С. В. Кривенков, С. И. Седлер, К. Н. Щура,
Д. И. Гавриловец, Е. Л. Заботин
(БелГУТ, Гомель)

МЕТОДИКА ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Программные генераторы псевдослучайных последовательностей (ПСП) перед использованием в криптологии и моделировании должны быть протестированы по ряду критериев. Существует несколько стандартных наборов тестов: «Diehard» Дж. Марсальи, Д. Кнута, NIST STS 800-22, FIPS 140-2 [2], а также отдельные статистические тесты, среди которых имеются и отечественные [3, 4].

Однако реализация и использование каждой из указанных совокупностей тестов имеет некоторые недостатки, среди которых основные: каждый критерий отыскивает лишь отдельные закономерности в тестируемой числовой последовательности; мощность статистических критериев неизвестна.

Отдельная пока мало изученная проблема – совместное тестирование нескольких генераторов ПСП используемых, например, для имитационного моделирования систем массового обслуживания [1] – разработанных статистических тестов в данной области недостаточно.

В работе предлагается методика тестирования генераторов ПСП, включающая следующие положения.

1. При тестировании генераторов ПСП необходимо использовать как можно большее множество известных статистических критериев, чтобы отслеживать все возможные закономерности.

2. Генератор можно использовать, если ни один из критериев не забракует его для уровня значимости 0,015–0,005. Данное значение обусловлено количеством известных авторам статистических критериев: 60–70. Увеличение уровня значимости до 0,02 приведет к тому, что в среднем каждый 50-ый тест будет браковать «истинно случайную» последовательность. А уменьшение уровня значимости ниже 0,005 приведет к отказу от браковки «весьма подозрительных» ПСП.

3. Тестирование генераторов должно проводиться на ПСП одинаковой длины.

4. За прохождение каждого теста генератору ПСП назначают «балл», характеризующий качество генератора по данному критерию. Для статистических критериев таким баллом может быть значение $P\text{-value} \in [0, 1]$, характеризующее вероятность того, что «ПСП неслучайна».

5. Каждому тесту назначают «значимость» – важность для той или иной предметной области. Например, в криптологии наиболее высоки требования к криптостойкости генератора, а в имитационном моделировании – к совпадению моментов и равномерности ПСП.

6. Выбор генератора ПСП для использования в той или иной области определяется суммой баллов, набранных по различным тестам, нормированных их значимостью для данной предметной области.

Многие статистические тесты критичны к длине ПСП и начинают обнаруживать статистически значимые закономерности, которые не обнаруживались на меньших длинах. Так, например, знаковый ранговый критерий (signed rank test) бракует такие достаточно известные и качественные генераторы, как Блюма-Блюма-Шуба (BBS), Шамира (RSA), «Marsaglia Multicarry» и «Xorshift» Дж. Марсальи, а также вихрь Мерсенна (MT19937) уже на 1,5-2 тысячах элементах ПСП. Предлагаемая система баллов поможет в выборе лучшего из доступных генераторов ПСП, если формально каждый из них будет забракован одним или несколькими статистическими критериями.

7. При совместном использовании нескольких генераторов ПСП необходимо дополнительное тестирование с определением взаимной корреляционной функции и других характеристик, список которых на данный момент не разработан.

Для реализации предлагаемого подхода авторами разрабатывается программный комплекс тестирования генераторов ПСП, который будет включать в себя все известные статистические и эвристические тесты. Комплекс базируется на MS Excel, что обусловлено наличием большого количества встроенных математических и статистических функций, возможностью программирования на VBA, наглядностью реализации и тестирования программ, созданных несколькими авторами.

Литература

1. Алиев, Т.И. Проблема сочетания генераторов псевдослучайных величин в GPSS-моделях / Т.И. Алиев, Г.К. Асафьев // Пятая всероссийская научно-практическая конференция по имитационному моделированию и его применению в науке и промышленности «Имитационное моделирование. Теория и практика (ИММОД-2011)». – СПб. – 2011. – т.1 – С. 95–100.

2. Иванов, М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : КУДИЦ-ОБРАЗ, 2003. – 240 с.

3. Кобзарь, А.И. Прикладная математическая статистика: для инженеров и научных работников / А.И. Кобзарь. – М.: Физматлит, 2006. – 813 с.

4. Харин, Ю.С. Проверка гипотез о независимости и равномерном вероятностном распределении элементов случайной последовательности / Ю.С. Харин, А.И. Петлицкий // Вестник БГУ. Сер. 1. 2007. № 3. – С. 74–80.