МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

КОСТІВ ЮРІЙ МИХАЙЛОВИЧ

УДК 621.319.5+004.3

ГЕНЕРАТОРИ ПУАССОНІВСЬКИХ ІМПУЛЬСНИХ ПОСЛІДОВНОСТЕЙ З ПОКРАЩЕНИМИ ХАРАКТЕРИСТИКАМИ

05.13.05 - комп’ютерні системи та компоненти

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Львів — 2014

Дисертацією є рукопис

Робота виконана у Національному університеті „Львівська політехніка” Міністерства освіти і науки України

***Науковий керівник*:** доктор технічних наук, професор
Максимович Володимир Миколайович,
Національний університет „Львівська політехніка”,
завідувач кафедри безпеки інформаційних технологій
(м. Львів, Україна)

***Офіційні опоненти*:** доктор технічних наук, професор
Карпінський Микола Петрович,
Університет в Бельску-Бялій,
завідувач закладу інформатики
(м. Бельско-Бяла, Польща)

кандидат технічних наук
Лукенюк Адольф Антонович,
Львівський центр Інституту космічних досліджень
Національної академії наук України та
Національного космічного агентства України,
директор (м. Львів, Україна)

Захист відбудеться **« 28 » березня 2014 р. о 16^{00} годині** на засіданні спеціалізованої вченої ради Д 35.052.08 у Національному університеті „Львівська (79013, м. Львів, вул. С. Бандери,12, *ауд. 226 головного корпусу*).

З дисертацією можна ознайомитися у бібліотеці Національного університету „Львівська політехніка” (79013, м. Львів,вул. Професорська, 1).

Автореферат розісланий**« 27 » лютого 2014 р.**

Вчений секретар спеціалізованої
вченої ради Д 35.052.08, д.т.н., професор **Луцик Я.Т.**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Генератори випадкових і псевдовипадкових імпульсних послідовностей використовуються в різних галузях науки та техніки, зокрема у моделюванні процесів, що описуються різними законами розподілу, в апаратних та програмних системах захисту інформації, в засобах криптографічного перетворення інформації.

Поряд із випадковими сигналами, що є неперервними функціями часу, на практиці важливу роль відіграють імпульсні випадкові сигнали. Серед імпульсних сигналів варто виділити так звані хаотичні імпульсні завади (ХІЗ). Під ХІЗ варто розуміти імпульси, випадкові за моментами появи. Послідовність буде підпорядковуватися закону Пуассона, якщо задовольняють три умови:

1) стабільність середньої частоти появи імпульсів (стаціонарність потоку);
2) незалежність ймовірності появи *i*-го імпульсу від того, в який момент появився *i*-1-й імпульс (відсутність післядії);
3) практична неможливість появи на як завгодно малому відрізку двох і більше імпульсів (ординарність потоку).

Процеси, які підпорядковуються пуассонівському закону розподілу, зустрічаються як в природі, так і в техніці. Тому важливим є вирішення задач з генерування чи моделювання таких процесів. Методи моделювання відрізняються в залежності від типу пуассонівського процесу, тобто простору, в якому протікає процес, і однорідності чи неоднорідності процесу.

Закону Пуассона, зокрема, підпорядковуються такі процеси: – кількість повідомлень, що надходять на телефонні, телеграфні станції; – виявлення будь-яких дефектів в процесі контролю якості; – розподіл молекул в деяких хімічних реакціях; – кількість замовлень на обслуговування промислових підприємств і т.ін. Закон Пуассона описує дискретні події, що виражаються кількістю заявок чи замовлень, що надійшли. Також генератори пуассонівських імпульсних послідовностей (ГПІП) використовують під час моделювання несправностей інтегральних схем, для імітації вихідних сигналів дозиметричних детекторів.

Закон Пуассона тісно пов'язаний з показниковим законом. А саме, якщо час між надходженнями двох складних заявок описується показниковим законом, то число таких заявок за визначений інтервал часу описується законом Пуассона.

Широке застосування розподілу Пуассона обумовлено тим, що він описує виникнення рідкісних подій з незмінною, або такою, що змінюється порівняно повільно середньою частотою. Тому серед усього різноманіття генераторів випадкових та псевдовипадкових чисел або послідовностей важливе місце займають ГПІП.

ГПІП, аналогічно до інших генераторів псевдовипадкових імпульсних послідовностей (ГПВП) чи генераторів псевдовипадкових чисел (ГПЧ) можуть реалізовуватися як апаратними так і програмними засобами залежно від мети їх застосування і забезпечення необхідних параметрів. Тому потрібно проводити пошук оптимальних методів побудови ГПІП, які б мали задовільні статистичні характеристики, високу швидкодію, можливість оперативної зміни середньої частоти вихідних імпульсів та простоту реалізації.

Незважаючи на значну кількість публікацій, що стосуються побудови і

дослідження характеристик ГПІП, невирішеними залишаються багато важливих питань. Оцінювання якості ГПІП проводиться за спрощеними методиками, які не враховують необхідності дослідження статистичних характеристик у всьому діапазоні значень середньої частоти вихідних сигналів (у всьому діапазоні значень керуючого коду) і без урахування сучасних стандартизованих методик дослідження статистичних характеристик ГПЧ і ГПВП, зокрема, методик стандартів NIST (США). Невирішені питання оптимізації параметрів простих і складених структур ГПЧ на основі регістрів зсуву з лінійними зворотними зв'язками (РЗЛЗЗ), як таких, що забезпечують найвищу швидкодію ГПЧ, а отже і ГПІП. Не знайшли свого вирішення задачі оптимізації параметрів ГПЧ на основі реалізації конгруентних залежностей, як складових частин ГПІП. Тому розроблення нових методів та засобів побудови генераторів пуассонівських імпульсних послідовностей є актуальним.

Зв'язок роботи з науковими програмами, планами, темами. Роботу виконано на кафедрі безпеки інформаційних технологій Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка». Тема дисертаційної роботи відповідає науковому напряму кафедри безпеки інформаційних технологій. Дисертація виконана в межах науково-дослідної роботи «Розробка та дослідження генераторів псевдовипадкових чисел і послідовностей» (№ державної реєстрації 0113U005267, квітень 2013р. – грудень 2017р., виконавець).

Результати використані при виконанні госпдоговірної науково-дослідної роботи № 0380 «Розроблення алгоритмів опрацювання вихідних сигналів дозиметричних детекторів» (термін виконання 20.03.11р.–31.12.12р.).

Мета і задачі дослідження. Метою роботи є розроблення нових методів і засобів побудови ГПІП, порівняльний аналіз їхніх характеристик, розробка методів оцінювання їхньої якості.

Для досягнення цієї мети необхідно було вирішити такі основні задачі:

– проаналізувати методи та засоби генерування пуассонівських імпульсних послідовностей і алгоритми оцінювання їх якості;

– запропонувати удосконалені методики оцінювання статистичних характеристик ГПІП;

– дослідити характеристики ГПІП на основі конгруентних генераторів та сформулювати рекомендації щодо вибору оптимальних параметрів лінійних конгруентних генераторів;

– модифікувати генератори Фібоначчі з метою реалізації на їх основі ГПІП з покращеними характеристиками;

– дослідити характеристики ГПІП на основі РЗЛЗЗ та сформулювати рекомендації щодо вибору оптимальних параметрів РЗЛЗЗ;

– запропонувати структуру ГПІП на основі генератора Джіффі, яка дозволить розширити діапазон значень керуючого коду, при якому досягаються задовільні статистичні характеристики вихідного сигналу;

– розробити покращену методику проектування ГПІП;

– спроектувати на програмовних логічних інтегральних середовищах (ПЛІС) ГПІП на основі модифікованих генераторів Фібоначчі і Джіффі та дослідити їхні параметри.

Об’єкт дослідження – процес генерування пуассонівських імпульсних послідовностей.

Предмет дослідження – методи та апаратні засоби для реалізації ГПІП, методи оцінювання їхньої якості.

Методи дослідження – теоретичні дослідження базуються на використанні основних положень теорії цифрових автоматів, теорії ймовірності, теорії похибок. При реалізації теоретичних досліджень і розробок використані методи комп'ютерного моделювання і система автоматизованого проектування ПЛІС.

Наукова новизна одержаних результатів. Найважливішими науковими результатами є такі:

- Вперше запропоновано спосіб визначення статистичних характеристик вихідних сигналів ГПІП, що ґрунтується на розбитті потоку вхідних тактових імпульсів на групи, кількість імпульсів в яких залежить від керуючого коду і відповідає однаковій середній кількості вихідних імпульсів, з подальшим використанням критерію Пірсона, що, на відміну від існуючих методик, дало можливість оцінити статистичні характеристики ГПІП у всьому діапазоні значень середніх частот вихідного сигналу;
- Вперше розроблено модифікований адитивний генератор Фібоначчі, в якому введення додаткової складової в процес додавання дає можливість формувати псевдовипадкові числа за модулем, що дорівнює степені двійки, і тим самим істотно спрощує його апаратну реалізацію у порівнянні з відомими рішеннями, при збереженні задовільних статистичних характеристик ГПІП, побудованих на його основі;
- Вперше розроблено ГПІП на основі модифікованого генератора Джіффі, в якому для формування псевдовипадкових чисел використовується мультиплексування розрядів ГПЧ на основі РЗЛЗЗ за допомогою виходу одного з розрядів керуючого РЗЛЗЗ, що дало можливість розширити діапазон значень керуючого коду, при якому досягаються задовільні статистичні характеристики вихідного сигналу;
- Отримали подальший розвиток методи проектування ГПІП, побудованих на основі РЗЛЗЗ і лінійних конгруентних генераторів (ЛКГ), які ґрунтуються на запропонованому способі оцінки якості ГПІП, що дозволило комплексно покращити їх параметри.

