УДК 681.3
© В. Максимович[1], Ю. Костів[1], А. Петришин[1], 2012

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАТИСТИЧНИХ ХАРАКТЕРИСТИК РІЗНИХ ТИПІВ ГЕНЕРАТОРІВ ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОСЛІДОВНОСТЕЙ

В роботі проведений аналіз статистичних характеристик двох типів генераторів пуассонівської імпульсної послідовності – з використанням генератора М–послідовностей і з використанням функції random мови програмування Delphi.

The statistical characteristics of two types of generators Poisson pulse sequence – using M–sequence generator and using a random function of the programming language Delphi have been analyzed in the paper.

1. ВСТУП

Генератори пуассонівських імпульсних послідовностей (ГПІП) широко використовуються у вимірювальній техніці для імітації вихідних сигналів дозиметричних детекторів і інших процесів, що мають випадковий у часі характер. Вони також використовуються в криптографії при реалізації потокових шифрів.

ГПІП можуть бути реалізовані як апаратними так і програмними засобами. Основною перевагою перших є висока швидкодія, других – універсальність. ГПІП повинні відповідати певним вимогам, що стосуються їх статистичних характеристик і криптостійкості.

Генератори, що розглядаються в даній роботі, націлені, в–першу чергу, на використання у вимірювальній техніці. У зв'язку з цим був проведений аналіз їх статистичних характеристик і не проводилась оцінка їх криптостійкості.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ, МЕТА РОБОТИ

ГПІП, в багатьох випадках, будують на основі генераторів випадкових чисел (ГВЧ). Структурна схема одного із варіантів такої реалізації, що була запропонована в роботі [2], наведена на рис. 1.

ГПІП складається з ГПЧ, схеми порівняння (СП) та логічного елементу І. Імпульси на виході генератора формуються за умови, що $A \le G$, де A – псевдовипадкове число на виході ГПЧ, а G –керуючий код. Середня частота вихідних імпульсів генератора визначається рівнянням:

[1] Національний університет «Львівська політехніка»

$$f_{вих} = \frac{G}{A_{max}} f_т, \quad (1)$$

де $f_т$ – частота вхідних тактових імпульсів; A_{max} – максимальне значення чисел на виході ГПЧ.

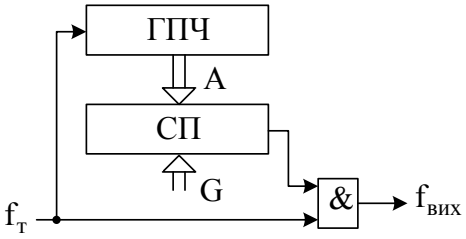

Рис. 1. Структурна схема ГПІП

Для побудови ГПЧ можуть бути використані різні пристрої, зокрема, конгруентні генератори і генератори М–послідовностей. При програмній реалізації ГПЧ можуть також використовуватись спеціальні функції різних мов програмування, наприклад, функція random мови програмування Delphi. Статистичні характеристики різних типів ГПІП, побудованих на основі наведеної структури (рис.1), досліджувались в роботах [1–3]. Однак, в цих роботах не був проведений повний порівняльний аналіз основних статистичних характеристик вихідних імпульсних потоків, до яких належать параметри відхилення від середніх значень кількості вихідних імпульсів за певні проміжки часу, для різних генераторів при однакових умовах.

В даній роботі для аналізу вибрані два типи ГПІП. В першому з них ГПЧ реалізований на генераторі М–послідовностей, в другому – з використанням функція random мови програмування Delphi. Такий вибір пояснюється тим, що вибрані генератори є одними з найбільш поширених, завдяки високій швидкодії першого при апаратній побудові, і простоті програмної реалізації другого.

3. МЕТОДИКА І РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Для дослідження обох типів генераторів були створені імітаційні моделі на мові програмування Delphi.

Визначення основних статистичних характеристик проводилось за такою методикою. Послідовність вхідних тактів ГПІП, була розділена на n_{max} груп. В кожній групі було зафіксовано i_{max} тактів.

Для кожної із $n_{\max}$ груп визначались:

кількість вихідних імпульсів ГППП:

$$n_{Вих_1},\ n_{Вих_2},\ \ldots,\ n_{Вих_{n_{\max}}};\qquad (2)$$

середнє статистичне значення:

$$n_{сер} = \frac{1}{n_{\max}} \sum_{s=1}^{n_{\max}} n_{Вих_s};\qquad (3)$$

дисперсія:

$$D = \frac{1}{n_{\max}} \sum_{s=1}^{n_{\max}} \left(n_{Вих_s} - n_{сер}\right)^2;\qquad (4)$$

кількість значень $n_{вих_s}$, що виходять за межі:

$$n_{сер} - 2\sqrt{n_{сер}} < n_{Вих\,s} < n_{сер} + 2\sqrt{n_{сер}}.\qquad (5)$$

При цьому враховувалось, що для ідеального імпульсного пуассонівського потоку дисперсія повинна дорівнювати середньому статистичному значенню – $D = n_{сер}$, а кількість значень $n_{Вих_s}$, що виходять за межі (5), повинна бути близькою до 5% від $n_{\max}$.

