УДК 681.3
© В. Максимович[1], Р. Смук[1], Ю. Сторонський[1], Ю. Костів[1], 2014

ДВІЙКОВО-ДЕСЯТКОВИЙ ГЕНЕРАТОР ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОТОКІВ

В роботі запропоновано структурну схему генератора псевдовипадкових імпульсних послідовностей на основі модифікованого генератора Фібоначчі, що може використовуватись для формування псевдовипадкової бітової послідовності і керованої по частоті пуасанівської імпульсної послідовності. Досліджені їхні статистичні характеристики Генератор може використовуватись, зокрема, для імітації вихідних сигналів дозиметричних детекторів.

The structural scheme of pseudorandom pulse sequences generator on the base of modified Fibonacci generators that can be used for formation of pseudorandom bit sequence and Poisson pulse sequence, which frequency can changed, are representing in the work. Their statistic characteristics are investigated. The generator can be used, in particular, for imitation of dosimetric detectors output signals.

1. ВСТУП

Генератори пуасонівських імпульсних потоків (ГПІП) використовуються, зокрема, для імітації вихідних сигналів дозиметричних детекторів (ДД) при проектуванні і попередніх випробовуваннях дозиметричних пристроїв [1]

В роботі [2] були запропоновані і досліджені ГПІП на основі модифікованих генераторів Фібоначі (МГФ). Розроблені генератори можуть використовуватись для формування керованого по частоті пуассонівського імпульсного потоку і бітової псевдовипадкової імпульсної послідовності. Таким чином, генератори можуть використовуватись як у вимірювальній техніці для імітації випадкових сигналів, так і для криптографічних перетворень. Однак, структурні елементи цих ГПІП працюють у двійковому коді, що створює певні незручності при їх використанні в дозиметрії.

[1] Національний університет “Львівська політехніка”

2. СТРУКТУРНА СХЕМА ГЕНЕРАТОРА

В даній роботі досліджений один з варіантів побудови ГПІП на основі МГФ, при функціонуванні його структурних елементів в двійково-десятковій системі числення. Відповідна структурна схема наведена на рис. 1.

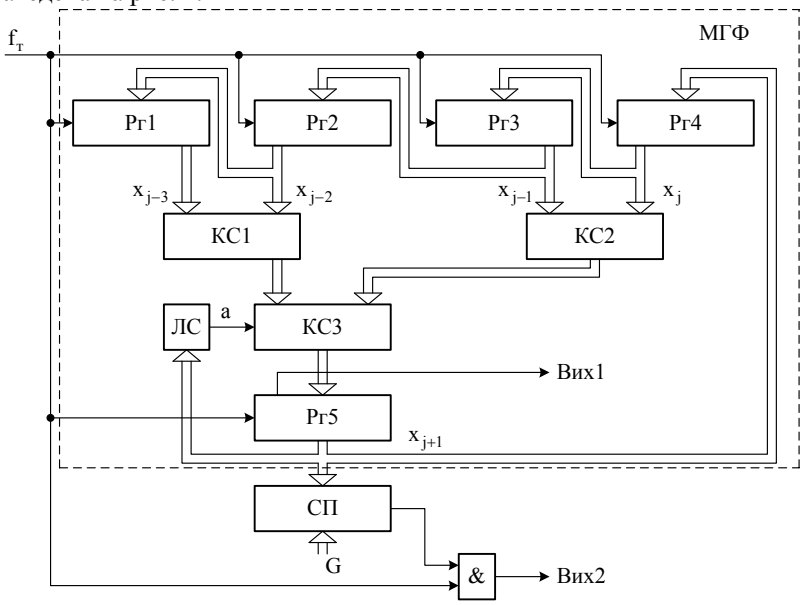


Рис. 1. Структурна схема ГПІП на основі МГФ

Власне МГФ складається з регістрів Рг1 - Рг5, комбінаційних суматорів КС1 – КС3, що працюють в двійково-десятковій системі числення і логічної схеми ЛС. Схема порівняння СП, яка також працює у двійково-десятковому коді, і логічний елемент І забезпечують формування імпульсного потоку з пуассонівським законом розподілу (Вих. 2).

