Аналіз статистичних характеристик ГПІП на основі функції random програмного середовища Delphi

Володимир Максимович[1], Юрій Костів[1], Марія Мандрона[2], Олег Гарасимчук[3]

1. Кафедра безпеки інформаційних технологій, Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С. Бандери, 12;

2. Кафедра управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, УКРАЇНА, м. Львів, вул. Клепарівська,35, E-mail: mandrona27@gmail.com

3. Кафедра захисту інформації, Національний університет "Львівська політехніка", УКРАЇНА, м.Львів, вул. С.Бандери, 12, E-mail:garasymchuk@ukr.net

The structure scheme of Puisson pulses sequence generator that is based on random function generator is present in the paper. There are also results of researching it statistical characteristics, depending on the value of control code.

Ключові слова – генератор псевдовипадкових імпульсних послідовностей, пуассонівський потік, статистичні характеристики.

Вступ

Відомий цілий ряд генераторів псевдовипадкових імпульсних послідовностей. Одними з основних їх характеристик є закони статистичного розподілу. Багато послідовностей характеризуються експоненційними законами розподілу імпульсів, причому параметри цих законів можуть бути різними. До таких імпульсних послідовностей можна віднести пуассонівську. Генератори пуассонівських імпульсних послідовностей (ГПІП) знайшли застосування в різних областях науки і техніки, зокрема, у системах захисту інформації.

Результати аналізу ГПІП

У роботі [1] нами була запропонована нова структура ГПІП (рис. 1), що складається з генератора псевдовипадкових чисел ГПЧ, схеми порівняння СП і логічного елементу "І".

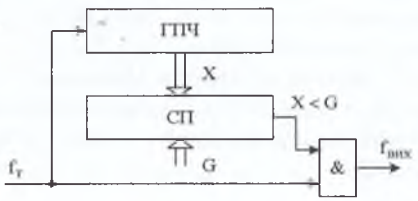

Рис. 1. Структурна схема ГПІП

Вхідні тактові імпульси проходять на вихід пристрою при умові коли число на виході ГПЧ – X є меншим від керуючого коду *G*. Середня частота вихідних імпульсів визначається рівнянням:

$$f_{вих} = \frac{G}{2^m} f_m , \qquad (1)$$

де m – кількість двійкових розрядів.

Також нами запропоновано [2, 3] удосконалення методики оцінки якості імпульсної послідовності на відповідність пуассонівському закону розподілу, де потік вхідних імпульсів розділяється на n однакових груп, кожна з яких складається з $i_{\max}$ імпульсів. Максимальна кількість груп – $n_{\max}$. Групам вхідних імпульсів відповідають групи вихідних імпульсів з числом імпульсів k_1, k_2, ..., $k_{n_{\max}}$.

Методика ґрунтується на класичній методиці перевірки гіпотези про розподіл генеральної сукупності за законом Пуассона з використанням критерію Пірсона (критерію χ^2) [4]. 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

$$i_{\max} = \frac{2^m}{G} k_c . \qquad (2)$$

У результаті використання запропонованої методики для кожного значення *G* визначається значення χ_c^2. Далі, за таблицями критичних точок розподілу χ^2 та вибраними рівнем значимості α (звичайно α надають одне з трьох значень –0,1; 0,05; 0,01) і числом степенів свободи r знаходять критичне значення $\chi_{кр}^2$. Якщо $\chi_c^2 < \chi_{кр}^2$ – немає підстав не приймати гіпотезу про відповідність імпульсного потоку пуассонівському закону розподілу.

Розроблена удосконалена методика була використана для оцінки ГПІП різних типів [2, 3], що дозволило, в певній мірі, оптимізувати їх структури і алгоритми роботи. Однак, велика кількість можливих варіантів реалізації ГПЧ, які є основою ГПІП, дає змогу продовжувати пошук кращих рішень, з урахуванням основних параметрів генераторів: статистичних характеристик імпульсної послідовності, діапазону її середніх частот, швидкодії, складності (технологічності) побудови при апаратній реалізації.

Особлива увага приділялась дослідженню діапазону значень керуючого коду G, при якому забезпечується відповідність вихідного імпульсного потоку пуассонівському закону розподілу, включаючи початкові стани регістрів генератора.

Результати аналізу статистичних характеристик ГПІП на основі функції random, отримані з допомогою імітаційного моделювання, наведені на рис. 2.

