разработанного алгоритма и широко известного стандарта AES показал практически одинаковые результаты.

Таким образом, предложенное преобразование при своей чрезвычайной простоте обеспечивает достаточную криптоустойчивость с одновременным уменьшением объёма данных.

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ X-КОДА: ТЕОРИЯ И ПРАКТИКА

Е.Н. ЛИВАК, О.Р. МЫСЛИВЕЦ

Изучены и систематизированы способы и механизмы внедрения произвольного кода в исполняемые файлы в формате Portable Executable. Целью исследования является определение применимости методов на практике в недеструктивных целях. Одной из основных проблем внедрения X-кода является работа «зараженного» исполняемого файла совместно с антивирусными средствами.

Проектирование X-кода включает решение следующих основных задач: размещение кода внутри файла-контейнера, перехват управления до начала выполнения основных функций, определение адресов API-функций, необходимых для функционирования файла-контейнера.

Проанализированы и практически проверены механизмы, которые не вызывают изменения адресации ни физического, ни виртуального образов; вызывающие изменения адресации только физического образа; вызывающие изменения адресации как физического, так и виртуального образов, а также механизмы внедрения кода в адресное пространство файла-контейнера косвенным путем.

Полученные в результате исследования выводы и практические рекомендации представлены в докладе.

КОРРЕЛЯЦИОННЫЕ СВОЙСТВА КРИПТОАЛГОРИТМА RIJNDAEL

М.В. МУЗЫЧЕНКО, А.В. МАРТИНОВИЧ, Д.М. БИЛЬДЮК

В системах связи, сбора и передачи информации широкое распространение получили методы расширения спектра сигналов. Одним из эффективных методов расширения спектра, при котором сигнал-переносчик информации занимает широкую полосу частот, является метод непосредственной модуляции несущей псевдослучайной последовательностью. При этом методе расширение спектра дополнительная модуляция несущей сигнала никак не связана с передаваемой информацией.

В данной работе были исследованы корреляционные свойства: М-последовательности, ЧКП, коды Касами, криптоалгоритм Rijndael.

Самая лучшая апериодическая АКФ найдена у М-последовательности, а периодическая АКФ — у ЧКП (в районе порога нет шума).

В процессе исследования было выяснено, что криптоалгоритм Rijndael совпадает с корреляционными функциями по боковым лепесткам по случайным последовательностям. Хоть Rijndael и имеет большой недостаток — высокий уровень боковых лепестков, но он имеет большие преимущества, которые не имеют другие последовательности. А именно: за счет криптографических свойств у него произвольная длина, обладает высокой структурной скрытностью.