УДК 681.3
© О. Гарасимчук[16], В. Максимович[1], Р. Смук [2], З. Стрілецький[1], 2011

АНАЛІЗ ХАРАКТЕРИСТИК ГЕНЕРАТОРА ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ З ПУАССОНІВСЬКИМ ЗАКОНОМ РОЗПОДІЛУ ПОБУДОВАНОГО НА ОСНОВІ ЛІНІЙНОГО КОНГРУЕНТНОГО ГЕНЕРАТОРА.

1. ПОСТАНОВКА ПРОБЛЕМИ

Генератори пуассонівської імпульсної послідовності (ГПІП), на сьогоднішній день, ефективно використовуються в різних галузях науки. Особливу популярність генератори такого типу здобули для використання у моделюванні різних подій та явищ а також у обчислювальній та вимірювальній техніці, зокрема при імітації вихідного сигналу дозиметричних детекторів.

Закон Пуассона описує імовірність появи рівно k імпульсів за час t згідно наступної формули [1]

$$P_k(Z,t) = \frac{(Zt)^k}{k!} e^{-Zt}, \qquad (1)$$

де Z – середнє число імпульсів за одиницю часу (середня інтенсивність).

Пуассонівським законом розподілу описуються події, які трапляються дуже рідко. До таких подій можна віднести, наприклад, число частинок радіоактивного розпаду, які зареєстровані лічильником протягом деякого часового проміжку t, число викликів, які поступили на телефонну станцію за час t, число дефектів у кусочку тканини або у стрічці фіксованої довжини, число нещасних випадків на виробництві і т.п. Також, простий потік пуассонівських імпульсів може використовуватися як вихідний для отримання більш складних потоків.

Саме використання генераторів пуассонівської імпульсної послідовності для вирішення конкретних практичних чи теоретичних задач потребує попереднього їх ґрунтовного дослідження та проектування з метою отримання ГПІП з характеристиками найбільш наближеними до теоретичних.

Особливо варто приділити увагу вивченню можливостей реалізації ГПІП на основі програмованих логічних інтегральних схем (ПЛІС),

[1] Національний університет «Львівська політехніка»
[2] ПП «НВПП «Спаринг-Віст Центр» (м. Львів)

оскільки поява ПЛІС дала потужний поштовх для розвитку напрямку конфігурованих комп'ютерів. Прилади програмованої логіки, основними представниками яких є ПЛІС, використовуються протягом останніх десятиріч для побудови інтерфейсних вузлів, пристроїв керування, моделювання, контролю і т.п.

2. АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

Питанням дослідження різноманітних методів та способів побудови генераторів імпульсних послідовностей з законами розподілу, що відрізняються від рівномірного не завжди приділяють належної уваги. Існує невелика кількість досліджень в цьому напрямку. Більшість наукових праць присвячені вивченню та дослідженню способів побудови та аналізу характеристик генераторів імпульсних послідовностей з рівномірним законом розподілу [2-6]. На ці праці варто опиратися при побудові ГПІП, оскільки відомим є факт, що для того, щоб отримати псевдовипадкову послідовність з законом розподілу, який відрізняється від рівномірного, необхідно спочатку отримати псевдовипадкову рівномірно розподілену послідовність чисел. Потім на основі певних перетворень можна отримати псевдовипадкову імпульсну послідовність з заданим законом розподілу.

На сьогоднішній день існує велика кількість алгоритмів, за допомогою яких можна отримати псевдовипадкові послідовності з рівномірним законом розподілу. Також існує велика кількість праць присвячених оцінюванню якості генераторів рівномірно розподілених псевдовипадкових чисел за допомогою певних тестів (графічних чи оціночних).

3. МЕТА РОБОТИ

Метою даної роботи є аналіз технічних характеристик ГПІП побудованого на основі лінійного конгруентного генератора та реалізованого на програмованих логічних інтегральних схемах, а також аналіз характеристик вихідного сигналу ГПІП при імітації вихідного сигналу дозиметричних детекторів.