Практичне значення одержаних результатів:

- Розроблений спосіб оцінювання якості ГПІП і методики на його основі можуть бути використані для дослідження статистичних характеристик таких генераторів і оптимізації їх параметрів;
- Розроблені імітаційні моделі структурних елементів ГПІП дозволяють оперативно проводити їх дослідження для різних типів ГПЧ, побудованих, зокрема, на РЗЛЗЗ і ЛКГ, знаходити можливості покращення їх характеристик, створювати нові більш досконаліші генератори;

- ГПІП, побудовані на основі модифікованих генераторів Фібоначчі і Джіффі, та імплементовані в ПЛІС, можуть бути використані при створенні спеціалізованих апаратних засобів;
- Теоретичні і практичні результати роботи використовуються при проектуванні і налагодженні дозиметричних пристроїв;
- Створено програмні і апаратні засоби імітації вихідних сигналів дозиметричних детекторів, що використовуються при розробленні і налагодженні пристроїв для вимірювання параметрів іонізуючого випромінювання у ПП «НВПП «Спаринг-Віст Центр» (м. Львів);
- Розроблений пакет прикладних програм та рекомендації використовуються у Національному університеті “Львівська політехніка” на кафедрі “Безпека інформаційних технологій” в курсах “Електроніка і мікросхемотехніка”, “Криптографічні системи та протоколи”, “Прикладна криптографія”.

Особистий внесок здобувача. Усі наукові результати дисертаційної роботи автор отримав самостійно. У друкованих працях, опублікованих у співавторстві, здобувачеві належить: аналіз існуючих варіантів генерування пуассонівських імпульсних послідовностей і методів оцінювання їх якості; розробка модифікованих генераторів і виконання експериментальних досліджень; математичне опрацювання та узагальнення отриманих результатів; формулювання основних положень дисертації та висновків.

Науковці, разом з якими проводились дослідження, є співавторами публікацій, в яких викладено результати дисертаційної роботи. Внесок автора у вирішення задач, які виносяться на захист, є основним.

Апробація результатів дисертації. Основні положення і результати дисертації доповідались, обговорювались та опубліковані в матеріалах міжнародних і вітчизняних конференцій: І міжнародної науково-практичної конференції «Безпека та захист інформації в інформаційних та телекомунікаційних системах».- (Харків, 2008); міжнародної науково-практичної конференції «Сучасні засоби та технології розроблення інформаційних систем».- (Харків, 2008); III, VI міжнародних конференцій молодих вчених «Комп’ютерні науки та інженерія – 2009, 2013».- (Львів, 2009, 2013); I, II міжнародних науково-технічних конференцій «Захист інформації і безпека інформаційних систем».- (Львів, 2012, 2013); The Second International Conference on Automatic Control and Information Technology 2013 (ICACIT'13) (Kraków, Poland, 2013).

Публікації. За темою дисертаційної роботи опубліковано 10 наукових статей – з них 9 у фахових виданнях України та 1 у науковому періодичному виданні іншої держави, а також 7 тез доповідей на міжнародних і вітчизняних наукових конференціях.

Структура і обсяг дисертації. Дисертаційна робота складається з вступу, основної частини (п’ять розділів), висновків, списку використаних джерел літератури (109 найменувань) і додатків; містить 58 рисунків і 27 таблиць. Повний обсяг дисертації – 155 сторінок; зміст основної частини викладений на 115 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано вибір та актуальність теми досліджень, визначено мету, об'єкт та предмет дослідження, показано наукову новизну та практичну цінність одержаних результатів, наведені відомості про реалізацію й апробацію роботи.

Перший розділ містить огляд літератури, в якому наведено умови формування імпульсних потоків з пуассонівським законом розподілу, сфери застосування ГПІП, апаратні і програмні засоби їх реалізації, основні характеристики і методи оцінювання їх якості, розглянуто основні проблеми, що виникають перед розробниками, переваги та недоліки існуючих напрацювань.

У результаті аналізу існуючих типів ГПІП показано, що найвдалішою для реалізації є структура, до складу якої входять ГПЧ і схема порівняння, оскільки вона забезпечує можливість оперативного керування середньою частотою вихідних імпульсів

$$f_{вих} = \frac{G}{X_{max}} f_т, \qquad (1)$$

де G – керуючий код, $f_т$ – частота тактових імпульсів, X_{max} – максимальне значення псевдовипадкового числа X на виході ГПЧ.

При цьому основні характеристики такого генератора (період повторення, швидкодія, статистичні характеристики) залежать від способу побудови ГПЧ. У зв'язку з цим розглянуто класифікацію ГПЧ. Проаналізовано основні методи побудови ГПЧ, до яких не висуваються вимоги забезпечення крипостійкості, а саме на основі: РЗЛЗЗ, генераторів Джіффі, генераторів Голлманна, лінійних конгруентних генераторів, генераторів Фібоначчі та ін.

Розглянуто основні методи оцінювання якості ГПІП і ГПЧ, зокрема, методи оцінювання їх статистичних характеристик. Обґрунтовано необхідність використання сучасних наборів тестів, зокрема тестів NIST STS. Показано, що методи аналізу якості ГПІП, що використовуються на даний час, не розраховані на визначення статистичних характеристик у всьому діапазоні значень середніх частот вихідних сигналів генераторів і, отже, потребують удосконалення.

У результаті проведених досліджень сформульовано задачі досліджень, що полягають, зокрема, у потребі оптимізації параметрів ГПЧ, що є структурними елементами ГПІП, з метою покращення характеристик останніх і у пошуку нових структур ГПЧ для забезпечення побудови ГПІП з покращеними характеристиками.

У другому розділі запропоновано нові способи визначення статистичних характеристик вихідних сигналів ГПІП, які ґрунтуються на розбитті потоку вхідних тактових імпульсів на групи, кількість імпульсів в яких залежить від керуючого коду і відповідає однаковій середній кількості вихідних імпульсів, з подальшим використанням інтервальних імовірнісних характеристик чи критерію Пірсона. На відміну від існуючих способів оцінювання якості ГПІП вони дають можливість

оцінити статистичні характеристики ГПІП у всьому діапазоні значень середніх частот вихідного сигналу.

Узагальнена методика дослідження параметрів вихідного сигналу ГПІП на відповідність пуассонівському закону розподілу з використанням критерію Пірсона полягає в тому, що потік вхідних імпульсів ГПІП розділяється на n однакових груп, кожна з яких складається з i_{max} імпульсів (рис. 1). Максимальна кількість груп – n_{max}. Групам вхідних імпульсів відповідають групи вихідних імпульсів з числом імпульсів k_1, k_2, …, $k_{n_{max}}$.

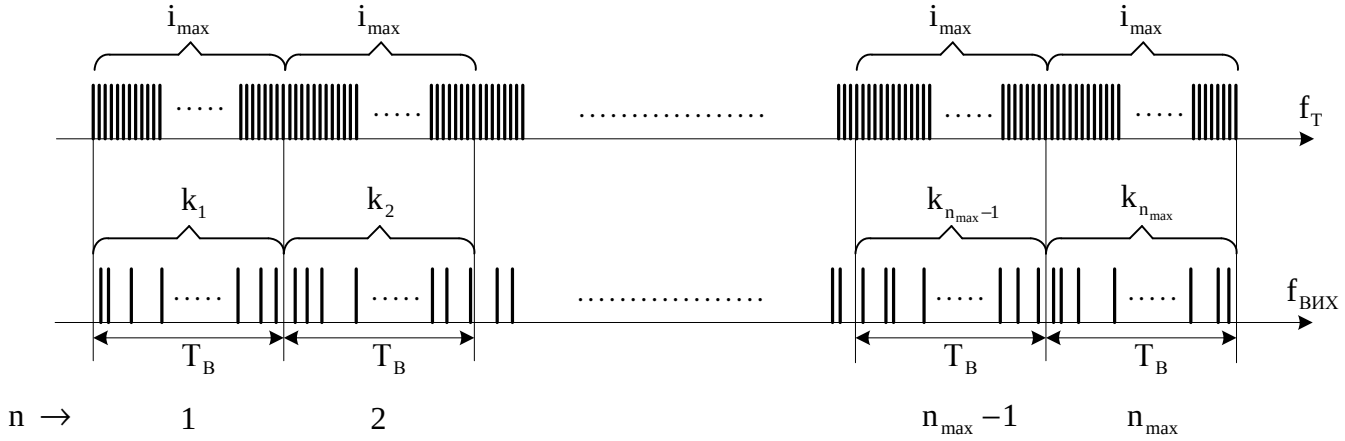


Рис.1. Розбиття вхідних і вихідних імпульсних потоків на групи

Запропонована методика ґрунтується на класичній методиці перевірки гіпотези про розподіл генеральної сукупності за законом Пуассона з використанням критерію Пірсона (критерію χ^2). При цьому, враховуючи специфіку побудови ГПІП, були запропоновано такі 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

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

Подальша перевірка гіпотези відбувається так:

