АЛГОРИТМ ХАОТИЧЕСКОГО ШИФРОВАНИЯ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО КЛЮЧЕЙ

А.А. Борискевич, И.А. Гордеев

Развитие телекоммуникационных и мультимедийных технологий способствует увеличению потоков информации и вызывает необходимость в создании новых алгоритмов защиты информации от несанкционированного доступа. В данной работе предлагается хаотический алгоритм для защиты мультимедийных данных, основанный на поточном их шифровании с использованием хаотических маскирующих последовательностей, обладающих высокой чувствительностью к ключевой информации (начальным значениям хаотической переменной и управляющему параметру).

Из особенностей разработанного алгоритма следует отметить:

– использование одновременно трех хаотических генераторов, работающих практически независимо друг от друга;

– инициализирующие параметры для генераторов берутся из динамического ключа, который изменяется на каждой итерации алгоритма;

– динамический ключ модифицируется зашифрованным байтом изображения, хаотическими отображениями и элементами статического ключа.

В качестве статического ключа используется md5-хеш ключевого слова, вводимого пользователем. Байты (субключи) хеша выступают в роли инициализирующих параметров динамического ключа.

Проверка качества шифрования выполнялась методом оценки межпиксельной корреляции и чувствительности к модификации одного пикселя исходного изображения. Результаты моделирования хаотического алгоритма на 13 тестовых изображений показали гарантированный уровень их защищенности. Установлено, что межпиксельная корреляция между двумя вертикально смежными пикселями, двумя горизонтально смежными пикселями и двумя по диагонали смежными пикселями зашифрованного изображения составляет порядка 10^{-3} и слабо зависит от используемого хаотического отображения.