На виході МГФ, тобто на виході Рг5, формується послідовність псевдовипадкових чисел у відповідності до виразу:

$$x_{j+1} = (x_j + x_{j-1} + x_{j-2} + x_{j-3} + a) \bmod m, \qquad (1)$$

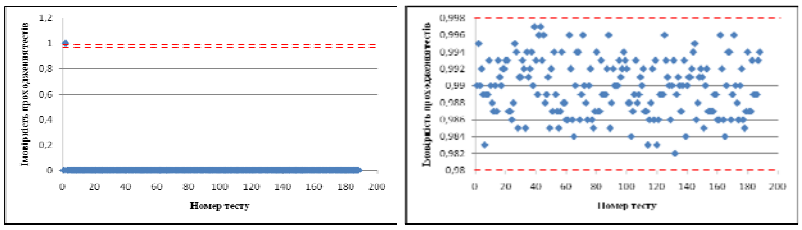
де x_j, x_{j-1}, x_{j-2}, x_{j-3} – числа в регістрах Рг4, Рг3, Рг2, Рг1 відповідно, $m = 10^q$, q – кількість декад структурних елементів схеми. Значення змінної а визначається логічним рівнянням

$$a = a_0 \text{ xor } a_1 \text{ xor } a_2 \text{ xor } \cdots \text{ xor } a_z, \qquad (2)$$

де a_i (i=0,1,…,z) – значення розрядів двійково-десяткового числа в Рг5. Кількість членів рівняння (2) може вибиратись з діапазону $0 \ldots 4 \cdot q$.

3. ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК БІТОВОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ (ВИХІД 1)

Псевдовипадкова бітова імпульсна послідовність формується на виході молодшого розряду регістру Рг5 (Вих. 1). Введення в склад генератора Фібоначі логічної схеми ЛС зумовлено необхідністю покращення статистичних характеристик цієї послідовності при апаратній реалізації генератора [2]. На рис. 2 наведено статистичні портрети імпульсної послідовності на Вих. 1 при відсутності (рис. 2а) і наявності ЛС (рис. 2б), що отримані з використанням тестів NIST [3]. При цьому були зафіксовано, що структурні елементи генератора містять 9 декад ($q = 9$, $m = 10^9$), а кількість аргументів логічного рівняння (2) дорівнює 30 ($z = 29$). На рис. 2 пунктирними лініями показані межі, в яких повинні знаходитись імовірності проходження тестів, для визнання імпульсної послідовності такою, що відповідає умовам випадковості. Отже, при наявності ЛС вихідна бітова послідовність відповідає установленим вимогам і розроблений генератор може використовуватись, зокрема, в криптографічних перетвореннях.



а *б*

Рис. 2. Статистичні портрети бітової послідовності (Вих. 1)

4. ДОСЛІДЖЕННЯ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК КЕРОВАНОЇ ПУАССОНІВСЬКОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ (ВИХІД 2)

Середня частота імпульсів на виході ГПІП (Вих. 2) визначається рівнянням

$$f_{вих} = \frac{G}{10^q} f_т, \qquad (3)$$

де G – керуючий код, $f_т$ – частота тактових імпульсів.

Результати дослідження статистичних характеристик ГПІП на базі МГФ, зафіксовані при $m = 10^9$, наведені на рис. 3. Дослідження проводились з допомогою узагальненої методики дослідження параметрів вихідного сигналу ГПІП на відповідність пуассонівському закону розподілу з використанням критерію Пірсона [4].

У відповідності до запропонованої методики потік вхідних імпульсів ГПІП розділяється на n однакових груп, кожна з яких складається з i_{max} імпульсів. Максимальну кількість груп – n_{max}. Групам вхідних імпульсів відповідають групи вихідних імпульсів з числом імпульсів k_1, k_2, …, $k_{n_{max}}$. Запропонована методика грунтується на класичній методиці перевірки гіпотези про розподіл генеральної сукупності за законом Пуассона з використанням критерію Пірсона (критерію χ^2) [5]. При цьому, враховуючи специфіку побудови ГПІП, були запропоновані наступні доповнення:

– фіксується номінальне (теоретичне) середнє значення чисел k_1, k_2 … $k_{n_{max}}$ – k_c, незалежно від значення керуючого коду G;

– значення i_{max} є змінним, залежить від значення G і визначається рівнянням

$$i_{max} = \frac{X_{max}}{G} k_c, \qquad (4)$$

де X_{max} – максимально можливе значення числа на виході регістра Рг5. У випадку, що розглядається $X_{max} = 10^q$.