- за емпіричним розподілом, отриманим в результаті моделювання роботи ГПІП, знаходять вибіркову середню величину значень k_1, k_2 … $k_{n_{max}}$ – $k_в$;

- приймають як параметр λ розподілу Пуассона вибіркову середню – $\lambda = k_в$;

- знаходять, за формулою Пуассона – $P_j = \lambda^j \frac{e^{-\lambda}}{j!} = k_в{}^j \frac{e^{-k_в}}{j!}$ імовірності появи рівно j імпульсів (на інтервалі i_{max}) в n_{max} випробовуваннях (j = 0, 1, 2, …);

- знаходять теоретичні частоти $Q_j = P_j \cdot n_{max}$;

- в процесі моделювання знаходять емпіричні частоти – N_j;

- для кожного значення j з допомогою критерію Пірсона визначають $S_j = \frac{(N_j - Q_j)^2}{Q_j}$ і $\chi_c^2 = \sum_{j=0}^{j_{max}} S_j$;

- при необхідності значення N_j, P_j і Q_j, що відповідають малим імовірностям P_j, об'єднуються в одну чи дві групи, і обчислення для S_j і χ_c^2 виконують з урахуванням цього факту;

- визначається число степенів свободи $r = d - 2$, де d – кількість груп, що залишились після можливого об'єднання;

- за таблицями критичних точок розподілу χ^2, за 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 для більшості значень керуючого коду G, $\chi_c^2 < \chi_{кр}^2$, тоді немає підстав не приймати гіпотезу про відповідність імпульсного потоку пуассонівському закону розподілу.

Також у роботі запропоновано спрощену методику дослідження статистичних характеристик вихідних сигналів ГПІП, що ґрунтується на використанні інтервальних імовірнісних характеристик. Згідно з нею кількість імпульсів пуассонівського імпульсного потоку, що зафіксована за час T_B, з надійною ймовірністю p=0,95, повинна знаходитись в межах $k_C - 2\sqrt{k_C} < k < k_C + 2\sqrt{k_C}$, де $k_c = \frac{G}{X_{max}} i_{max}$.

Ефективність запропонованих методів оцінки якості ГПІП доведено на прикладах їх побудови з використанням різних типів ГПЧ.

У третьому розділі з використанням запропонованого способу оцінювання якості здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові ГПЧ на основі РЗЛЗЗ. При цьому для РЗЛЗЗ знайдено твірні поліноми, типи і степені матриці, при яких ці характеристики є задовільними в широкому діапазоні значень середніх частот вихідного сигналу.

Варіанти побудови РЗЛЗЗ необхідно розглядати, виходячи з рівняння його функціонування $Q(t+1) = T^r Q(t)$, де $Q(t)$ і $Q(t+1)$ – стани регістра для попереднього і наступного тактів роботи, степені і виду твірного поліному $\Phi(x) = \sum_{i=0}^{N} a_i x^i$ ($a_N = a_0 = 1$, $a_j \in \{0,1\}$, $j = \overline{1,(N-1)}$), вигляду (T_1 чи T_2) матриці, значення степені матриці r. Вибір структури РЗЛЗЗ потрібно починати з вибору твірного поліному, оскільки від його степеня залежить період повторення псевдовипадкової послідовності, одного з основних параметрів генератора.

На рис. 2 наведено результати дослідження статистичних характеристик ГПІП, побудованого на основі РЗЛЗЗ відповідно до поліному $\Phi(x) = 1 \oplus x^{18} \oplus x^{31}$, типу матриці Т1 при $r = 3$ (рис. 2 а,б) і $r = 10$ (рис. 2 в,г). При цьому на рис. 2 а, в представлено залежності χ_c^2 від керуючого коду G, а на рис. 2 б, г – залежності поточних усереднених значень $\chi_{c\,сер}^2$ від G.

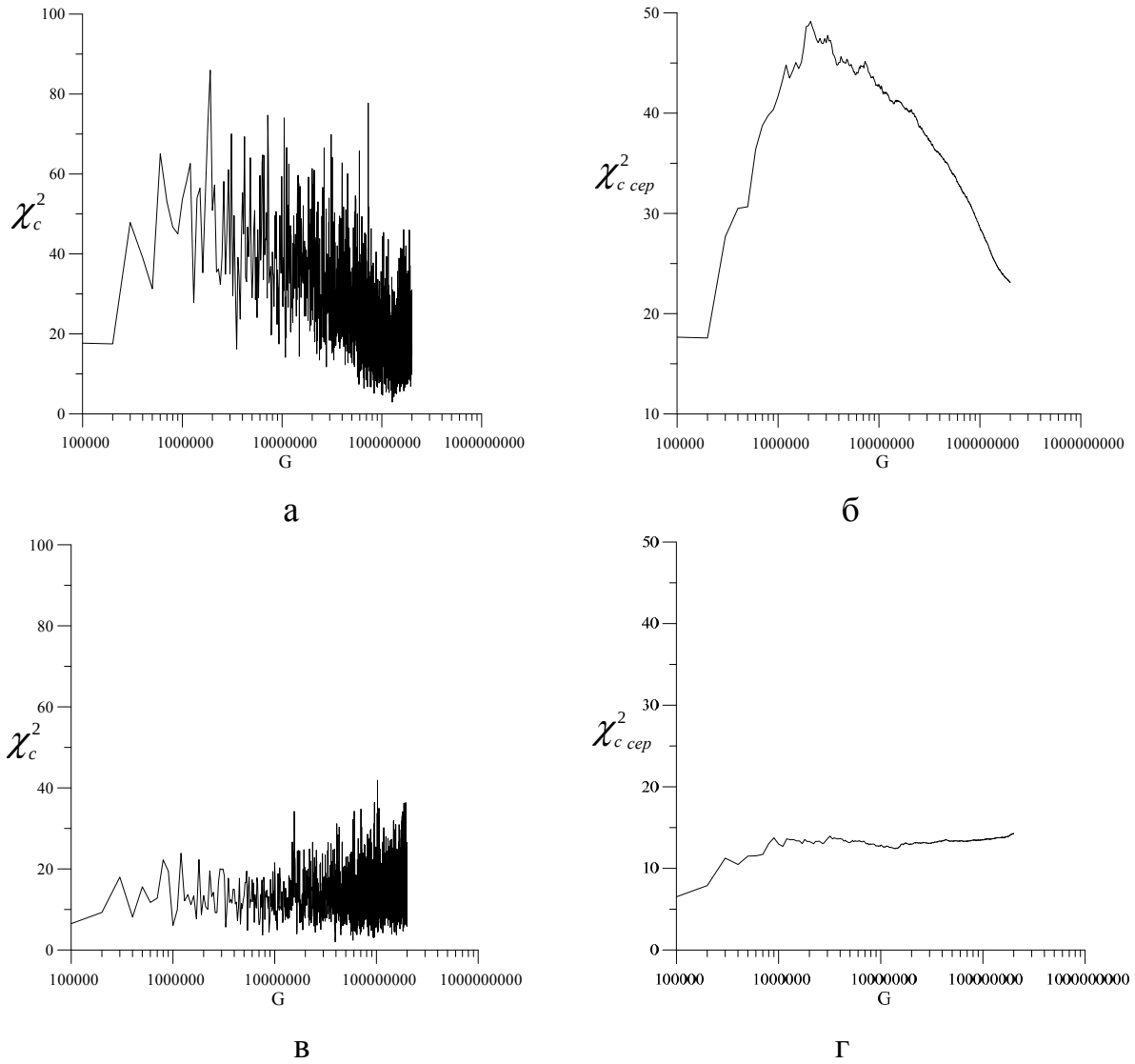


Рис. 2. Статистичні характеристики ГППП на основі РЗЛЗЗ

При рівні значимості $\alpha = 0{,}05$ і ступенів свободи $k = 12$ – $\chi^2_{кр} = 21{,}0$. З наведених графіків видно, що при $r = 10$ в основному виконується умова $\chi^2_c < \chi^2_{кр}$. Особливо чітко це простежується за залежністю $\chi^2_{c\,сер}$ від G. При подальшому збільшені значення r суттєвого покращення статистичних характеристик не спостерігається, натомість структура РЗЛЛЗ ускладнюється. Отже, за допомогою запропонованої методики можна визначати оптимальні параметри РЗЛЛЗ і діапазон значень керуючого коду G, в якому забезпечуються задовільні характеристики ГППП.

Було також проведено дослідження для випадку побудови РЗЛЗЗ на основі тих самих поліномів і степенів матриць, але при іншому їх типі – T_2. Дослідження показали, що тип матриці незначно впливає на характеристики вихідного сигналу ГППП.

Запропоновано структуру ГППП на основі модифікованого генератора Джіффі, в якому для формування псевдовипадкових чисел використовується мультиплексування розрядів двох РЗЛЗЗ за допомогою виходу одного з розрядів керуючого РЗЛЗЗ (рис. 3), що дозволило розширити діапазон значень керуючого коду, при якому досягаються задовільні статистичні характеристики вихідного сигналу.

