ISSN 2222-2944. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я. 2023

АНАЛІЗ ТА ТЕСТУВАННЯ ГЕНЕРАТОРІВ ВИПАДКОВИХ І ПСЕВДОВИПАДКОВИХ ЧИСЕЛ З ВИКОРИСТАННЯМ НАБОРУ СТАТИСТИЧНИХ ТЕСТІВ NIST STS

Некрасова М.В., Гнатенко В.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Випадкові числа відіграють важливу роль у багатьох галузях науки й техніки. Наприклад, вони використовуються у сфері кібербезпеки для створення безпечних систем шифрування, в статистиці для проведення експериментів і аналізу даних, в ігрових технологіях для створення випадкових подій і сценаріїв і т. д.

Але, на жаль, генерація випадкових чисел є складним завданням, і іноді згенеровані випадкові числа можуть мати не неочікуваний результат та бути недостатньо "випадковими". Це може призвести до вразливості в системах, де вони використовуються, і до невірних результатів у статистичних дослідженнях.

Отже, постійно виникає потреба у нових та надійних методах генерації випадкових чисел. Однак, якість генерованих чисел може відрізнятись в залежності від алгоритму їх генерації. Тому важливо мати єдиний уніфікований та надійний підхід для оцінки якості генераторові випадкових чисел.

NIST Statistical Test Suite (Набір статистичних тестів Національного інституту стандартів і технологій) — це набір статистичних тестів, розроблений Національним інститутом стандартів і технологій США для оцінки властивостей генераторів випадкових чисел. NIST STS, розроблені з метою визначення відповідності послідовності бітів (наприклад, послідовності, що представляються як випадкові числа) певним математичним моделям.

Вона включає 15 тестів, які можуть використовуватися для аналізу як псевдовипадкових, так і випадкових послідовностей. Наприклад, деякі тести перевіряють, чи має послідовність бітів рівномірний розподіл, тоді як інші перевіряють, чи існує кореляція між попередніми та наступними бітами у послідовності. Для проведення тестування за допомогою NIST Statistical Test Suite необхідно ввести послідовність випадкових чисел у програму, яка виконує тести та повертає результати. Результати тестування представлені у вигляді числових значень, які характеризують якість генератора випадкових чисел.

У дослідженні проаналізовано основні принципи генерації випадкових чисел, проводиться їх тестування за системою NIST STS та виявлено проблеми, пов'язані з використанням псевдовипадкових чисел з недостатньою ентропією.

Література:

1. Irvine, Cynthia, Matthew Rose, and Naomi Falby, editors. Practical and Experimental Approaches to Information Security Education. Naval Postgraduate School, 2006.
2. Zaman, J K M Sadique Uz, and Ranjan Ghosh. "A Review Study of NIST Statistical Test Suite: Development of an Indigenous Computer Package." arXiv.org, Cornell University Library, 28 Aug. 2012