОВЕ СКРЕМБЛИРОВАННЫХ СИГНАЛОВ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Берёзкин Р.В.

Дубровский В.В. – к.ф.-м. н., доцент

Наибольшая часть аппаратуры засекречивания речевых сигналов использует в настоящее время метод аналогового скремблирования, поскольку, во-первых, это дешевле, во-вторых, эта аппаратура применяется в большинстве случаев в стандартных телефонных каналах с полосой 3 кГц, в-третьих, обеспечивается коммерческое качество дешифрованной речи и, в-четвертых, гарантируется достаточно высокая стойкость закрытия.

Скремблирование может выполняться с различными целями. Наиболее распространенная цель - защита передаваемых данных от несанкционированного доступа. Для ее достижения разработано множество методов кодирования и схемных решений. Но нас интересует иная задача, связанная с "разравниванием" спектра сигнала и повышением надежности синхронизации приемника с источником передаваемых по линии данных. Применительно к этой задаче цель скремблирования состоит в исключении из потока данных длинных последовательностей лог. 0, лог. 1 и периодически повторяющихся групп битов. Для этого необходимо преобразовать данные так, чтобы они выглядели как случайные, т. е. лишенные какой-либо видимой закономерности. Обычно скремблирование осуществляется непосредственно перед модуляцией.

Скремблирование (от англ.слова to scramble – перемешивать) производится на передающей стороне с помощью устройства – скремблера, реализующего логическую операцию суммирования по модулю 2 исходного и преобразующего псевдослучайного двоичных сигналов. Например, скремблер может реализовать соотношение:

$$B_i = \mathrm{A}_i \oplus B_{i-3} \oplus B_{i-5}$$

где – двоичная цифра результирующего кода, полученная на i-м такте работы скремблера, – двоичная цифра исходного кода, поступающая на i-м такте на вход скремблера; и – двоичные цифры результирующего кода, полученные на предыдущих тактах работы скремблера, соответственно на 3 и на 5 тактов ранее текущего такта; – операция исключающего ИЛИ (сложение по mod2).

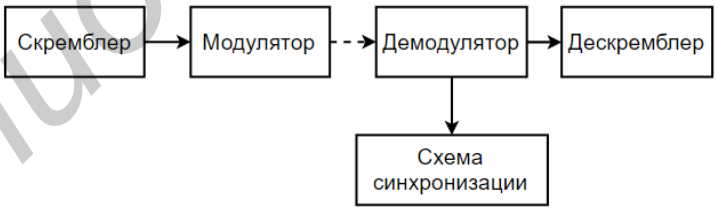

Рис. 1 – Схема включения скремблера и дескремблера в канал связи

Различные алгоритмы скремблирования отличаются количеством слагаемых, которые определяют цифру результирующего кода, и сдвигом между слагаемыми. Основной частью скремблера является генератор псевдослучайной последовательности (ПСП) в виде линейного n-каскадного регистра с обратными связями, формирующий последовательность максимальной длины 2n-1.

Исключительно удобна универсальность, которая заключается в возможности сквозной передачи скремблированного сигнала по сети связи через любые цифровые тракты, так как скремблирование исходной двоичной последовательности осуществляется без преобразования его в другой вид, а выделение исходного сигнала производится только в приемном оборудовании оконечной станции.

Список использованных источников:
1. Оппенгейм А., Шафер Р. Цифровая обработка сигналов. Москва: Изд-во Техносфера, 2006. – 858 с.
2. Сергиенко А.Б. Цифровая обработка сигналов. СПб: Изд-во Питер, 2003. – 604 с.
3. Сато Ю. Без паники! Цифровая обработка сигналов. Москва: Изд-во Додэка-XXI, 2010. – 176 с.