УДК 681.326.7

ГЕНЕРИРОВАНИЕ РАВНОВЕРОЯТНОСТНЫХ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА РЕГИСТРАХ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ

***Д.Г. ВОЛОШИН*[1], *А.В. ЛОГВИНОВА*[1], *А.Н. РЫСОВАНЫЙ*[2*]**

[1] *магистрант кафедры вычислительной техники и программирования, НТУ «ХПИ», Харьков, УКРАИНА*

[2] *доцент кафедры вычислительной техники и программирования, канд. техн. наук, НТУ «ХПИ», Харьков, УКРАИНА*

[*] *email: rysov@rambler.ru*

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

Сложность средств цифровой техники давно уже привела к усложнению проверки их работоспособности. При тестировании схемы наилучшие результаты достигаются при помощи средств встроенного самотестирования, в связи с тем, что обнаруживаются как статические (константные), так и динамические неисправности. Основным элементом любой системы встроенного самотестирования является источник тестовых воздействий. В основном в качестве тестовых воздействий применяют псевдослучайные последовательности максимальной длины или *M*-последовательности (так как в этом случае упрощается схема). В качестве генератора *M*-последовательности используется, как правило, линейный сдвиговый регистр с сумматорами по модулю два в цепи обратной связи. Но для увеличения длины последовательности целесообразнее применять нелинейные обратные связи.

В работе рассмотрены общие свойства псевдослучайных последовательностей; особенности рабочего режима формирования *M*-последовательности; рассмотрена нормированная периодическая автокорреляционная функция. Анализ ГПСП с использованием производящей функции дал возможность связать циклические свойства неоднородных рекуррентных последовательностей m-го порядка с соответствующими свойствами однородных рекуррентных последовательностей $(m + 1)$-го порядка. Рассмотрены некоторые характерные троичные рекуррентные последовательности и их статистические свойства. 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. По результатам каждого теста получены графические представления исследуемых последовательностей, сделаны выводы, не противоречащие теоретическим исследованиям.