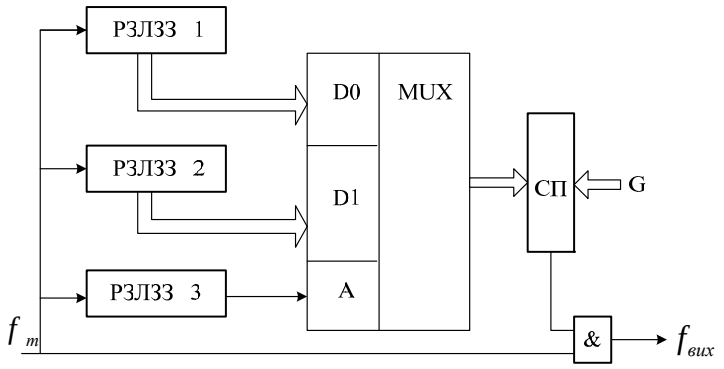


Рис. 3. Структурна схема ГППП на основі генератора Джіффі

РЗЛЗЗ 1, РЗЛЗЗ 2 і РЗЛЗЗ 3 побудовано згідно поліному $\Phi(x) = 1 \oplus x^{18} \oplus x^{25}$ типу матриці Т1 і степенів матриці $r = 10$, $r = 5$ і $r = 3$ відповідно.

Доведено можливість формування пуассонівської імпульсної послідовності (ППП) на основі псевдовипадкової бітової послідовності (ПБП). Оскільки для ППП характерні низькі значення середньої частоти повторення імпульсів, а ПБП характеризуються однаковою середньою частотою наявності і відсутності імпульсів в тактові моменти часу (однаковою частотою формування 1 і 0), формування ППП на основі ПБП може бути реалізоване відповідно до структури на рис. 4, до складу якої входять генератор ПБП (ГПБП) і керований кодом $К_Д$ дільник частоти (КДЧ).

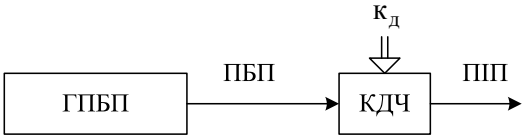
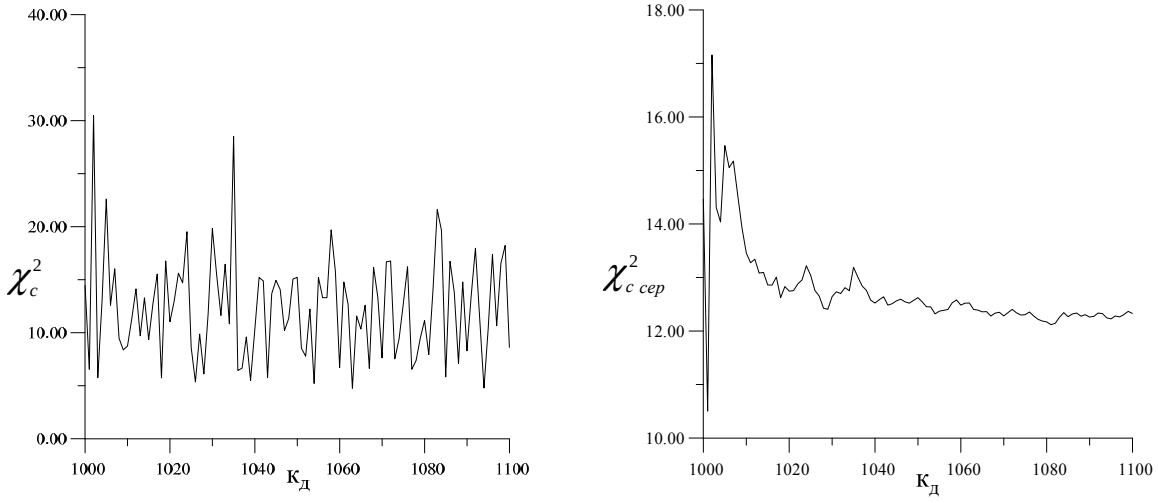


Рис. 4. Структурна схема формування ППП

Для побудови ГПБП вибрано генератор Голлманна, статистичні характеристики різних варіантів побудови якого було досліджено з допомогою тестів NIST. В результаті реалізовано варіант побудови на трьох однакових РЗЛЗЗ, кожен з яких відповідає поліному $\Phi(x) = 1 \oplus x^{18} \oplus x^{25}$, матриці Т1 і степені матриці $r = 1$.

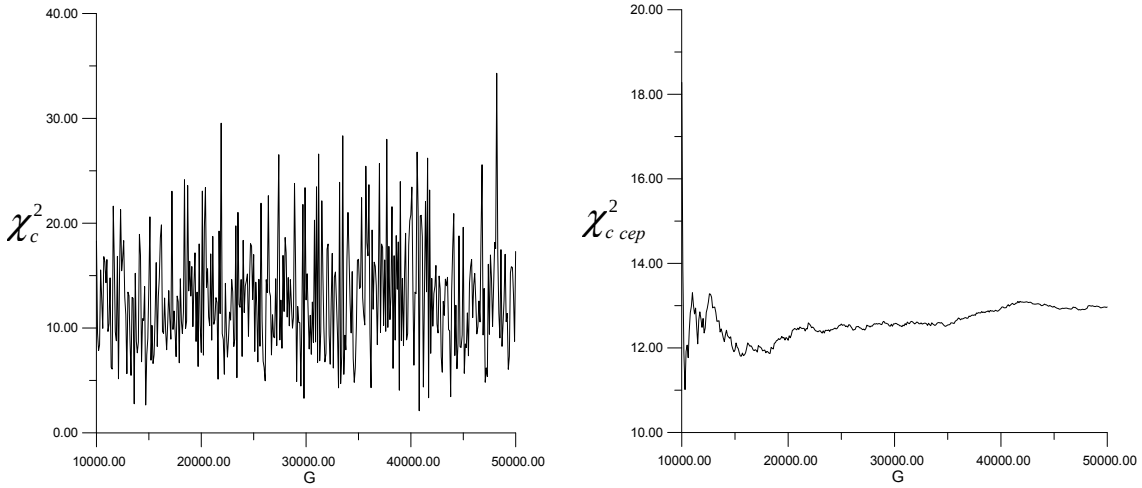


а б

Рис. 5. Статистичні характеристики ГППП на основі генератора Голлманна

На рис. 5 наведено результати оцінки якості ППП у випадку реалізації роботи КДЧ за розробленим алгоритмом, які підтверджують задовільну якість генератора, оскільки для більшості значень $К_Д$ виконується умова $\chi^2_c < \chi^2_{кр}$.

У четвертому розділі здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові ГПЧ на основі ЛКГ. При цьому для ЛКГ знайдено коефіцієнти рекурентних рівнянь, при яких ці характеристики є задовільними у визначеному діапазоні значень середніх частот вихідного сигналу. Для прикладу, на рис. 6 наведено результати аналізу при функціонуванні ЛКГ у відповідності до рівняння $X_{i+1} = (aX_i + b) \bmod m$ при a = 105, b = 12345, m = 2097152



а б

Рис. 6. Статистичні характеристики ГПІП на основі ЛКГ

Розроблено модифікований алгоритм і схеми генераторів Фібоначчі, які можуть використовуватись для формування керованого за частотою пуассонівського імпульсного потоку. Генератори Фібоначчі, відомі як пристрої для формування псевдовипадкових чисел і бітових послідовностей, в основному призначені для програмної реалізації. Це пояснюється складністю апаратної реалізації алгоритму $x_{j+1} = (x_j + x_{j-1}) \bmod m$ за умови, що m – просте або будь-яке число, що не дорівнює степені двійки. Якщо ж $m = 2^s$ (s – ціле додатне число) статистичні характеристики генератора є незадовільними.

Розроблено схему ГПІП на основі модифікованого генератора Фібоначчі зображена на рис. 7. Власне модифікований генератор Фібоначчі (МГФ) містить регістри Рг1 – Рг3, комбінаційний суматор КС і логічну схему ЛС.

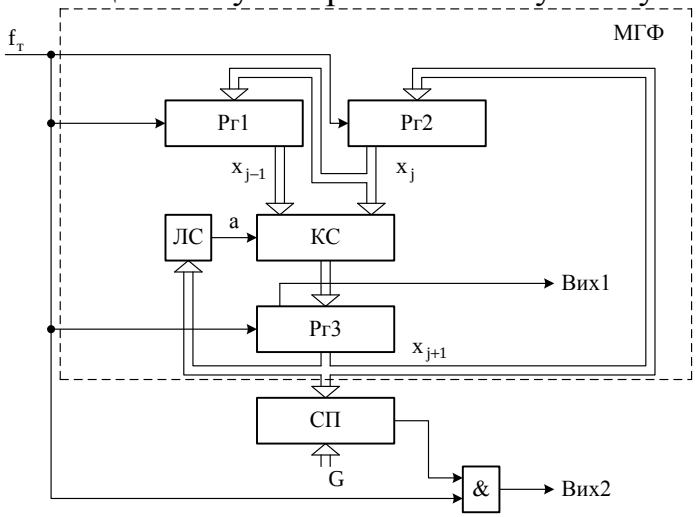


Рис. 7. ГПІП на основі модифікованого генератора Фібоначчі

На виходах МГФ формується послідовність псевдовипадкових чисел відповідно до виразу:

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

де $m = 2^s$, s – кількість двійкових розрядів структурних елементів. Значення змінної а визначається логічним рівнянням

$$a = a_0 \oplus a_1 \oplus a_2 \oplus \cdots \oplus a_z, \qquad (4)$$

де a_i (i=0,1,…,z) – значення двійкових розрядів числа в РгЗ. Кількість членів рівняння (4) може вибиратись у діапазоні 0 … m-1.

