# ОПРЕДЕЛЕНИЕ КАЧЕСТВЕННЫХ ХАРАКТЕРИСТИК ПСЕВДОСЛУЧАЙНОЙ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ, ПОЛУЧЕННОЙ С ПОМОЩЬЮ СРНОС

**Караман Д. Г.**

***Национальный технический университет «Харьковский политехнический институт» г. Харьков***

Для непрерывной генерации ключа в потоковых криптографических шифрах традиционно находят применение генераторы псевдослучайных последовательностей, получаемых с помощью объединения выходных последовательностей нескольких регистров с линейной обратной связью (СРЛОС) с помощью некоторой нелинейной функции. В работе Т. Сигенталера показано, что число попыток взлома таких систем шифрования может быть существенно сокращено в результате применения корреляционных методов анализа генерируемой последовательности. Действенность такого анализа подтверждается сравнением результатов компьютерного моделирования и теоретических исследований. В ряде работ показано, что раскрытие шифров, организованных по описанной схеме, является вычислительно выполнимым с помощью атаки на базе известного открытого текста размером всего лишь 15 символов. Для проведения атаки, основанной лишь на закрытом тексте, число необходимых символов определяется посредством корреляционной атаки. Проведенный ранее анализ позволяет заключить, что выходная последовательность псевдослучайного генератора, а, соответственно, и последовательности, генерируемые СРЛОС, должны обладать высокими статистическими качественными характеристиками и удовлетворять наиболее жестким требованиям. Кроме этого, высокая подверженность корреляционной атаке ограничивает выбор нелинейной объединяющей функции.

Для получения более качественной псевдослучайной битовой последовательности в работе предложено использование сдвиговых регистров с нелинейной обратной связью (СРНОС). Проход по полному набору всех возможных состояний в автоматной модели такого регистра (гамильтонову циклу) обеспечивает равновероятное появление логического 0 и 1 на его выходе, в отличие от СРЛОС, в цикле переходов которого исключено нулевое состояние. Для определения качественных характеристик случайности последовательности, генерируемой СРНОС, использованы специализированные наборы статистических тестов DIEHARD и NIST STS, которые применяются при оценке качества криптографических систем.