КОНСТРУКЦИЯ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ, ПОРОЖДАЮЩЕГО НОРМАЛЬНЫЕ (ПО БОРЕЛЮ) ПОСЛЕДОВАТЕЛЬНОСТИ

АВТОР: д.т.н. Рябко Б.Я.

Генераторы псевдослучайных чисел (ГПСЧ) находят широкое применение в криптографических системах защиты информации, в численных методах и многих других разделах информатики, и к настоящему время разработаны национальные и международные стандарты для ГПСЧ и тестов для их проверки. Разработкой и изучением ГПСЧ и тестов заняты десятки исследователей как у нас в стране, так и за рубежом, и важная часть этих исследователей – проверка «качества» ГПСЧ при которой порождаемые ГПСЧ бинарные последовательности проверяются наборами («батареями») известных статистических тестов, предназначенных для обнаружения отклонений от распределения Бернулли с параметрами (0.5 , 0.5). Если какой-либо тест обнаруживает такие отклонения, то данный генератор «бракуется», то есть не рекомендуется для практического использования. Важно отметить, что «надежность» практически всех используемых генераторов базируется только на их экспериментальной проверке, а не математическом доказательстве их свойств.

Автором предложена конструкция ГПСЧ, для которого доказано, что порождаемые им последовательности из нулей и единиц являются нормальными по Борелю. (По определению, бинарная последовательность нормальна по Борелю, если каждое двоичное слово U встречается в этой последовательности с предельной частотой $\frac{1}{2}^{|U|}$, где |U| длина U. Например, частота встречаемости 01 равна ¼, 0110 – $^1/_{16}$ и т.д.). Важно отметить, что для Бернуллиевской последовательности это свойство выполняется (с вероятностью 1). Данный ГПСЧ был реализован в виде программы (совместно с выпускником магистратуры ММФ НГУ В.Журавлевым) и проверен всеми известными батареями статистических тестов, которые ГПСЧ успешно выдержал.

ПУБЛИКАЦИИ

1. *Ryabko B.* A Pseudo-Random Generator Whose Output is a Normal Sequence // International Journal of Foundations of Computer Science. - 2021.
2. *Ryabko B., Zhuravlev V.* Construction of a pseudo-random number generator whose output is a normal sequence. 2021 XVII International Symposium" Problems of Redundancy in Information and Control Systems"(REDUNDANCY), pp. 1-4.
3. *Ryabko B., Fionov A.* Cryptography in the Information Society. - Singapore: World Scientific Publishing, - 2021. - 280 p. - ISBN 978-981-122-615-1.