В результаті застосування методики знаходять значення χ^2_c. За таблицями критичних точок розподілу χ^2 [5], за вибраними рівнем значимості α (звичайно α надають одне з трьох значень – 0,1; 0,05; 0,01) і числом степенів свободи k знаходять критичне значення $\chi^2_{кр}$.

Якщо для $\chi_c^2 < \chi_{кр}^2$ – немає підстав не приймати гіпотезу про відповідність імпульсного потоку пуассонівському закону розподілу.

Результати наведені на рис. 3 отримані при $k_c = 10$ і $n_{max} = 1000$. Тут зображені залежності χ_c^2 (SS_n) і середнього значення $\chi_c^2 - \chi_{c\,сер}^2$ (SS_n_av) від значення керуючого коду G при таких умовах:

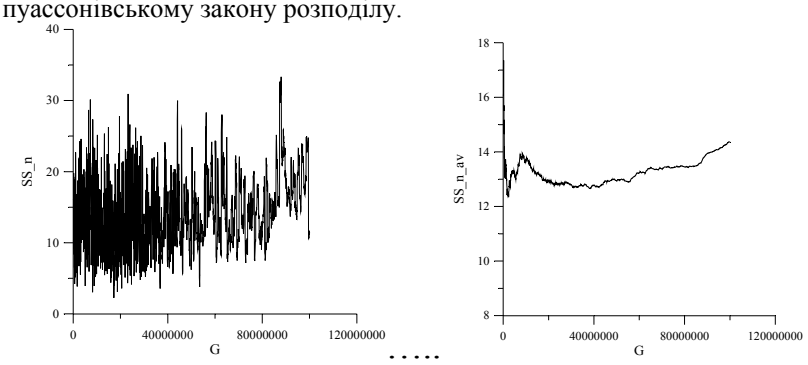
а, б – при відсутності в структурі МГФ логічної схеми ЛС;

в, г – при наявності ЛС ($z = 4$);

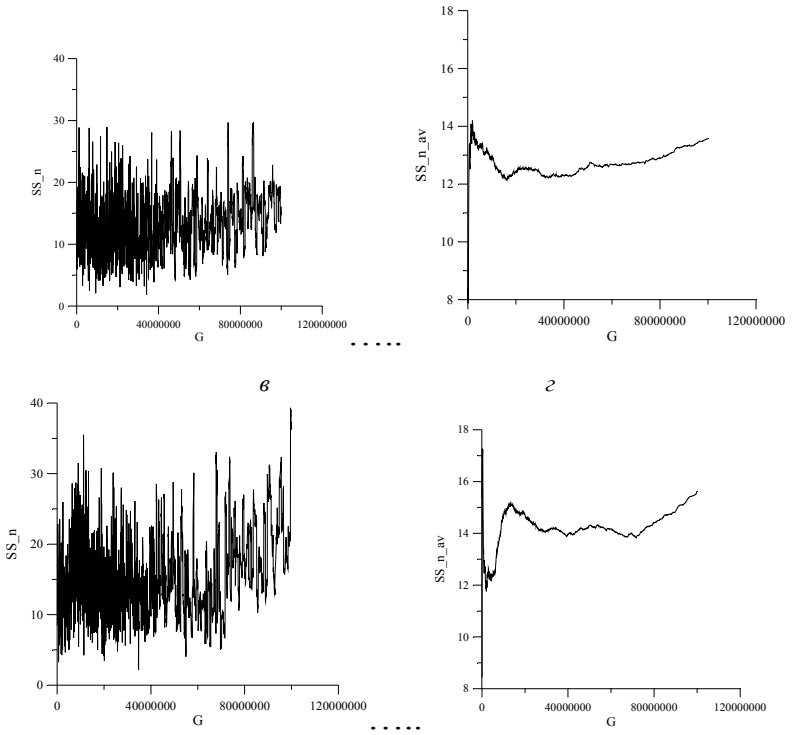
д, у – при наявності ЛС ($z = 29$).