4. Оцінювання основних технічних характеристик ГПІП, побудованого на основі лінійного конгруентного генератора

Реалізація лінійного конгруентного генератора виконувалась згідно відомого рівняння [3-5]

$$X_{n+1} = \left(a \cdot X_n + b\right) \bmod m, \qquad (2)$$

де Xn+1, Xn – чергове та попереднє значення випадкового числа, a – множник, b – приріст, m – модуль.

Узагальнена структурна схема ГПІП реалізованого на базі лінійного конгруентного генератора, з використанням схеми множення, наведена на рис. 1 [7]. Вона складається з кількох основних частин, а саме: комбінаційних суматорів КС1 і КС2, регістрів РГ1 і РГ2, схеми множення СМ, схеми порівняння СП і логічного елементу І.

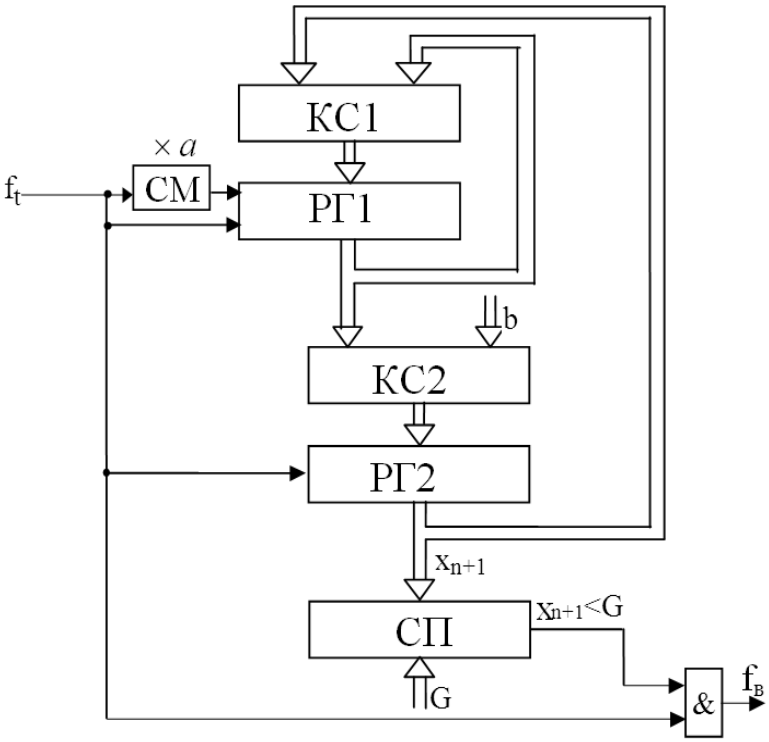

Рис. 1. Структурна схема ГПІП на базі лінійного конгруентного генератора з використанням схеми множення

Нами досліджувався ГПІП реалізований на основі лінійного конгруентного генератора з такими параметрами: a=109; b=12345; m=224, а також m=228, m=230. Ці параметри були обрані в результаті попереднього імітаційного моделювання.

Для дослідження ГПІП побудованих на основі лінійного конгруентного методу, оцінки якості таких генераторів, їх апаратної реалізації у вигляді сучасних ПЛІС, було виконане імітаційне моделювання їхньої роботи за допомогою системи моделювання Foundation фірми Xilinx.

Під час побудови ГПІП на основі лінійного конгруентного генератора ми скористалися стандартними елементами з бібліотеки елементів фірми Xilinx серії SpartanXL. Але, оскільки бібліотечних елементів для додавання двох чисел з розрядністю більшою 30 не існує, тому необхідно будувати комбінаційні суматори, що складаються з декількох послідовно з'єднаних суматорів з меншою розрядністю.

З метою вибору найбільш оптимального, було досліджено три способи побудови 30-ти розрядних нагромаджувальних суматорів, використаних при реалізації ПЛІС ГПІП на основі лінійного конгруентного генератора.