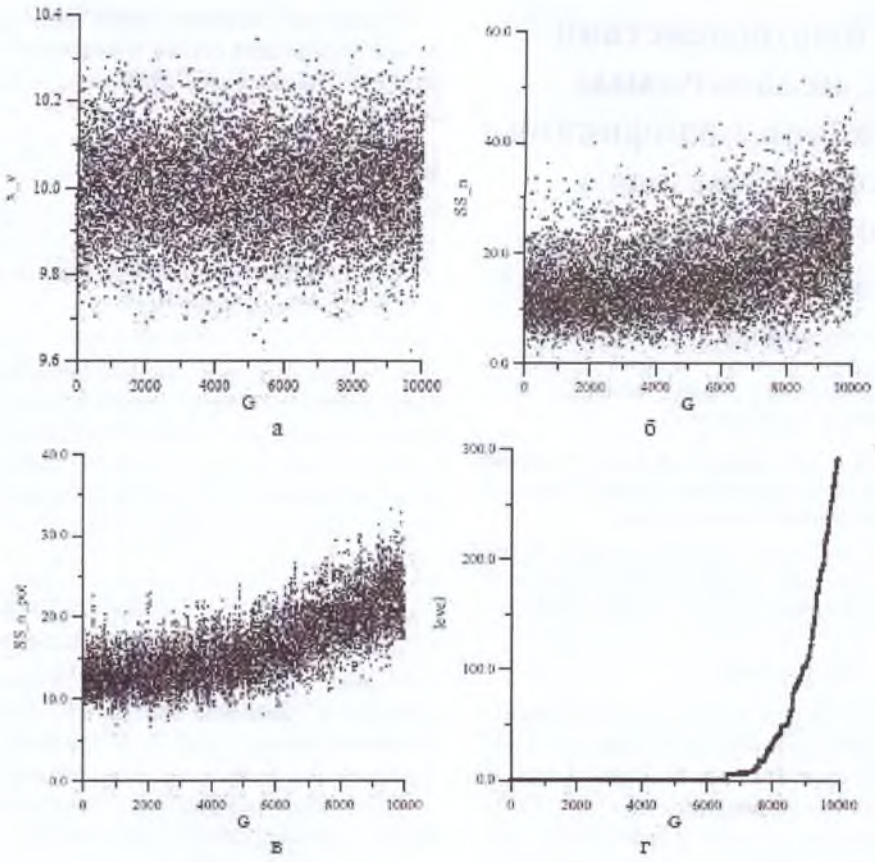

Рис. 3. Статистичні характеристики ГПІП на основі функції random

Тут представлені залежності наступних величин від значення керуючого коду G:

а) середньої величини значень k_1, k_2 … $k_{n_{\max}}$ – $k_в$ (x_v);

б) значення χ_c^2 (SS_n);

в) усередненої величини п'яти останніх значень χ_c^2 – $\chi_{ссер}^2$ (SS_n_pot);

г) кількості значень $\chi_{ссер}^2$, що перевищили $\chi_{кр}^2$ – k_{level} (level).

Результати отримані при

$$m = 16,\ n_{\max} = 1000,\ k_c = 10,\ \chi_{кр}^2 = 25. \qquad (3)$$

В доповнення до попередніх робіт [3, 4], в яких використовувалась запропонована методика, в даній роботі введені величини $\chi_{ссер}^2$ і k_{level}, що дозволяє більш зручно (більш інтегрально) оцінювати якість імпульсної послідовності. Зокрема, залежність k_{level} від G (рис. 2г) дозволяє зробити висновок, що в діапазоні $0 \div 6500$ значень керуючого коду G, вихідна імпульсна послідовність ГПІП відповідає пуассонівському закону розподілу. Тут і далі діапазони значень G визначаються приблизно і, при потребі, можуть бути уточнені.

Висновки

ГПІП на основі функції random програмного середовища Delphi забезпечують статистичні характеристики вихідної імпульсної послідовності, що відповідає пуассонівському закону розподілу, в достатньо ширшому діапазоні значень керуючого коду.

Література

[1] Генератори тестових імпульсних послідовностей для дозиметричних пристроїв / [Гарасимчук О.І., Дудикевич В.Б., Максимович В.М., Смук Р.Т.] // Вісник НУ "Львівська політехніка" – "Теплоенергетика. Інженерія довкілля. Автоматизація". – 2004. – №506. – С. 187-193.

[2] Методика оптимізації параметрів генераторів пуассонівських імпульсних послідовностей побудованих на основі лінійних конгруентних генераторів / [Костів Ю.М., Максимович В.М., Гарасимчук О.І., Мандрона М.М.] // Науковий вісник НЛТУ України : збірник науково-технічних праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 23.11. – С. 322-328.

[3] Methodology for research of Poisson pulse sequence generators using Pearson's Chi-squared test / [Kostiv Yu.M., Maksymovych V.M., Harasymchuk O.I., Mandrona M.M.] // Sustainable development : International journal. – Varna : Euro-Expert Ltd. – 2013. – № 9. – Pp. 67-72.

[4] Критические точки распределения χ2. [Електронний ресурс].– Доступно з: http://math.semestr.ru/group/xixi.php.