Бітова псевдовипадкова імпульсна послідовність формується на виході молодшого розряду регістрів РгЗ – Вихід 1, а пуассонівська імпульсна послідовність – на виході логічного елемента І – Вихід 2.

Кількість регістрів МГФ, що запам’ятовують попередні значення псевдовипадкових чисел, може бути різною, зокрема, при чотирьох регістрах алгоритм роботи є таким:

$$x_{j+1} = (x_j + x_{j-1} + x_{j-2} + x_{j-3} + a) \bmod m. \qquad (5)$$

За допомогою імітаційної моделі були досліджені періоди повторення МГФ (табл. 1).

Таблиця 1

Періоди повторення МГФ

Алгоритм роботи МГФ	m	Кількість членів рівняння (4)			
		0	4	8	16 (10 для $m = 2^{10}$)
Алгоритм (3)	2^{10}	3584	53536	8206435	727654100
	2^{20}	3670016	86933504	$>10^9$	$>10^9$
	2^{30}	$>10^9$	$>10^9$	$>10^9$	$>10^9$
Алгоритм (5)	2^{10}	15872	758763936	$>10^9$	$>10^9$
	2^{20}	16252928	$>10^9$	$>10^9$	$>10^9$
	2^{30}	$>10^9$	$>10^9$	$>10^9$	$>10^9$

Отже, збільшення періоду повторення МГФ досягається при: збільшенні кількості регістрів, що запам’ятовують попередні значення псевдовипадкових чисел; збільшенні кількості розрядів структурних елементів; збільшенні кількості членів рівняння, що реалізується логічною схемою ЛС.

Усі ці чинники також істотно впливають на статистичні характеристики бітової послідовності (Вихід 1), що було досліджено з допомогою статистичних тестів NIST. На рис. 8 наведено статистичні портрети бітової послідовності для варіанту реалізації МГФ за алгоритмом (5) при $m = 2^{20}$ і різній кількості членів рівняння (4): а – 0, б – 4, в – 8, г –16.

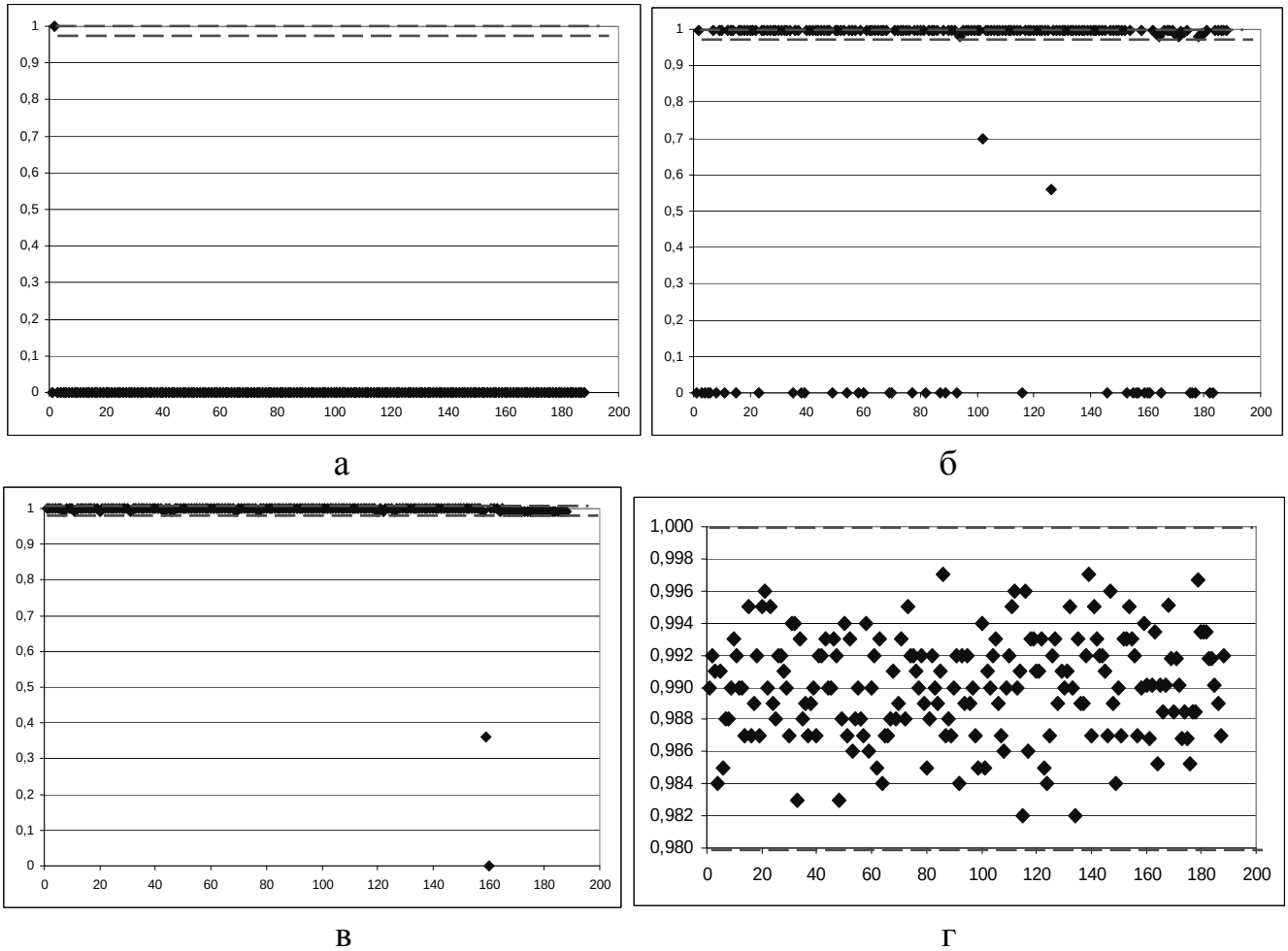


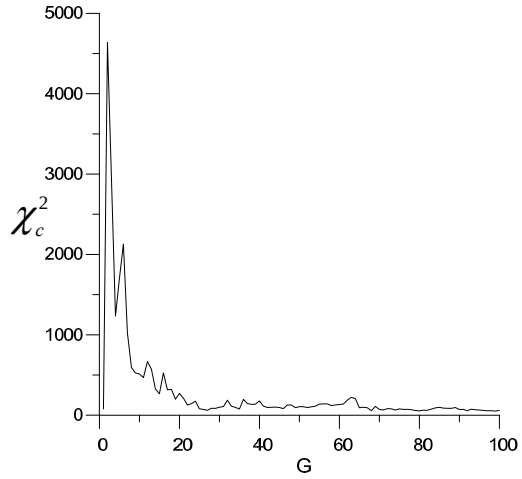
Рис. 8. Статистичні портрети бітової послідовності МГФ

Тут по осі абсцис відкладено номер тесту NIST, по осі ординат – імовірність проходження тесту. Тест вважається пройденим, якщо імовірність проходження тесту потрапить у межі від 0,98 до 1,00, в іншому випадку – тест не пройдено.

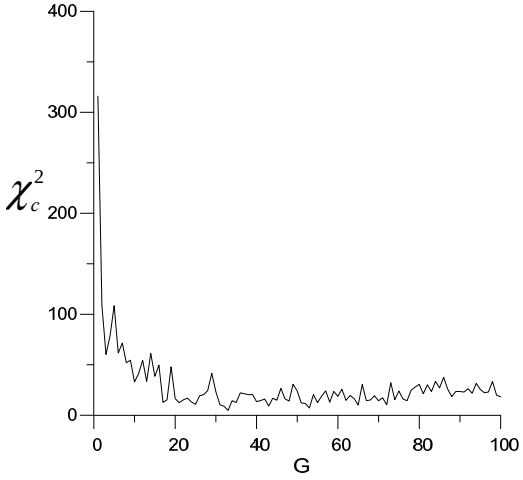
Результати дослідження статистичних характеристик вихідних сигналів ГППП, для деяких варіантів побудови МГФ, наведено на рис. 9. Тут позначення XOR=0, XOR=4 вказують на відповідну кількість членів рівняння (4). Варіант А відповідає алгоритму (3), а варіант Б – алгоритму (5).

За результатами проведених досліджень можна зробити висновок, що основним чинником, який дозволив істотно покращити статистичні характеристики ГППП, побудованого на основі МГФ, є введення до їх структури логічної схеми ЛС. Це пояснюється тим, що завдяки додаванню до молодшого розряду вихідного комбінаційного суматора МГФ біту, значення якого залежить від певної кількості розрядів вихідного регістру, формування усіх його розрядів наближається до випадкового процесу.

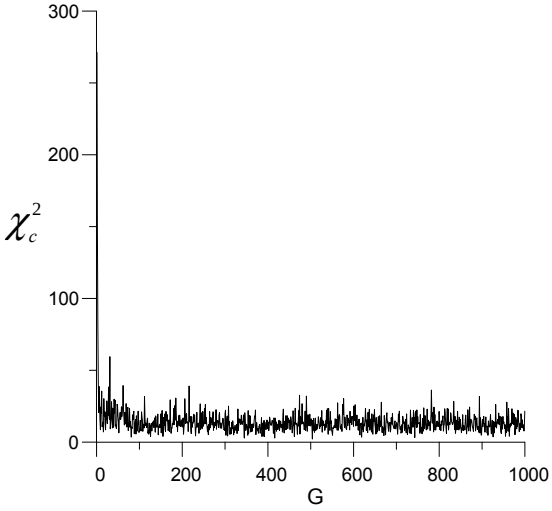
Дослідження МГФ з допомогою статистичних тестів NIST і дослідження ГППП, в основі якого є МГФ, з допомогою запропонованого способу визначення статистичних характеристик, дозволяють оптимізувати параметри генераторів і доводять те, що вказані методи оцінювання якості ГПЧ і ГППП доповнюють один одного.