Кожне із таких досліджень (для $n_{\max}$ груп) проводилось j разів.

В результатах, що наведені нижче, були вибрані наступні значення: $j = 10$, $n_{\max} = 100$, $i_{\max} = 1000000$.

При дослідженні характеристик ГППП на базі генератора М–послідовностей був вибраний пристрій на основі твірного поліному $\hat{O}(x) = 1 \oplus x^{18} \oplus x^{31}$ для матриці T_1 при $r = 10$ (рис. 2) [1].

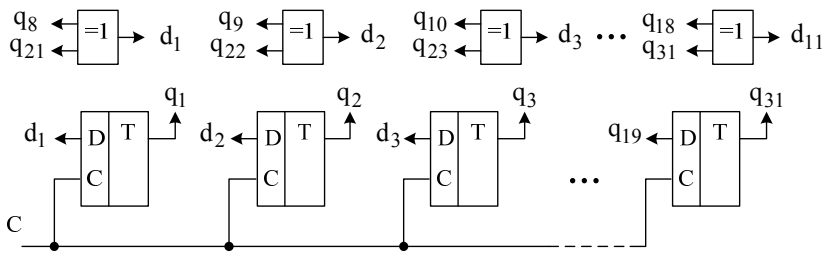

Рис. 2. Генератор М–послідовностей

Результати дослідження, для різних значень керуючих кодів, зведені в табл. 1 і табл.2.

Таблиця 1

Характеристики ГПІП на основі генератора М–послідовностей

G	j	$n_{сер}$	D	Кількість значень $n_{Вих_s}$ за межами (5)
100	1	101,64	77,54	2
	2	98,49	86,59	3
	3	102,19	91,75	4
	4	99,81	83,11	0
	5	102,34	106,42	4
	6	100,15	102,35	3
	7	102,08	97,18	4
	8	98,92	85,92	3
	9	101,61	116,71	7
	10	100,62	97,00	5
1000	1	1009,67	909,95	4
	2	994,24	823,06	2
	3	1005,78	1001,34	8
	4	1001,99	937,41	4
	5	1007,86	864,06	2
	6	993,71	845,55	2
	7	998,69	866,39	5
	8	1005,81	848,89	5
	9	998,53	658,89	1
	10	996,17	741,01	0

Таблиця 2

Характеристики ГПІП на основі функції random
мови програмування Delphi

G	j	$n_{сер}$	D	Кількість значень $n_{Вих_s}$ за межами (5)
100	1	100,26	105,34	4
	2	99,17	114,03	6
	3	98,50	110,66	6
	4	101,23	80,41	3
	5	99,32	102,10	4
	6	100,62	86,40	4
	7	98,88	91,14	3
	8	99,76	86,08	4
	9	101,45	102,39	5
	10	99,55	104,17	4
1000	1	1001,39	1019,69	6
	2	1005,57	1036,59	4
	3	1003,48	961,64	4
	4	999,24	1079	4
	5	996,73	910,57	3
	6	996,93	932,17	3
	7	1003,30	1021,16	5
	8	998,31	1055,89	5
	9	998,56	1121,90	6
	10	995,67	1004,29	5

4. ВИСНОВКИ

Отримані в результаті імітаційного моделювання статистичні характеристики ГПІП, які є близькими до необхідних теоретичних, дозволяють зробити висновок, що обидва типи генераторів можуть мати практичне застосування. При цьому, для випадку використання як базового генератора М–послідовностей, необхідно дотримуватись умови, щоб його період повторення перевищував часовий інтервал, що використовується для формування вихідної імпульсної послідовності. Для наведеного прикладу це означає, що повинна виконуватись умова $2^{31} > j_{\max} \cdot n_{\max} \cdot i_{\max}$.

1. В.М. Максимович, О.І. Гарасимчук, Ю.М. Костів Оптимізація параметрів генератора М–послідовностей, як структурного елемента генератора пуассонівської імпульсної послідовності // Вісник Національного університету «Львівська політехніка» «Автоматика, вимірювання та керування», № 26, 2011. 2. Гарасимчук О.І., Дудикевич В.Б., Максимович В.М., Смук Р.Т. Генератори тестових імпульсних послідовностей для дозиметричних пристроїв // Вісник Національного університету "Львівська політехніка" "Теплоенергетика. Інженерія довкілля. Автоматизація", №506, 2004. – с. 186–192.
3. О.Гарасимчук, В.Максимович, Р.Смук, З.Стрілецький. Аналіз характеристик генератора імпульсної послідовності з пуассонівським законом розподілу побудованого на основі лінійного конгруентного генератора // Вісник Української академії друкарства "Комп'ютерні технології друкарства", №25, 2011. – С. 157–163.