ТЕСТИРОВАНИЕ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

Рисованый А.Н.

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

Тестирование псевдослучайных последовательностей – это совокупность методов определения меры близости заданной псевдослучайной последовательности к случайной. В качестве такой меры обычно выступает наличие равномерного распределения, большого периода, равной частоты появления одинаковых подстрок и т. п.

Генераторы случайных и псевдослучайных последовательностей являются основными криптографическими примитивами и находят самое широкое приложение в разных системах безопасности.

Актуальность работы состоит в том, что от качества генерируемой последовательности зависит безопасность криптографической системы.

В работе разработана математическая модель криптографической системы на основе регистра сдвига с нелинейными обратными связями с учетом многих параметров. На основе полученной многокритериальной модели получены последовательности, проверены теоретические разработки и сравнены с практическими результатами. Полученные результаты подтвердили работоспособность предложенной модели.

Кроме того, в работе исследованы псевдослучайные последовательности, полученные с регистра сдвига с нелинейными обратными связями на основе тестов:

- гистограмма распределения элементов на плоскости;
- распределение на плоскости;
- проверка серий;
- проверка на монотонность;
- автокорреляционная функция;
- профиль линейной сложности;
- графический спектральный тест.

По результатам каждого теста получены графические представления исследуемых последовательностей, сделаны выводы, не противоречащие теоретическим исследованиям.

В работе определены задачи дальнейших исследований и пути получения предполагаемых новых результатов.