ПРОГРАММНЫЙ МОДУЛЬ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В СЕТЯХ ПОДВИЖНОЙ РАДИОСВЯЗИ

А.О. Дударенков, О.Б. Зельманский

Широкое распространение сетей подвижной радиосвязи обуславливает необходимость обеспечения защиты передаваемой по ним информации. В настоящее время шифрование речевой информации осуществляется на основе программных средств, не позволяющих подтвердить отсутствие незадекларированных возможностей и оценить их эффективность. Таким образом, задача защиты речевой информации, передаваемой по сетям радиосвязи, является весьма актуальной.

Предложен программный модуль для передачи зашифрованного речевого сигнала между мобильными устройствами. Данный модуль осуществляет передачу сигнала с минимальными искажениями, что позволяет избежать лавинного эффекта в криптографических преобразованиях. Предлагаемый модуль реализован на базе Sinch API на языке Java. Для тестирования модуля была сформирована база из 150 wav файлов, содержащих речевые сигналы длительностью от 3 до 10 с. В результате сравнительного анализа таких алгоритмов шифрования как AES, RSA, Triple DES, XOR, в качестве наиболее подходящего алгоритма шифрования был выбран алгоритм AES, средняя скорость шифрования и дешифрования которого составила 325 кб/с, а процент блоков, дешифрованных с ошибкой составил 4,738 %.

Разработанный программный модуль применяется совместно с удаленной гарнитурой и ограничением доступа речевого сигнала к встроенному микрофону мобильного устройства путем использования зашумляющего чехла, звуконепроницаемой камеры или его демонтажа.