УДК 004.056:061.68

Методы маскирования информации при передаче по каналам связи

Бокуть Л.В., Деев Н.А.*
Белорусский национальный технический университет
Объединенный институт проблем информатики НАН Беларуси*

Для защиты речевой информации от прослушивания часто используются технические средства, разработанные на основе аналоговых методов скремблирования. При аналоговом скремблировании речевой сигнал можно преобразовывать по амплитуде, частоте и времени. Амплитудные преобразования при скремблировании не применяются из-за проблем точного восстановления амплитуды речевого сигнала при его обработке. При частотном преобразовании сигнала используются частотная инверсия сигнала, разбиение полосы частот речевого сигнала на несколько сегментов и частотная инверсия спектра в каждом сегменте относительно его средней частоты, разбиение частоты речевого сигнала на несколько сегментов и их частотные перестановки.

При временных преобразованиях производится разбиение сигнала на речевые сегменты и их перестановка во времени: инверсия по времени сегментов речи, временные перестановки сегментов речевого сигнала. При комбинированных методах преобразования сигнала используют одновременно несколько различных способов скремблирования.

Несмотря на высокое качество и разборчивость восстанавливаемой речи, аналоговые скремблеры обеспечивают лишь низкий или средний уровень защиты информации, но их практическая реализация проще и дешевле. При цифровом скремблировании предполагается дискретизация исходного аналогового сигнала и передача его основных компонент путем преобразования их в цифровой поток данных. Этот поток смешивается с некоторой псевдослучайной последовательностью, вырабатываемой ключевым генератором по одному из криптографических алгоритмов. Полученное таким образом сообщение с помощью модема передается в канал связи, на приемной стороне производятся обратные преобразования с целью получения открытого речевого сигнала. Реализация цифрового скремблирования на практике оказывается довольно сложной и дорогостоящей. Предлагается метод маскирования информации, основанный на формировании и обработке скремблированного частотно-модулированного сигнала, произведением двоичных последовательностей, одна из которых псевдослучайная с известным законом формирования, другая – случайная, формируемая с помощью источника физического шума и компаратора.