За допомогою часового аналізатора, який входить до складу системи моделювання Foundation, виконаной аналіз часових характеристик ПЛІС ГПІП. Для цього, спочатку, за допомогою опції Implementation, виконано оптимальне розміщення елементів всередині ПЛІС і трасування зв'язків між ними. Результати оцінювання часових характеристик і показників якості ГПІП подані в табл. 1.

Таблиця 1

Зведена таблиця основних технічних характеристик

Кількість розрядів ГПІП	24 розряди	28 розрядів	30 розрядів		
Кількість розрядів секцій нагромаджувального суматора	чотирирозрядний			восьми-розрядний	шістнадцяти-розрядний
Період повторення псевдовипадкових чисел T	16777216	268435456	1073741824		
Мінімальний період тактових імпульсів	40,304 нс	56,116 нс	52,540 нс	40,744 нс	28,866 нс
Максимальна частота тактових імпульсів fмакс	24,811 МГц	17,820 МГц	19,033 МГц	24,543 МГц	34,643 МГц
Максимальна затримка зв'язків	9,065 нс	12,690 нс	11,551 нс	9,777 нс	9,608 нс
Діапазон вихідних частот fв_мін÷fв_макс	1,479 Гц – 24,811 МГц	0,066 Гц – 17,820 МГц	0,018 Гц –19,033 МГц	0,023 Гц – 24,543 МГц	0,032 Гц – 34,643 МГц
Надійна ймовірність	Показники якості				
p =0,68	71,26 %	71,91 %	75,90 %		
p =0,95	95,21 %	96,72 %	96,80 %		
p =0,997	99,4 %	99,93 %	99,98 %		

Таблиця 1 є зведеною, оскільки в ній подані часові результати отримані внаслідок імітаційного моделювання в системі моделювання Foundation фірми XILINX, а також результати програмування в середовищі Delphi.

В таблиці наведені: мінімальний період тактових імпульсів (в наносекундах); максимальні частоти при яких дана ПЛІС ГППП може працювати; максимальна затримка зв'язків, які існують в ПЛІС; діапазон вихідних частот; показники якості ГППП для різних значень надійної ймовірності залежно від способу побудови даних генераторів.

Загальна формула для середньої частоти вихідних імпульсів генератора має вигляд

$$f_в = \frac{G}{m} \cdot f_T , \tag{3}$$

де f_T – частота тактових імпульсів.

Діапазон середніх вихідних частот $f_{в\_мін} \div f_{в\_макс}$ обчислено при умові $f_T = f_{макс}$ за формулами

$$f_{в\_мін} = \frac{1}{m} \cdot f_{макс} \tag{4}$$

$$f_{в\_макс} = \frac{m-1}{m} \cdot f_{макс} \tag{5}$$

Показники якості досліджуваних ГППП знайдено в результаті імітаційного моделювання і співставлено з відомим фактом, що кількість імпульсів пуассонівського імпульсного потоку, яка зафіксована за час ТВ:

а) з надійною ймовірністю p=0,68 знаходиться в межах [8]

$$k_{сер} - \sqrt{k_{сер}} < k < k_{сер} + \sqrt{k_{сер}} ; \tag{6}$$

б) з надійною ймовірністю p=0,95 – в межах

$$k_{сер} - 2\sqrt{k_{сер}} < k < k_{сер} + 2\sqrt{k_{сер}} ; \tag{7}$$

в) з надійною ймовірністю p=0,997 – в межах

$$k_{сер} - 3\sqrt{k_{сер}} < k < k_{сер} + 3\sqrt{k_{сер}} , \tag{8}$$

де

$$k_{сер} = T_B \cdot f_в . \tag{9}$$

Також було проведено оцінювання характеристик вихідного сигналу ГПІП, побудованого на основі лінійного конгруентного генератора, при імітації вихідного сигналу дозиметричних детекторів.