Аналіз наведених результатів дозволяє зробити такі висновки. Наявність в складі ГППП логічної схеми ЛС не призводить до значного покращення статистичних характеристик вихідного імпульсного потоку, а при збільшенні членів рівняння (2), спостерігається навіть їх незначне погіршення – збільшення значень χ_c^2 і $\chi_{c\,сер}^2$.

Порівнявши значення χ_c^2 і $\chi_{c_{сер}}^2$ з $\chi_{кр}^2 = 27{,}7$ (отриманому при рівні значимості $\alpha = 0{,}01$ і числу степенів свободи $k = 13$ [5]) в усьому діапазоні значень керуючого коду G, можна зробити висновок про відповідність, в основному, вихідної імпульсної послідовності ГППП пуассонівському закону розподілу.



а *б*



в *г*

д *е*

Рис. 3. Статистичні характеристики ГПІП на основі двійково-десяткового МГФ

В таблиці 1 наведені статичні характеристики ГПІП на базі МГФ при різних значеннях тактової частоти $f_т$.

Таблиця 1

Статичні характеристики ГППП на базі МГФ

$f_т$, Гц	$\Delta f_{вих}$, Гц	$\Delta\lambda$, $\frac{мкР}{год}$	$G_{min} \div G_{max}$	$f_{вих_{min}} \div f_{вих_{max}}$, Гц	$\lambda_{min} \div \lambda_{max}$, $\frac{мкР}{год}$
$2 \cdot 10^4$	$2 \cdot 10^{-5}$	10^{-3}	$10^4 \div 10^8$	$2 \cdot 10^{-1} \div 2 \cdot 10^3$	$10^1 \div 10^5$
$2 \cdot 10^5$	$2 \cdot 10^{-4}$	10^{-2}	$10^4 \div 10^8$	$2 \cdot 10^0 \div 2 \cdot 10^4$	$10^2 \div 10^6$
$2 \cdot 10^6$	$2 \cdot 10^{-3}$	10^{-1}	$10^4 \div 10^8$	$2 \cdot 10^1 \div 2 \cdot 10^5$	$10^3 \div 10^7$
$2 \cdot 10^7$	$2 \cdot 10^{-2}$	10^0	$10^4 \div 10^8$	$2 \cdot 10^2 \div 2 \cdot 10^6$	$10^4 \div 10^8$

Тут: $\Delta f_{вих} = \frac{1}{10^q} f_т$ – крок зміни середнього значення частоти вихідного сигналу ГППП; $\Delta\lambda = \frac{\Delta f_{вих}}{\gamma}$ – крок зміни значень потужності експозиційної дози (ПЕД) при імітації джерела випромінення; $G_{min} \div G_{max}$, $f_{вих_{min}} \div f_{вих_{max}}$ і $\lambda_{min} \div \lambda_{max}$ – діапазони зміни значень керуючого коду, середнього значення частоти вихідного сигналу ГППП і значень ПЕД відповідно. Дані в табл. 1 отримані при значенні чутливості блоку детектування $\gamma = 0{,}02 \frac{Гц}{мкР/год}$.

5. ВИСНОВКИ

Розроблений двійково-десятковий ГППП може використовуватись для імітації вихідних сигналів дозиметричних детекторів і в системах криптографічного захисту інформації. В останньому випадку необхідною умовою забезпечення задовільних статистичних характеристик вихідного сигналу є введення до його складу логічної схеми ЛС.

1.Бобало Ю.Я., Дудикевич В.Б, Максимович В.М., Хорошко В.О., БісикА.М., Смук Р.Т., Сторонський Ю.Б. : Методи і засоби опрацювання вихідних сигналів дозиметричних детекторів: Монографія. – Львів:

Видавництво Національного університету "Львівська політехніка", 2009. – 200 с. 2.Максимович В.М., Гарасимчук О.І.,Костів Ю.М., Мандрона М.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі. Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2013. – № 29. – с. 167-174. 3.NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [web source]. Accessed: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf. 4.Kostiv Yu.M. Methodology for research of Poisson pulse sequence generators using Pearson's Chi-squared test / Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk, M.M. Mandrona // Sustainable development : International journal. – Varna :Euro-Expert Ltd. – 2013. – № 9. – P. 67-72. 5.Гмурман В. Е. Теория вероятностей и математическая статистика. М., "Высш. школа", 1999. – 479 с.