Міністерство освіти і науки України
Національний університет «Львівська політехніка»

Круліковський Олег Валерійович

УДК 621.391.01

СИНТЕЗ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ БАГАТОВИМІРНИХ НЕЛІНІЙНИХ ДИНАМІЧНИХ СИСТЕМ

05.12.13 – радіотехнічні пристрої та засоби телекомунікацій

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Львів – 2018

Дисертацією є рукопис.

Робота виконана в Чернівецькому національному університеті імені Юрія Федьковича Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Політанський Леонід Францович,
Чернівецький національний університет
імені Юрія Федьковича,
завідувач кафедри радіотехніки
та інформаційної безпеки.

Офіційні опоненти: доктор технічних наук, професор
Матвійчук Ярослав Миколайович,
Національний університет «Львівська політехніка»,
професор кафедри систем автоматизованого проектування;

доктор технічних наук, старший науковий співробітник
Наконечний Володимир Сергійович,
Київський національний університет імені Тараса Шевченка,
професор кафедри кібербезпеки та захисту інформації.

Захист відбудеться «02» березня 2018 р. о 15 годині на засіданні спеціалізованої вченої ради Д 35.052.10 у Національному університеті «Львівська політехніка» (79013, м. Львів, вул. С. Бандери, 12, ауд. 226 головного навчального корпусу).

З дисертацією можна ознайомитись у науковій бібліотеці Національного університету «Львівська політехніка» (79013, м. Львів, вул. Професорська, 1).

Автореферат розісланий «31» січня 2018 р.

Вчений секретар
спеціалізованої вченої ради І.В. Демидов

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У зв'язку з активним розвитком інформаційних технологій зростає багатогранність та складність проблем інформаційної безпеки, збільшуються обсяги передавання, оброблення та зберігання інформації з обмеженим доступом. Відомо, що найбільш ефективними засобами захисту конфіденційних даних є кодування та зашифрування. Однак постійне покращення методів і засобів криптоаналізу та радіорозвідки зумовлює систематичне підвищення вимог до комунікаційних систем. Сучасні телекомунікаційні мережі використовують відомі та добре вивчені сигнали (М-послідовності, коди Голда, послідовності Уолша, Баркера та ін.), які не можуть забезпечити необхідну структурну прихованість та конфеденційність процесу передавання інформації. Формування сигналів довільної ємності є актуальним науково-практичним завданням при розробленні нових радіотехнічних пристроїв. Підвищення вимог до кібербезпеки та електромагнітної сумісності вимагає розвитку нових областей дослідження та розробки генераторів сигналів з великою інформаційною ємністю.

Одним із перспективних напрямків досліджень є генератори випадкових (ГВП) та псевдовипадкових (ГПВП) послідовностей на основі нелінійних динамічних систем (НДС), спектральні і статистичні характеристики яких керуються параметрами компонентів їх електричних кіл.

Значний вклад у дослідження властивостей генераторів випадкових та псевдовипадкових послідовностей на базі нелінійних динамічних систем та розв'язання проблем їх застосування у радіотехнічних пристроях і засобах телекомунікацій належить зарубіжним і вітчизняним вченим Люпчо Коцареву, Рене Лоці, Джанлука Сетті, Матвійчуку Я.М., Скобелеву В.Г., Скобелеву В.В., Васюті К.С., Захарченко М.В., Костенко П.Ю. та іншим.

На сьогоднішній день запропоновано багато алгоритмів і методів побудови ГПВП і ГВП у яких використовуються дискретні одновимірні хаотичні системи. Проте нещодавно в роботах Васюти К.С. та інших показано, що послідовності, утворені за допомогою одновимірних хаотичних систем (логістичне, квадратичне, тентове відображення та відображення Чебишева) не забезпечують необхідного рівня прихованості передавання, оскільки можуть бути розкриті застосуванням специфічних методів нелінійного аналізу (BDS- статистики, рекурентного аналізу, фрактальних розмірностей).

Для побудови системи зв'язку необхідно використовувати два ідентичних генератори хаотичних коливань. Однак, внаслідок впливу теплових шумів та технологічних обмежень на прецизійність елементів електричних кіл, виникає проблема встановлення стійкої синхронізації. Синхронізація генераторів хаотичних коливань забезпечується при розкиді параметрів електричних компонентів, що не перевищує 1%. Реалізація ідентичних генераторів можлива в інтегральному виконанні з лазерною підгонкою на інтегральній мікросхемі. Тому технологічна складність забезпечення ідентичності рознесених генераторів хаотичних коливань обмежує їх застосування в системах зв'язку, однак НДС можуть бути використані в якості бази ГВП.

Використання сучасних програмованих логікових інтегральних схем (ПЛІС) уможливлює розроблення генераторів псевдовипадкових сигналів на основі

багатовимірних НДС із кільцевим зв'язком, що дає змогу мінімізувати вплив обмеження точності обчислень при розрахунках та отримувати послідовності довільної довжини при врахуванні значень кореляційної розмірності системи.