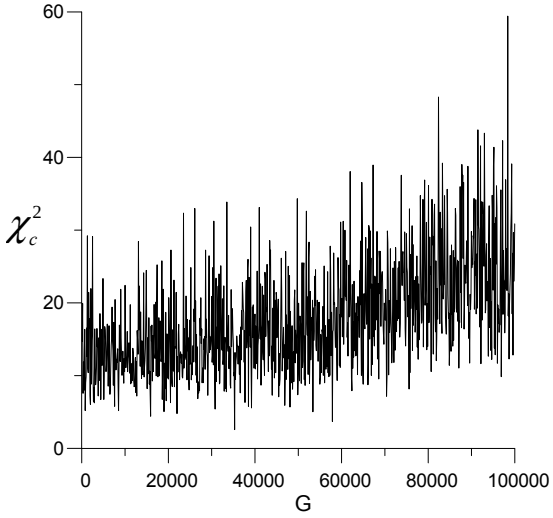
а



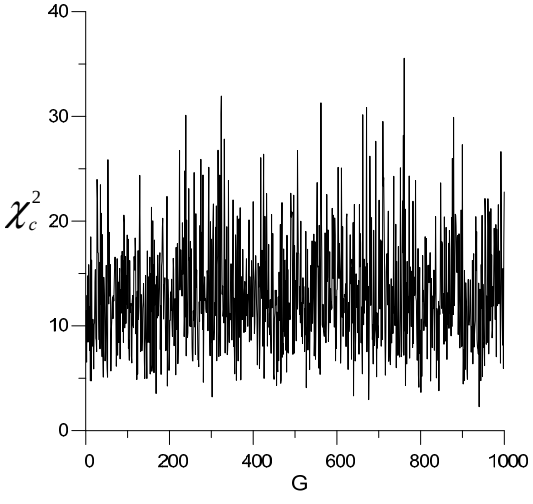
б



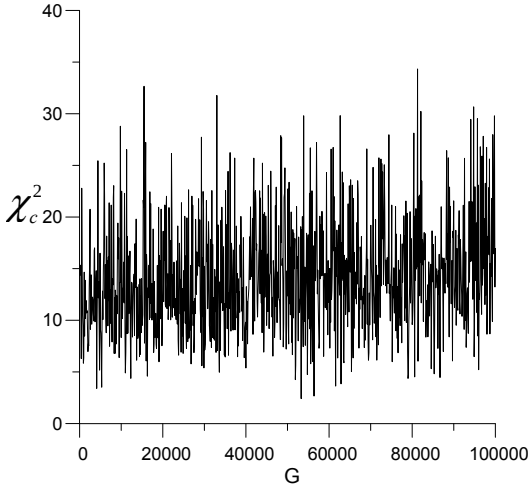
в



г



д



е

Рис. 9. Залежності χ_c^2 від керуючого коду G при: а – МГФ – варіант А, $m = 2^{10}$, XOR=0, G=1…100; б – МГФ – варіант А, $m = 2^{10}$, XOR=4, G=1…100; в – МГФ – варіант А, $m = 2^{20}$, XOR=4, G=1…1000; г – МГФ – варіант А, $m = 2^{20}$, XOR=4, G=100…100000; д – МГФ – варіант Б, $m = 2^{20}$, XOR=4, G=1…1000; е – МГФ – варіант Б, $m = 2^{20}$, XOR=4, G=100…100000.

У п'ятому розділі наведено методику проектування ГПІП із заданими характеристиками і результати реалізації генераторів у ПЛІС.

Перед початком проектування ГПІП, виходячи з прикладної задачі, що вирішується, необхідно задавати: статистичні характеристики вихідного сигналу; $f_{вих_{min}}$ – мінімальна середня частота вихідних імпульсів; $f_{вих_{max}}$ – максимальна середня частота вихідних імпульсів; $\Delta f_{вих}$ – крок зміни середньої частоти вихідних імпульсів. Статистичні характеристики можуть бути задані: періодом повторення псевдовипадкової послідовності $T_п$; критичним значенням $\chi^2_{кр}$ при вибраному рівні значимості α і числу степенів свободи r.

Порядок проектування є таким:

- визначається період повторення $T_п$ псевдовипадкових чисел на виході ГПЧ, а, отже і період повторення псевдовипадкової послідовності на виході ГПІП, виходячи з умов прикладної задачі і враховуючи те, що від цього істотно залежать статистичні характеристики вихідного сигналу;
- визначається тактова частота $f_т$, виходячи з можливостей елементної бази реалізації генератора, наприклад, можливостей ПЛІС;
- визначається максимально можливе число на виході ГПЧ:

$$X_{max} = T_п \cdot f_т; \qquad (6)$$

- вибирається структура ГПЧ, наприклад, на основі РЗЛЗЗ при необхідності забезпечення максимальної швидкодії;
- визначаються параметри структурних елементів ГПЧ;
- знаходяться уточнене значення X'_{max} виходячи з умови $X'_{max} \geq X_{max}$ і визначається значення $\Delta f'_{вих} = \frac{1}{X'_{max}} f_т$;
- створюється імітаційна модель роботи ГПЧ і ГПІП в цілому;
- визначаються статистичні характеристики вихідного сигналу ГПІП, за допомогою запропонованої удосконаленої методики з використанням критерію Пірсона, у всьому діапазоні значень керуючого коду G_{min} - G_{max}, що відповідають діапазону середніх значень вихідних часто $f_{вих_{min}}$ - $f_{вих_{max}}$, де $f_{вих_{min}} = \frac{G_{min}}{X'_{min}} f_т$ і $f_{вих_{max}} = \frac{G_{max}}{X'_{max}} f_т$;
- визначаються діапазони G'_{min} - G'_{max} і $f'_{вих_{min}}$ - $f'_{вих_{max}}$, при яких для переважної більшості значень керуючого коду G виконується умова $\chi^2_с < \chi^2_{кр}$ при вибраному рівні значимості α і числі степенів свободи r;
- реалізується структура ГПІП з допомогою системи автоматизованого проектування ПЛІС і перевіряється її працездатність.

За допомогою системи автоматизованого проектування Foundation Series 4.1i фірми Xilinx здійснено імітаційне моделювання та проведено оцінювання основних технічних характеристик ГПІП на базі генератора Фібоначчі. Результати подано в табл. 2, 3. Тут варіант А відповідає алгоритму (3), а варіант Б – алгоритму (5).

Таблиця 2

Технічні характеристики ГППП на основі МГФ (Варіант А)

Кількість розрядів ГППП	2^{10}	2^{20}	2^{30}
Період повторення	53536	86933504	$>10^9$
Мінімальний період тактових імпульсів	9,7 нс	14,1 нс	13,3 нс
Максимальна частота тактових імпульсів $f_{т_{max}}$	51,5 МГц	35,4 МГц	37,6 МГц
Діапазон вихідних частот $f'_{вих_{min}} - f'_{вих_{max}}$	0,5 МГц – 5,1 МГц	337,6 Гц – 1,01 МГц	3,5 Гц – 3,76 МГц
Крок зміни середньої частоти вихідних імпульсів $\Delta f_{вих}$	50 кГц	33,76 Гц	0,035 Гц
$\chi^2_{с\,сер}$	≤ 14	≤ 14	≤ 18

Таблиця 3

Технічні характеристики ГППП на основі МГФ (Варіант Б)

Кількість розрядів ГППП	2^{10}	2^{20}	2^{30}
Період повторення	758763936	$>10^9$	$>10^9$
Мінімальний період тактових імпульсів	10,6 нс	14,1 нс	13,4 нс
Максимальна частота тактових імпульсів $f_{т_{max}}$	47,2 МГц	35,4 МГц	37,7 МГц
Діапазон вихідних частот $f'_{вих_{min}} - f'_{вих_{max}}$	0,46 МГц – 4,7 МГц	337,6 Гц – 1,01 МГц	3,51 Гц – 3,77 МГц
Крок зміни середньої частоти вихідних імпульсів $\Delta f_{вих}$	46 кГц	33,76 Гц	0,035 Гц
$\chi^2_{с\,сер}$	≤ 14	≤ 14	≤ 18

При проектуванні ГППП, що використовуються для імітації вихідних сигналів дозиметричних детекторів (ДД), необхідно виходити з таких міркувань. Якщо не враховувати мертвий час ДД, що працюють в імпульсному режимі, імпульсний потік на їх виході підпорядковується пуассонівському закону розподілу. У випадку використання ДД для реєстрації гамма випромінювання, зв'язок між потужністю експозиційної дози (ПЕД) – Р і середньою частотою вихідних імпульсів детекторів визначається виразом

$$f_{вих} = P \cdot \gamma, \qquad (7)$$

де γ – чутливість ДД. Звідси слідує:

$$P_{min} = \frac{f'_{вих_{min}}}{\gamma},\ P_{max} = \frac{f'_{вих_{max}}}{\gamma},\ \Delta P = \frac{\Delta f'_{вих}}{\gamma}. \qquad (8)$$

У табл. 4 наведено результати оцінювання основних технічних характеристик генераторів при імітації вихідного сигналу дозиметричного детектора, які підтверджують можливість практичного використання розроблених ГППП при проектуванні і тестуванні дозиметричних пристроїв. Характеристики були обчислені для типової чутливості дозиметричних детекторів Гейгера – Мюллера - $\gamma = 0.02 \frac{Гц}{мкР/год}$.

