Дрига Артем Вадимович
Національного університету «Одеська юридична академія»,
студент 1-го курсу факультету кібербезпеки
та інформаційних технологій

АКТУАЛЬНІСТЬ РОЗРОБКИ КРИПТОСТІЙКИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Нині випадкові числа використовуються в ІТ-розробках різної спрямованості. Послідовності випадкових та псевдовипадкових чисел широко застосовують при реалізації моделювання складних систем та об'єктів, у задачах чисельного аналізу, при розробленні комп'ютерних ігор, в онлайн-сервісах для створення різних паролів, генеруванні електронних підписів для електронного документообігу тощо. Крім того, псевдовипадкові випадкові числа (ПВЧ) і відповідно генератори псевдовипадкових чисел (ГПВЧ) використовуються в задачах захисту даних від несанкціонованого доступу в системах криптографії та інформаційної безпеки: при тестуванні ефективності алгоритмів шифрування, генеруванні унікальних ідентифікаторів, контролі цілісності даних, хешуванні даних, породженні синхронних потокових шифрів і потокових шифрів, що самосинхронізуються, формуванні сигналів, які забезпечують приховану передачу даних, та інших задачах. Саме тому можна стверджувати, що від якості та ефективності методів формування випадкових та псевдовипадкових послідовностей, специфіки відповідних генераторів таких чисел залежать характеристики криптографічних підсистем систем безпеки, позаяк при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому є вразливою.

Генератори псевдовипадкових послідовностей (ГПВЧ), відповідно до стандарту NIST Special Publication 800–90A, можуть бути засновані на використанні функцій хешування, які є необоротними або односторонніми функціями перетворень [1]. Детерміновані алгоритми ГПВЧ генерують майже незалежні один від одного і числа, які підкоряються заданому

розподілу (зазвичай рівномірному) [2]. У такому алгоритмічному (програмному) генераторі задають початкові значення, на базі яких і створюються псевдовипадкові послідовності. Очевидно, що здобута внаслідок таких операцій послідовність не є повною мірою випадковою, оскільки визначається формулою і початковим числом. Хоча для більшості прикладних задач такі ПВЧ цілком прийнятні, проте вони мають свої недоліки. ГПВЧ можна вважати ненадійним, якщо він має:

– надто короткий період генерації послідовності;

– члени послідовності, які недостатньо непередбачувані та незалежні від попередніх.

Щоб ГПВЧ вважався надійним, його алгоритм повинен:

– генерувати послідовність чисел, які мають бути максимально незалежними один від одного та непередбачуваними;

– мати можливість відтворити раніше створену послідовність чисел;

– витрачати тільки ту частину пам'яті комп'ютера, яка необхідна для вирішення поставленої мети.

Суттєвою перевагою програмних ГПВП є «нульова» собівартість, позаяк у вільному доступі є численні бібліотеки для різного програмного оточення.

На відміну від алгоритмічного ГПВЧ, апаратні (фізичні) генератори формують істинно випадкові числа на основі опрацювання вимірюваних, хаотично змінюваних параметрів при протіканні певних фізичних явищ (різного роду шумів, фотоелектричних фотоефектів, квантових явищ тощо) [4]. Попри те, що послідовності, створені цим генератором, можна вважати цілковито випадковими, вони мають низку недоліків, з-посеред яких головними є складність реалізації (такі генератори зазвичай є окремими пристроями) та повільна швидкість їхньої роботи (кількість згенерованих чисел в секунду), у порівнянні з програмним ГПВЧ. Також апаратні генератори залежать від протікання фізичних явищ – при затуханні, генератор деградуватиме. Саме тому їх треба тестувати на статистичну випадковість перед кожним використанням.

Сучасні тенденції побудови таких генераторів використовують різні квантові процеси для генерації випадкових чисел, опису їх імовірнісних схем з позицій квантової фізики. Найбільш відмітною характеристикою квантового ГВЧ є науковий доказ випадковості його вихідних послідовностей, що є гарним рішенням для криптографії та інших сфер застосування, де критично важливою є якість випадкових послідовностей. Проте суттєвим недоліком квантового підходу у пошуку рішень ГВЧ є необхідність застосування доволі габаритних фізичних рішень без можливості їх мініатюризації до рівня застосування сучасних технологій виробництва мікросхем [5].

Проблема створення швидкого, ефективного ГПВЧ, позбавленого традиційних недоліків, є доволі складною, проте актуальною задачею, адже від якості роботи ГПВЧ залежить точність результатів. Наприклад, генерація ключів безпеки, методи шифрування та дешифрування – все це опосередковано залежить від якості та надійності роботи ГПВЧ. Позаяк безпека криптосистеми зосереджена на ключі, то при використанні ненадійного процесу генерації ключів, вся криптосистема в цілому стає вразливою. Перспективним напрямом досліджень є розроблення ГПВЧ, які генеруватимуть послідовності випадкових чисел, максимально наближені до дійсно випадкових послідовностей.

Список використаних джерел:

1. NIST Special Publication 800–90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. 2012. URL: http://csrc.nist.gov/ publica-tions/nistpubs/800–90A/SP800–90A.pdf. (дата звернення: 01.11.2020).

2. Методы генерации случайных чисел / В. С. Гончарук, Ю. С. Атаманов, С. Н. Гордеев. *Молодой ученый.* 2017. № 8(142). С. 20–23. URL: https://moluch.ru/archive/142/40025/ (дата обращения: 01.11.2020).

3. Слеповичев И. И. Генераторы псевдослучайных чисел: учебн. пособие. 2017. Саратов: СГУ, 2017. 118 с.

4. Bardis N.G., Markovskyi A. P., Doukas N., Karadimas N. V. True Random Number Generation Based on Environmental Noise Measurements for Military Applications. *Proceedings of the 8th WSEAS International Conference on Signal Processing, Robotics, and Automation*. 2009. P. 68–73.

5. Гріненко Т.О., Нарєжній О. П. Квантові генератори випадкових чисел в криптографії. *Системи обробки інформації*. 2015. Вип. 10(135). С. 86–89.

Ключові слова: послідовності псевдовипадкових чисел, генератор псевдовипадкових чисел.

Ключевые слова: последовательности псевдослучайных чисел, генератор псевдослучайных чисел.

Keywords: sequences of pseudorandom numbers, pseudorandom number generator

***Науковий керівник**: к.т.н., доц. Трофименко О. Г.*

Дроздов Богдан Михайлович
Національний університет «Одеська юридична академія»,
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

СИСТЕМА ІДЕНТИФІКАЦІЇ З ЕЛЕМЕНТАМИ КОНТРОЛЮ ДОСТУПУ ДО ПРИМІЩЕННЯ

Охорона всякого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках значущим кордоном буде система управління контролю доступом (СУКД) на об'єкт.

Якісно організована із застосуванням новітніх технічних засобів СУКД дозволить вирішувати цілий ряд завдань. До числа особливо головним можна віднести наступні:

- протидія індустріального шпигунства;
- протидія розкраданню;
- протидія саботажу;