# ЗАЩИТА РЕЧЕВЫХ СООБЩЕНИЙ НА ОСНОВЕ ПСЕВДОСЛУЧАЙНЫХ И ОДНОРОДНЫХ ПЕРЕСТАНОВОК

А.А. БОРИСКЕВИЧ, А.Ю. ЛАГОЙКО

Известные методы блочного скремблирования речевого сигнала (РС) во временной области не обеспечивают нулевой разборчивости, сохранения ширины спектра и высокой криптостойкости. Для устранения этих недостатков предлагаются два алгоритма скремблирования РС во временной области, основанные на псевдослучайных и однородных перестановках речевых отсчетов, позволяющие управлять соотношением остаточной разборчивости, криптостойкости и времени задержки. Алгоритмы псевдослучайных и однородных перестановок основаны на формировании с использованием секретных ключей криптографических матриц размером, определяемым длительностью кадра, и состоящие из нулей и единиц, позиции последних задают новое расположение отсчета РС в кадре. В случае однородных перестановок на передающей и приемной стороне секретные ключи представляют собой взаимообратные числа по модулю,

равным размеру кадра. Для метода псевдослучайных перестановок множество секретных ключей определяется количеством примитивных полиномов и разрядностью регистра сдвига с линейной обратной связью. Для алгоритмов скремблирования исследована зависимость остаточной разборчивости и времени задержки от длительности кадра, и установлено, что оба алгоритма обеспечивают минимальную алгоритмическую задержку и нулевую разборчивости РС при минимальном размере кадра РС. Определено, что ширина спектра скремблиро-ванного РС не изменяется, а характер спектра приближается к равномерному распределению частотных составляющих с увеличением длительности кадра. Преимущество алгоритма однородных перестановок для решения задач скремблирования состоит в том, что количество возможных секретных ключей увеличивается значительно быстрее с ростом числа отсчетов в кадре, чем для псевдослучайных перестановок, Кроме того, он обеспечивает более высокую временную криптостойкость и минимальное время задержки при минимальном размере кадра РС. Моделирование процесса скремблирования и дескремб-лирования проведено в среде программирования MATLAB.