Науково-прикладним завданням, розв'язанню якого присвячена дисертаційна робота, є синтез та практична реалізація генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалася відповідно до наукового напряму кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича та в межах науково-дослідницьких робіт:

"Фізико-технологічні проблеми радіотехнічних пристроїв та засобів телекомунікацій і інформаційних технологій" (Держ. реєстр. №0111U000183, 2013-2015 рр.), а також "Методи та засоби передавання, оброблення і зберігання інформації в інфо-комунікаційних системах" (Держ. реєстр. №0116U001433, 2016-2017 рр.)

Мета і завдання дослідження. Метою дисертаційної роботи є аналіз та синтез генераторів великих ансамблів псевдовипадкових та випадкових послідовностей на основі нелінійних динамічних систем.

Для досягнення поставленої мети необхідно розв'язати наступні завдання:

1. Провести ретельний аналіз сучасного стану методів побудови ГПВП та ГВП на базі нелінійних динамічних систем.
2. Дослідити статистичні властивості часових рядів, генерованих логістичним відображенням.
3. Розробити генератори псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком.
4. Дослідити статистичні властивості часових рядів, що генеруються з використанням математичних моделей нелінійних динамічних систем на основі мемристивних структур при реалізації на ПЛІС.
5. Розробити схемотехнічне рішення для генераторів випадкових коливань на базі відображень Тратаса та Лоці із неперервною біфуркаційною діаграмою. Провести аналіз часових рядів, що генеруються системою Тратаса.
6. Провести аналіз перестановок пікселів на основі стандартного відображення Чирікова-Тейлора та розробити відображення для змішування пікселів в растрових зображеннях $N \times N$ розмірності з потужністю простору ключів $(N^2 - 1)!$.

Об'єктом досліджень є процес формування псевдовипадкових та випадкових послідовностей на базі нелінійних динамічних систем.

Предметом дослідження є генератори псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем для радіотехнічних та телекомунікаційних систем.

Методи дослідження. Під час розв'язання поставлених завдань у роботі використовувалися методи чисельного інтегрування систем нелінійних диференційних рівнянь, нелінійної динаміки (біфуркаційні діаграми, спектри показників Ляпунова, фазові портрети), методи теорії імовірності і випадкових

процесів та елементи криптоаналізу, методи рекурентного аналізу та елементи теорії алгоритмів і комбінаторики.

Наукова новизна отриманих результатів:

– Вперше запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком, що відрізняється від відомих використанням найменш значущих збалансованих бітів, що дало змогу формувати великі ансамблі послідовностей, які доцільно використовувати у радіотехнічних пристроях та засобах телекомунікацій;

– Вперше запропоновано метод збільшення періоду реалізацій хаотичних систем шляхом підвищення їх розмірності, який відрізняється від існуючих урахуванням кореляційної розмірності нелінійної динамічної системи та дає змогу передбачити середню тривалість періоду повторення послідовностей;

– Удосконалено метод генерування псевдохаотичних послідовностей на основі програмної реалізації математичних моделей мемристивних хаотичних систем, який відрізняється від існуючих обґрунтованим використанням чисельного методу інтегрування Ейлера, що дає змогу збільшити швидкість генерування цих послідовностей при збереженні однакової середньої довжини періоду повторення та статистичних характеристик;

– Удосконалено двовимірне відображення Чирікова шляхом введення додаткової нелінійності, що дало змогу збільшити потужність простору ключів перестановок від N^{N-1} до $(N^2-1)!$ для матриць розмірності $N \times N$.

Практичне значення одержаних результатів. При виконанні дисертаційної роботи отримано наступні практичні результати:

– Схемотехнічно реалізовано генератори випадкових сигналів на основі двовимірних відображень Лоці та Тратаса із кільцевим зв'язком, зі швидкістю генерування випадкових послідовностей 0,84 Мбіт/с для двовимірної системи з частотою тактового сигналу 30 кГц. Підвищення швидкодії може бути досягнуто за рахунок інтегрального виконання генератора, що уможливлює збільшення розмірності системи та її тактової частоти.

– Досліджено періодичність розв'язків логістичного відображення реалізованого на ПЛІС із використанням арифметики з фіксованою комою Q3.29. Показано, що потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів та становить $24797 \approx 2^{14}$. Зокрема, модифіковане багатовимірне відображення в якості бази генератора псевдовипадкових послідовностей реалізованого на ПЛІС забезпечує збільшення середнього значення періоду повторення з 2^{14} до 2^{73} при використанні шестивимірної модифікації логістичного відображення.

– Розроблено та реалізовано апаратні рішення на базі ПЛІС для генерування псевдовипадкових послідовностей зі швидкістю до 19,2 Гбіт/с чотирьохвимірними хаотичними системами. Розроблена структура генератора уможливлює формування псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв'язком довільної розмірності.

– Розроблено апаратне рішення методу генерування псевдо хаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури, що забезпечує незалежність середньої тривалості періоду повторення в межах

$10^6 \div 2 * 10^6$ ітерацій від кроку дискретизації, що становить $\Delta t = 0,0005 \div 0,02$ при умові використання арифметики з фіксованою комою Q8.16.