Таблиця 4

Вид генератора	Модифікований генератор Джіффі	МГФ (Варіант А)	МГФ (Варіант Б)
P_{min}	515 мкР/год	175 мкР/год	175,5 мкР/год
P_{max}	1540 мР/год	188 Р/год	188,5 Р/год
ΔP	51 мкР/год	1,75 мкР/год	1,75 мкР/год

ВИСНОВКИ

У дисертаційній роботі наведено теоретичне узагальнення і нове вирішення наукового завдання покращення статистичних характеристик вихідних сигналів ГПІП, що дозволило комплексно покращити їх параметри.

При цьому отримано такі наукові та практичні результати:

1. В результаті аналізу існуючих типів ГПІП показано, що найбільш вдалою для апаратної реалізації є структура, до складу якої входять ГПЧ і схема порівняння, оскільки така структура забезпечує можливість оперативного керування середньою частотою вихідних імпульсів. При цьому основні характеристики такого генератора (період повторення, швидкодія, статистичні характеристики) залежать від способу побудови ГПЧ;
2. За результатами аналізу та досліджень визначено, що існує необхідність пошуку нових структур базових ГПЧ чи оптимізації параметрів уже існуючих з метою побудови на їх основі ГПІП з покращеними характеристиками; також визначено, що методи оцінювання якості ГПІП, що використовуються на даний час не розраховані на визначення статистичних характеристик у всьому діапазоні значень середніх частот вихідного сигналу;
3. Запропоновано спосіб визначення статистичних характеристик вихідних сигналів ГПІП, що ґрунтується на розбитті потоку вхідних тактових імпульсів на групи, кількість імпульсів в яких залежить від керуючого коду і відповідає однаковій середній кількості вихідних імпульсів, з подальшим використанням критерію Пірсона. На відміну від існуючих способів оцінки якості ГПІП, він дає можливість оцінити статистичні характеристики ГПІП у всьому діапазоні значень середніх частот вихідного сигналу;
4. Запропоновано спрощену методику дослідження статистичних характеристик вихідних сигналів ГПІП, що ґрунтується на використанні інтервальних імовірнісних характеристик;
5. Ефективність запропонованих методів оцінювання якості ГПІП доведена при її застосуванні для різних варіантів побудови базових ГПЧ;
6. З використанням запропонованого способу оцінки якості здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові ГПЧ на основі РЗЛЗЗ. При цьому для РЗЛЗЗ визначено твірні поліноми, типи і степені матриці, при яких ці характеристики є задовільними в робочому діапазоні значень середніх частот вихідного сигналу;
7. Запропоновано структуру ГПІП на основі модифікованого генератора Джіффі, в якому, для формування псевдовипадкових чисел використовується мультиплексування розрядів ГПЧ на основі РЗЛЗЗ за допомогою виходу одного з розрядів керуючого РЗЛЗЗ, що дозволило мінімум у 3 рази розширити діапазон значень керуючого коду, при якому досягаються задовільні статистичні характеристики вихідного сигналу;
8. Доведено можливість формування пуассонівської імпульсної послідовності на основі псевдовипадкової бітової послідовності, зокрема, при формуванні останньої з допомогою генератора Голлманна;
9. З використанням запропонованого способу оцінювання якості здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові ГПЧ на

основі ЛКГ. При цьому для ЛКГ знайдено коефіцієнти рекурентних рівнянь, при яких ці характеристики є задовільними в робочому діапазоні значень середніх частот вихідного сигналу;

10. Запропоновано спосіб побудови модифікованого адитивного генератора Фібоначчі, в якому введення додаткової складової в процес додавання, дає змогу формувати псевдовипадкові числа за модулем, що дорівнює степені двійки, і тим самим істотно спрощує його апаратну реалізацію у порівнянні з відомими рішеннями, при збереженні високих статистичних характеристик ГПІП, побудованих на його основі. При цьому період повторення псевдовипадкової послідовності збільшується на кілька порядків у порівнянні з ГПІП на основі класичного генератора Фібоначчі, наприклад, у 15 разів при застосуванні логічної схеми з трьох логічних функцій і у 2290 раз – з семи логічних функцій;

11. Досліджено модифікований генератор Фібоначчі з допомогою статистичних тестів NIST і досліджено ГПІП, з допомогою запропонованого способу визначення статистичних характеристик, що дозволило оптимізувати параметри останнього і довести те, що вказані методи оцінки якості ГПЧ і ГПІП є взаємодоповнюючі;

12. Результати реалізації в програмовних логічних інтегральних середовищах модифікованих генераторів Фібоначчі і Джіффі підтвердили практичне значення теоретичних розробок ГПІП;

13. Розроблені ГПІП використовуються для імітації вихідних сигналів дозиметричних детекторів при проектуванні і тестуванні дозиметричних пристроїв, що підтверджено актом впровадження.

Основний зміст дисертації опубліковано у наукових працях:

1 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. /Автором запропоновано методику на основі критерію Пірсона, яка може ефективно застосовуватись для дослідження та оцінювання параметрів вихідного сигналу будь-якого генераторів пуассонівської імпульсної послідовності на відповідність пуассонівському закону розподілу./

2 Костів Ю.М. Методика оптимізації параметрів генераторів пуассонівських імпульсних послідовностей побудованих на основі лінійних конгруентних генераторів / Ю.М. Костів, В.М. Максимович, М.М. Мандрона, О.І. Гарасимчук // Науковий вісник НЛТУ України: збірник науково-технічних праць. – Львів : РВВ НЛТУ України. – 2013. – Вип. 23.11. – С. 322-328. /Автором подано результати моделювання генераторів пуассонівських імпульсних послідовностей з різними параметрами лінійного конгруентного генератора. /

3 Костів Ю.М. Дослідження впливу параметрів генератора Голлманна на статистичні характеристики вихідного сигналу / М.М. Мандрона, В.М. Максимович, Ю.М. Костів, О.І. Гарасимчук // Вісник Кременчуцького національного університету імені Михайла Остроградського. – Кременчук: КрНУ. – 2013. – Випуск 4 (81). – С. 98-103. / Автором виконано оцінку якості статистичних характеристик за допомогою набору тестів NIST. Побудовано статистичні портрети генераторів псевдовипадкових послідовностей з використанням довірчого інтервалу. Здійснено підрахунок

кількості структурних елементів./

4 Костів Ю.М. Апаратна реалізація і дослідження модифікованих генераторів Фібоначчі / Ю.М. Костів, В.М. Максимович, О.І. Гарасимчук, М.М. Мандрона // Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2013. – № 29. С. – 167-174. / Автором запропоновано структурні схеми модифікованих генераторів Фібоначчі, що можуть використовуватись для формування псевдовипадкової бітової послідовності і керованою по частоті пуасанівської імпульсної послідовності. Досліджені їхні статистичні характеристики. /

5 Костів Ю.М. Визначення оптимальних параметрів генератора Голлманна за допомогою статистичних тестів NIST / Ю.М. Костів, В.М. Максимович, О.І. Гарасимчук, Я.Р. Совин, М.М. Мандрона // Вісник Національного університету "Львівська політехніка" - "Автоматика, вимірювання та керування", № 753, 2013. – С. 57-67. / Автором представлені результати дослідження генератора Голлманна при різній кількості базових генераторів М-послідовностей і різній степені їх поліномів, що проводилось з використанням статистичних тестів NIST. /

6 Костів Ю. Використання статистичних тестів НІСТ США для дослідження генераторів М – послідовностей / Ю. Костів, В. Максимович, М. Мандрона, Ю. Рибак // Вісник Національного університету "Львівська політехніка" - "Автоматика, вимірювання та керування", № 741, 2012. – С. 82-87. / Автором сформульовані вимоги до генераторів псевдовипадкових імпульсних послідовностей при їх використанні в криптографії та для імітації вихідних сигналів дозиметричних детекторів. Представлені результати тестування п'яти генераторів М – послідовності. /

7 Костів Ю.М. Порівняльний аналіз статистичних характеристик різних типів генераторів пуассонівських імпульсних послідовностей / В.М. Максимович, Ю.М. Костів, А.В. Петришин // Комп'ютерні технології друкарства : збірник наукових праць. – Львів : Вид-во Української академії друкарства. – 2012. – №27, – С.170-175. / Автором проведено аналіз статистичних характеристик двох типів генераторів пуассонівської імпульсної послідовності – з використанням генератора М-послідовностей і з використанням функції random мови програмування Delphi. /

8 Костів Ю.М. Оптимізація параметрів генератора М-послідовностей як структурного елемента генератора пуассонівської імпульсної послідовності / В.М. Максимович, О.І. Гарасимчук, Ю.М. Костів. // Вісник Національного університету "Львівська політехніка" - "Автоматика, вимірювання та керування", № 695, 2011. – С. 46-51. / Автором досліджено статистичні характеристики генератора пуассонівської імпульсної послідовності, побудованого на основі генератора М-послідовності. Дослідження проводились для різних типів і степенів матриць, що задають спосіб формування зворотних зв'язків і формують їх конфігурацію у відповідності з рівнянням функціонування генератора М-послідовностей. /