Якщо не враховувати “мертвий час” детекторів, то середню частоту імпульсів на виході блоку детектування, яка залежить від потужності експозиційної зони (ПЕД) іонізуючого випромінювання λ і чутливості детектора γ, можна обчислити за формулою

$$f_в = \lambda \cdot \gamma . \qquad (10)$$

В табл. 2 подані характеристики ГПІП, реалізованого на базі лінійного конгруентного генератора, при імітації вихідного сигналу дозиметричного детектора. Ці характеристики обчислені за умови, що $\gamma = 0.02 \frac{Гц}{мкР/год}$.

Таблиця 2

Характеристики ГПІП на базі лінійного конгруентного генератора

Кількість розрядів ГПІП	24 розряди	28 розрядів	30 розрядів		
Кількість розрядів секцій нагромаджувального суматора	чотирирозрядний			восьмирозрядний	шістнадцятирозрядний
Період повторення T_n	0,676 сек	15,064 сек	56,415 сек	43,749 сек	30,994 сек
Діапазон значень ПЕД λ	73,95 мкР/год – 1240,55 Р/год	3,3 мкР/год – 891 Р/год	0,9 мкР/год – 951,65 Р/год	1,15 мкР/год – 1227,15 Р/год	1,6 мкР/год – 1732,15 Р/год

Період повторення ГПІП T_n та діапазон значень ПЕД λ визначено за формулами

$$T_n = \frac{m}{f_{макс}} \qquad (11)$$

$$\lambda = \frac{f_{в\_макс} \div f_{в\_мін}}{\gamma} \qquad (12)$$

5. ВИСНОВКИ

Оскільки розроблені ГППП забезпечують достатньо широкий діапазон значень імітації ПЕД і задовільні статистичні характеристики вихідного імпульсного потоку, вони можуть ефективно використовуватись при розробленні і налагодженні дозиметричних пристроїв різного призначення.

1. Бобнев, М. П. Генерирование случайных сигналов [Текст] / М. П. Бобнев// Изд. 2-е перераб. и доп. – М., "Энергия", 1971. – 239 с. 2. Гарасимчук, О.І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості [Текст] / О. І. Гарасимчук, В. М. Максимович// "Захист інформації", м.Київ, – 2002. 7 – С. 80-87. Иванов, М. А., Теория, применение и оценка качества генераторов псевдослучайных последовательностей [Текст] / М. А Иванов, И. В. Чугунков // (СКБ – специалисту по компьютерной безопасности), М.: КУДИЦ – ОБРАЗ, 2003. –240 с. 4. Гундарь К. Ю. Защита информации в компьютерных системах [Текст] / К. Ю. Гундарь, А. Ю. Гундарь, Д. А. Янишевский // К.: "Корнейчук", 2000. – 152 с., 5. Кнут. Д. Искусство программирования для ЭВМ: В 3-х т. Получисленные алгоритмы. [Текст] / Д. Кнут // Пер. с англ. – М.: Мир, 1977. – Т.2. – 724 с. 6. Романец, Ю. В. Защита информации в компьютерных системах и сетях [Текст] / Ю. В. Романец, П. А. Тимофеев, В.Ф. Шаньгин // Под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с. 7. Гарасимчук, О. І., Генератори тестових імпульсних послідовностей для дозиметричних пристроїв [Текст] / О. І. Гарасимчук, В. Б. Дудикевич, В. М. Максимович, Р. Т. Смук // Вісник Національного університету "Львівська політехніка" "Теплоенергетика. Інженерія довкілля. Автоматизація", – 2004. – №506. – С. 186-192. 8. Орнатский, П. П. Теоретические основы информационно-измерительной техники [Текст] / П. П. Орнатский // [Учебн. для вузов по спец. "Информ. – изм. техника"] – 2-е изд., перераб. и доп. – Киев : Вища школа, 1983. – 455 с.