МЕТОД ШИФРОВАНИЯ РЕЧИ И ДАННЫХ НА ОСНОВЕ РЕКУРСИВНЫХ РАЗВЕРТОК И МУАРОВЫХ КЛЮЧЕЙ

А.А. БОРИСКЕВИЧ, В.Ю. ЦВЕТКОВ

Для современных инфокоммуникационных систем и сетей актуальна проблема унификации алгоритмов обработки и распределения различных видов информации, составляющих мультимедийные данные. Представляют интерес универсальные алгоритмы шифрования, эффективные для защиты всех компонент медиаданных – видео, неподвижных изображений, речи, файлов данных. Ключевым вопросом унификации алгоритмов шифрования является представление защищаемой информации в виде, соответствующем структуре выбираемого криптоалгоритма. Предлагается метод защиты речевых сообщений в сетях с коммутацией пакетов, включающий преобразование одномерного пространства речевого сигнала в двумерное посредством рекурсивных разверток и шифрование полученных речевых 2D образов посредством муаровых ключей. Использование рекурсивных разверток для формирования речевых 2D образов обусловлено возможностью сохранения корреляции речевых отсчетов и применения методов визуальной криптографии для защиты речевых фрагментов. Для шифрования предлагается использовать 2D ключи, сформированные на основе муаровых эффектов. Муаровые ключи могут быть использованы также для защиты файлов данных. Преобразование одномерного представления файлов данных в двухмерное может осуществляться посредством как рекурсивных, так и линейных разверток, ввиду отсутствия пространственной корреляции между информационными единицами. Предлагаемый метод визуальной криптографии на основе муа-

ровых ключей и рекурсивных разверток является эффективным для защиты видео, речевой и документальной конференцсвязи.