9 Костів Ю.М. Оцінка ефективності систем захисту інформації / О.І. Гарасимчук, Ю.М. Костів // Вісник Кременчуцького національного університету. – Кременчук: КрНУ. – 2011. - Випуск № 1/2011 (66) (частина 1). - С. 16-20. / Автором розглянуто питання оцінювання ефективності систем захисту інформації, основні підходи та методи такого оцінювання, їх переваги та недоліки. /

10 Костів Ю.М. Оцінка якості генератора Голлманна реалізованого на основі

модифікованих генераторів М – послідовностей / О.І. Гарасимчук, Ю.М. Костів, Т.Г. Паршенко // Системи обробки інформації. Вісник Харківського університету повітряних сил ім. Івана Кожедуба. – Харків. – 2010. - № 6 (87). – С.35-38. / Автором за допомогою імітаційного моделювання досліджені характеристики псевдовипадкової імпульсної послідовності на виході генератора Голлманна реалізованого на основі різних типів базових генераторів М-послідовностей. Дослідження проводились в результаті зміни кількості базових генераторів М-послідовностей, основних принципів їх реалізації, та послідовності включення в загальну схему генератора. Оцінка ефективності здійснювалась автором на основі обраної групи відомих статистичних тестів. /

11 Yuriy Kostiv. Optimization of parameters related to generator Dzhiffi structural elements / Yuriy Kostiv, Oleg Harasymchuk // The Second International Conference on Automatic Control and Information Technology 2013 (ICACIT'13), 7-8 December 2013: - Cracow, Poland, 2013.

12 Kostiv Yu. Examination of optimal settings for a Gollman generator / Yu. Kostiv, M. Mandrona, V. Maksymovych, O. Harasymchuk, Yu. Malynovskiy // Proceedings of the 6th International Conference of Young Scientists «Computer Science and Engineering 2013» (CSE-2013), November 21–23, 2013, Lviv. – p. 70-71.

13 Костів Ю. Дослідження генератора Голлмана за допомогою статистичних тестів NIST / Ю. Костів, В. Максимович, О. Гарасимчук, М. Мандрона // Матеріали II-ої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем», 30 травня - 01 червня 2013 р. – Львів. – с.88-89.

14 Костів Ю. Використання статистичних тестів NIST STS для дослідження генераторів М-послідовностей / Ю. Костів, В. Максимович, М. Мандрона, Ю. Рибак // Матеріали І-ої Міжнародної науково-технічної конференції “Захист інформації і безпека інформаційних систем”, 31 травня - 01 червня 2012 р. – Львів. – с. 118-119.

15 Костів Ю.М. Способи покращення параметрів модифікованого генератора Голлманна / В. Максимович, Ю. Костів // Матеріали III Міжнародної конференції молодих вчених «Комп’ютерні науки та інженерія - 2009» (CSE-2009), Національний університет «Львівська політехніка», 14-16 травня 2009р., – Львів. – с. 71-72.

16 Костів Ю.М. Дослідження параметрів генератора Голлманна / Ю.М. Костів, В.М. Максимович // Міжнародна науково-практична конференція «Сучасні засоби та технології розроблення інформаційних систем», Збірник наукових статей, ХНЕУ, 20-21 листопада 2008р., – Харків, с. 54.

17 Костів Ю. М. Дослідження параметрів модифікованого генератора Джіффі / В.Б. Дудикевич, В.М. Максимович, Ю.М. Костів // І міжнародна науково-практична конференція «Безпека та захист інформації в інформаційних і телекомунікаційних системах». Збірник наукових статей, ХНЕУ, 28-29 травня 2008 р., – Харків. - №6, - с. 74-76.

АНОТАЦІЯ

Костів Ю.М. Генератори пуассонівських імпульсних послідовностей з покращеними характеристиками – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти. – Національний університет „Львівська політехніка”, Міністерство освіти і науки України. – Львів, 2014.

Дисертаційна робота присвячена розробленню генераторів пуассонівських імпульсних послідовностей з покращеними характеристиками.

Запропоновано нові способи визначення статистичних характеристик вихідних сигналів генераторів пуассонівських імпульсних послідовностей (ГПІП), що ґрунтуються на використанні інтервальних імовірнісних характеристик та критерію Пірсона, які дають можливість здійснювати оцінювання у всьому діапазоні значень середніх частот вихідного сигналу.

Здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові генераторів псевдовипадкових чисел (ГПЧ), що є в структурі ГПІП, на основі регістрів зсуву з лінійними зворотними зв'язками. Запропоновано структуру ГПІП на основі модифікованого генератора Джіффі, що дозволило розширити робочий діапазон значень керуючого коду. Доведено можливість формування пуассонівської імпульсної послідовності на основі псевдовипадкової бітової послідовності.

Здійснено аналіз статистичних характеристик вихідних сигналів ГПІП при побудові ГПЧ на основі лінійних конгруентних генераторів. Запропоновано модифікований алгоритм і схеми генераторів Фібоначчі, які можуть використовуватись для формування керованого за частотою пуассонівського імпульсного потоку і забезпечують просту апаратну реалізацію.

Розроблено методику проектування ГПІП із заданими характеристиками і наведені результати реалізації таких генераторів в програмовних логічних інтегральних середовищах.

Ключові слова: генератори пуассонівських імпульсних послідовностей, модифікований адитивний генератор Фібоначчі, критерій Пірсона, генератор Джіффі, генератор Голлманна, генератори псевдовипадкових чисел.

АННОТАЦИЯ

Костив Ю.М. Генераторы пуассоновских импульсных последовательностей с улучшенными характеристиками – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Национальный университет „Львовская политехника", Министерство образования и науки Украины. – Львов, 2014.

Диссертационная работа посвящена разработке генераторов пуассоновских импульсных последовательностей с улучшенными характеристиками.

Предложены новые способы определения статистических характеристик выходных сигналов генераторов пуассоновских импульсных последовательностей (ГПИП), основанные на использовании интервальных вероятностных характеристик и критерия Пирсона, которые дают возможность осуществлять оценку во всем диапазоне значений средних частот выходного сигнала.

Осуществлен анализ статистических характеристик выходных сигналов ГПИП при построении генераторов псевдослучайных чисел (ГПЧ), имеющихся в структуре ГПИП, на основе регистров сдвига с линейными обратными связями. Предложена структура ГПИП на основе модифицированного генератора Джиффи, что позволило расширить рабочий диапазон значений управляющего кода. Доказана возможность формирования пуассоновской импульсной последовательности на основе псевдослучайной битовой последовательности.

Доказана возможность формирования пуассоновским импульсной последовательности на основе псевдослучайной битовой последовательности, в частности, при формировании последней при помощи генератора Голлманна. Исследования проводились в результате изменения количества базовых генераторов на основе регистров сдвига с линейными обратными связями, основных принципов их реализации, и последовательности включения в общую схему генератора. При этом для регистров сдвига с линейными обратными связями найдены образующие полиномы, типы и степени матрицы, при которых эти характеристики являются удовлетворительными в рабочем диапазоне значений средних частот выходного сигнала.

Осуществлен анализ статистических характеристик выходных сигналов ГПИП при построении ГПЧ на основе линейных конгруэнтных генераторов. Предложен модифицированный алгоритм и схемы генераторов Фибоначчи, которые могут использоваться для формирования управляемого по частоте пуассоновского импульсного потока и обеспечивают простую аппаратную реализацию.

Разработана методика проектирования ГПИП с заданными характеристиками и приведены результаты проектирования таких генераторов на программируемых логических интегральных схемах.

Ключевые слова: генераторы пуассоновских импульсных последовательностей, модифицированный аддитивный генератор Фибоначчи, критерий Пирсона, генератор Джиффи, генератор Голлманна, генераторы псевдослучайных чисел.

SUMMARY

Kostiv Yu.M. Poisson pulse sequence generators with improved characteristics – Manuscript.

Ph.D. thesis on technical sciences in specialty 05.13.05 – computer systems and components. – Lviv Polytechnic National University, Ministry of Education and Science of Ukraine. – Lviv, 2014.

The thesis deals with the development of Poisson pulse sequence generators with improved characteristics.

Author proposed new methods of determining the statistical characteristics of source signal Poisson generator pulse sequences (PGPS), based on the use of interval probabilistic characteristics and Pearson criterion, which allow evaluating the entire range of midrange output values.

The analysis of the PGPS output signals statistical characteristics during the construction of pseudo-random number generators (PRNG) in the PGPS structure, based on shift registers with linear feedback, was carried out. The author proposed a PGPS structure, based on modified Geffe generator, which allowed to extend the working range of control code values, as well as proved the possibility of the Poisson pulse sequence formation based on pseudorandom bit sequence.

The statistical characteristics of the PGPS output signals during the PRNG construction based on linear congruent generators were analyzed. The author proposed a modified algorithm and Fibonacci generators circuits, that can be used to create a controlled frequency Poisson pulse flow and ensure simple hardware implementation.

Also a PGPS design method with specified characteristics was developed and the results of such generators design using programmable logic devices were presented.

Keywords: Poisson pulse sequence generators, modified additive Fibonacci generator, Pearson criterion, Geffe generator, Hollmann generator, pseudo-random number generators.