УДК 003.26

КРИПТОГРАФИЧЕСКИЕ И СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Студенты гр. 113127 Матюшенок И.И., Русакевич К.В.,
старший преподаватель Н.А.Кондратьева
Белорусский национальный технический университет

В настоящее время защита информации является очень важным вопросом во всем мире. Одним из способов его решения является программа, включающая в себя основы криптографии и стеганографии. Конфиденциальная информация шифруется с помощью алгоритма RSA (Rivest, Shamir, Aldeman – изобретатели алгоритма). RSA – это система коллективного пользования, в которой каждый из пользователей имеет свои ключи зашифровывания и расшифровывания данных, причем секретен, только ключ расшифровывания. Для шифрования исходной последовательности необходимо сначала сгенерировать два больших простых числа p и q. Найти $N = p \cdot q$. Выбрать число E (обычно порядка 10000) взаимно простое с $m = (p-1)(q-1)$, т.е. числа E и m не имеют никаких общих делителей, кроме 1. Генерируется число D такое, что $(E \cdot D) \pmod{m} = 1$ – эта запись означает, что $(E \cdot D-1)$ делится на m. Числа N и E публикуются как открытый ключ, а число D держится в секрете – это закрытый ключ. Сообщение зашифровывается по формуле $y = x \cdot E \pmod{N}$, где x – исходное сообщение, а y – зашифрованное.

Полученный шифр проходит операцию архивирования, при этом данному пакету присваивается определенный код.

Третьим этапом является шифрование получившегося пакета в 24-х битную картинку методом наименее значащих битов (НЗБ-метод). Этот метод основан на замене незначащих битов картинки битами информации. В итоге получается изображение с зашифрованным в нем пакетом, визуально не отличающееся от оригинала.

Статистика показывает, что во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем основные причины убытков связаны не столько с недостаточностью средств безопасности как таковых, сколько с отсутствием взаимосвязи между ними, т.е. с нереализованностью системного подхода. Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты.