П. В. Гаврилик, Д. В. Ратобыльская
(ГГУ им. Ф. Скорины, Гомель)

РАЗРАБОТКА СИСТЕМЫ ТЕСТОВ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Случайные числа широко используются в современных информационных технологиях. К областям, где их применение играет ключевую роль, относятся имитационное моделирование и криптография.

Генератор псевдослучайных чисел (ГПСЧ) – алгоритм, порождающий последовательность чисел, элементы которой почти независимы друг от друга и подчиняются заданному распределению. Качественный генератор псевдослучайной последовательности (ГПСП), ориентированный на использование в системах защиты информации, должен иметь: высокую криптографическую стойкость; хорошие статистические свойства; большой период формируемой последовательности; эффективную аппаратную и программную реализацию; высокое быстродействие[1].

В 1999 году разработчиками Национального института стандартизации и технологий США был представлен статистический набор тестов НИСТ и предложена методика проведения статистического тестирования шифров и ГПСЧ [2]. Опираясь на требования к генераторам для систем защиты информации, а также данные методики и предлагаемые НИСТ тесты, составлена система тестов ГПСП.

Для апробации системы тестов, были реализованы и протестированы пять ГПСП: линейный конгруэнтный генератор, квадратичный конгруэнтный генератор, генератор RSA, линейный сдвиговый регистр, самоуправляемый 2-линейный регистр сдвига.

С помощью методов статистического тестирования, проводилась проверка генераторов по следующим критериям: близость к равномерному распределению (тест n-серий); случайность и независимость (тест критерий серий), сжимаемость последовательности (тест Маурера),

эффективная аппаратная реализация; максимально возможная длина последовательности.

Анализируя результаты тестирования, в качестве наилучшего по заданным характеристикам был выбран ГПСП на основе линейного сдвигового регистра. Предложенная система тестов позволила подобрать оптимальные параметры моделирования для выбранного генератора.