

УДК 621.316

А.П. Румянцев (6 курс, каф. РТТК), Ю.В. Ветров, к.т.н., доц.

ИСПОЛЬЗОВАНИЕ АЛГОРИТМА БПФ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕФОННЫХ КАНАЛАХ СВЯЗИ

В современном мире повсеместно применяются телефонные каналы связи. При этом возникает проблема защиты телефонных переговоров. Шифрование телефонного разговора является одним из часто используемых способов защиты. Алгоритмы шифрования телефонных переговоров должны обеспечивать возможность передачи зашифрованного сигнала по существующим телефонным линиям со стандартной частотной полосой, приемлемым качеством расшифрованного сигнала и минимальной задержкой передаваемого сообщения.

Целью данной работы является реализация и исследование особенностей работы алгоритма частотного перемешивания, не требующего временной синхронизации. Этот алгоритм работает с цифровым сигналом, что позволяет использовать быстрые алгоритмы обработки цифровой информации и ускоряет обработку сигнала в масштабе реального времени.

Алгоритм базируется на использовании гребенки квазиидеальных цифровых полосовых фильтров. Входной дискретизованный сигнал пропускается через гребенку фильтров, затем производится перестановка по псевдослучайному закону шифрования откликов полосовых фильтров. После этого из полученной последовательности отчетов создается зашифрованный сигнал, который можно передавать по аналоговой линии связи. В приемном устройстве сигнал дискретизируется и снова поступает на гребенку квазиидеальных цифровых полосовых фильтров, отклики которых переставляются по закону дешифрования и из этой последовательности отчетов получают восстановленный сигнал.

В [1] приводится эффективный метод реализации алгоритма частотного перемешивания, не требующий временной синхронизации. В этом методе, для ускорения вычислений, используется алгоритм БПФ. В [2] показывается, что операция свертки при прохождении сигнала через гребенку полосовых фильтров может быть реализована с помощью БПФ.

Таким образом, в рамках настоящей работы на основе использования БПФ программно реализован алгоритм частотного перемешивания, не требующий временной синхронизации.

ЛИТЕРАТУРА:

1. L.S. Lee, G.C. Chou and C.S.Chang "A New Frequency Domain Speech Scrambling System Which Does Not Require Frame Synchronization" IEEE Trans. On Communication, VOL. COM-32, NO.4, pp. 444-456, April 1984.
2. M.R.Portnoff, "Implementation of the digital phase vocoder using the fast Fourier transform." IEEE Trans. Acoust., Speech, Signal Processing, vol. ASSP-24, pp. 243-248, June 1976.