УДК 004.3, 004.421.5, 004.056.5

Остапець Д.О., к.т.н., доцент
Русакевич С.Р. , здобувач
Український державний університет науки і технологій

ОГЛЯД І АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ГЕНЕРАЦІЇ ВИПАДКОВИХ ЧИСЕЛ

Випадкові числа застосовуються в безлічі сфер – криптографії, комп'ютерному моделюванні, аналізі, статистичних вибірках, фізиці, інженерії, медицині та ін. Ці способи використання мають різні рівні вимог до ступеня випадковості чисел.

Існують дві принципово різні стратегії генерації випадкових бітів. Одна стратегія полягає у недетермінованому створенні бітів, де кожен біт виводу базується на фізичному процесі, який є непередбачуваним. Генератори чисел, побудовані на цій концепції називаються генераторами випадкових чисел (ГПЧ), а створені за допомогою нього числа – істино випадковими. Інша стратегія полягає у детермінованому обчисленні бітів за допомогою алгоритму перетворення певного початкового значення (зерна). Такий генератор має назву генератор псевдовипадкових чисел (ГПВЧ). Початкове значення, що використовується для ініціалізації ГПВЧ, повинно містити достатню ентропію, щоб забезпечити гарантію випадковості. Якщо початкове значення було підібрано вірно, а алгоритм добре розроблений, біти, що виводяться ГПВЧ, будуть непередбачуваними на рівні ГВЧ [1].

Безпека багатьох параметрів криптографічних систем (таких як криптографічні ключі, вектори ініціалізації, нонси) залежить від наявності надійних випадкових чисел. Використання джерел ентропії в ГВЧ є фундаментальною вимогою для забезпечення криптографічної стійкості системи. Недостатня випадковість чисел може призвести до передбачуваності ключів, створених для шифрування інформації, що в свою чергу значно знижує надійність захисту інформації.

Джерела ентропії зазвичай поділяють на дві категорії:

- Природні (фізичні) джерела ентропії;
- Програмно-апаратні джерела ентропії.

Багато природних явищ генерують статистично випадкові сигнали шуму – тепловий та дробовий шум, фотоелектричний ефект, броунівський рух, атмосферний шум та ядерний розпад [2]. Тепловий шум виникає внаслідок хаотичного теплового руху носіїв заряду в провідниках, тоді як дробовий шум є наслідком дискретної природи електричного заряду. Фотоелектричний ефект та ядерний розпад

забезпечують особливо високу якість випадковості, оскільки ґрунтуються на квантових феноменах, які є принципово непередбачуваними навіть теоретично. Всі ці джерела є надійними та добре дослідженими, проте для їх практичного використання в ГВЧ необхідне спеціалізоване апаратне забезпечення – аналого-цифрові перетворювачі, підсилювачі шуму або детектори випромінювання, – що здатне зафіксувати фізичний процес і перетворити його на послідовність бітів, придатну для використання в якості зерна ГВЧ.

Програмно-апаратні джерела шуму натомість використовують системні дані для генерації випадковості, не потребуючи спеціалізованого фізичного обладнання. Прикладами таких джерел можуть бути: стан оперативної пам'яті, часові мітки переривань, рухи комп'ютерної миші, натискання клавіш, мережеві події, завантаженість процесора, а також дані API операційної системи [3]. В якості джерела ентропії можна взяти й дані з акселерометра, гіроскопа та магнітометра [4]. Використання таких джерел є значно простішим в реалізації, оскільки вимагає лише програмного забезпечення, здатного обробити надані системою дані і перетворити їх в послідовність бітів. Недоліком даного типу джерел є їх залежність від активності користувача або стану системи, однак цей недолік можна усунути комбінацією декількох джерел для генерації потоку бітів.

Список використаних джерел

1. Barker E., Kelsey J. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. NIST SP 800-90A Rev. 1. URL: http://dx.doi.org/10.6028/NIST.SP.800-90Ar1

2. D. Ostapets, V. Dziuba, P. Ivin, Hardware random numbers generator based on microcontroller. *MATEC Web of Conferences 390*, 04002. 2024. URL: https://doi.org/10.1051/matecconf/202439004002

3. Turan M. S., Barker E., Kelsey J., McKay K. A., Baish M. L., Boyle M. Recommendation for the Entropy Sources Used for Random Bit Generation. NIST SP 800-90B. URL: https://doi.org/10.6028/NIST.SP.800-90B

4. Остапець Д., Опрятний А. Дослідження можливості використання окремих датчиків мобільних пристроїв у якості джерела ентропії генератора випадкових чисел. *Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах»*. 2025. 82(2). С. 88–92. URL: https://doi.org/10.31891/2219-9365-2025-82-12