ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ НЕЛИНЕЙНЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Рысованый А.Н., Зыков Д.В., Хмеленко Д.Ю.
Национальный технический университет "Харьковский политехнический институт ", г. Харьков

В большинстве алгоритмов шифрования, особенно потоковых шифрах, используются генераторы ключевой последовательности. Генератор ключевой последовательности выдает поток битов, который выглядит случайными, но в действительности является детерминированным и может быть в точности воспроизведен на стороне получателя. Чем больше генерируемый поток похож на случайный, тем больше времени потребуется криптоаналитику для взлома шифра. Лучшими свойствами обладают нелинейные генераторы псевдослучайных чисел (НГПСЧ), в которых производится преобразование в цепях обратных связей регистра сдвига.

Поэтому актуальной научной задачей является создание программного комплекса, позволяющего проводить полнофункциональное статистическое исследование ПСП, в том числе проводить испытания на всех существующих графических и оценочных тестах, оценивать корреляцию между различными выборками последовательности и др.

В работе:

– рассматриваются многочлены над конечным полем;

– рассматриваются типы генераторов последовательности;

– построена модель НГПСЧ и предъявлены требования;

– сформулированы требования, предъявляемые к НГПСЧ ответственного назначения;

– разработана классификация существующих алгоритмов генерации НГПСЧ;

– проведен анализ существующих методов анализа непредсказуемости НГПСЧ;

– сформулированы требования, предъявляемые к системе оценки качества НГПСЧ, и проведен анализ существующих систем аналогичного назначения;

– рассмотрены свойства рекуррентных последовательностей не максимальной длины.

– рассмотрены вопросы разложения многочленов на различные множители и проанализированы их свойства