Отримані в дисертаційній роботі наукові та практичні результати використовуються для формування цифрових хаотичних послідовностей на базі програмованих логікових мікросхем, зокрема для передавання інформаційних сигналів у системах зв'язку (ПАТ «Укртелеком»), при дослідженнях процесів формування хаотичних коливань на базі мемристивних структур (ОКБ «Рута»), а також впроваджені в навчальний процес на кафедрі радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, що підтверджується відповідними актами впровадження.

Достовірність отриманих результатів підтверджується узгодженістю теоретичних розрахунків та результатів моделювання із експериментально отриманими даними.

Апробація результатів дисертаційної роботи. Основні результати дисертаційних досліджень були предметом обговорень на:

– наукових семінарах кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича;

– наукових семінарах дослідницької групи «Linear and Nonlinear Circuits & Systems» (Politecnico di Torino, Torino, Italy, 2015-2016);

– 18th «Mediterranean Electrotechnical Conference» (MELECON 2016), Limassol, Cyprus, 18-20 April 2016;

– XIII Inter. Conf. on «Modern Problems of Radio Engineering, Telecommunications and Computer Science» (TCSET'2016), Lviv-Slavske, 23-26 February, 2016;

– міжнародній науково практичній конференції «Проблеми інформатики та комп'ютерної техніки» (ПІКТ 2016), м. Чернівці, 21 - 24 травня 2016 року;

– міжнародній науково практичній конференції «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка» (НМІТФ-2016), м. Кременчуг, 26 - 28 травня 2016 року;

– міжнародній науково практичній конференції «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (PREDT -2016). – м. Чернівці, 3- 5 листопада 2016 року;

– міжнародній науково-практичній конференції «Обробка сигналів і негаусівських процесів – 2017» (ОСНП-2017). – м. Черкаси, 24-26 травня 2017 р.;

– ІІ міжнародній конференції з інформаційно-телекомунікаційних технологій та радіоелектроніки «УкрМіКо 2017».– м. Одеса, – 11-15 вересня 2017 року.

Структура та обсяг дисертації. Дисертація складається зі вступу, 5 розділів, загальних висновків, бібліографічного списку використаних джерел, 2 додатків. Загальний обсяг роботи становить 156 сторінок друкарського тексту, із них 7 сторінок вступу, 118 сторінок основного тексту, 73 рисунки, 16 таблиць, список використаних джерел зі 125 найменувань, 2 додатки на 5 сторінках.

Публікації. Результати дисертаційних досліджень опубліковані в 15 наукових працях, зокрема опубліковано 6 статей у наукових фахових виданнях [1-6] і здійснено 9 публікацій у збірниках матеріалів закордонних та всеукраїнських конференцій міжнародного рівня [7-15].

Особистий внесок здобувача. Всі результати дисертації, що виносяться на захист, отримані здобувачем особисто. У роботах, опублікованих у співавторстві, автору належать: [1] – дослідження динамічних режимів роботи системи Тратаса, аналіз часових рядів, генерованих багатовимірною системою Тратаса; [2] – проведення аналізу відображень для змішування пікселів в методах захисту растрових зображень; [3, 11, 13,14] – розроблення методів захисту зображень для систем технічного захисту інформації; [4,10] – аналіз дискретних хаотичних систем в якості бази ГПВП та формування вимог, яким повинні відповідати такі системи; [5] – розроблення ГПВП на базі багатовимірних відображень із кільцевим зв'язком, апаратна реалізація ГПВП на ПЛІС Altera Cyclone IV, тестування псевдовипадкових характеристик генерованих послідовностей; [6, 12] – розроблення методів генерування ПВП з урахуванням збалансованості бітів у бінарному представленні значень, генерованих гіперхаотичною системою Тратаса; [7, 9] – дослідження хаотичної системи на базі мемристивної структури, реалізація на ПЛІС математичної моделі з використанням методів Ейлера та Рунге-Кутти четвертого порядку, розроблення методу генерування ПВП, дослідження періодичності розв'язків; [8] – дослідження особливостей перестановок пікселів на базі дискретизованого відображення Чирікова; [15] – аналіз часових рядів, генерованих чотиривимірною системою Тратаса за допомогою рекурентних діаграм.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету, завдання, визначено об'єкт і предмет дослідження, представлено наукову новизну одержаних автором результатів та їх практичне значення, зазначено особистий внесок здобувача, а також дані щодо публікацій за темою дисертації та апробацій роботи.

У першому розділі приведено аналіз аспектів використання генераторів ПВП на основі НДС, висвітлено основні положення теорії НДС. Детально розглянуто властивості хаотичних систем, що обумовлюють переваги їх використання у системах передавання інформації.

Під детермінованим хаосом розуміють складні неперіодичні коливання, що породжуються НДС. При цьому нелінійність системи є необхідною, але недостатньою умовою для виникнення хаосу. Можливість застосування генераторів псевдовипадкових послідовностей на базі детермінованого хаосу в системах передавання інформації обумовлена існуванням методу їх відтворюваності.

Проаналізовано принципи побудови генераторів ПВП і наведено вимоги щодо їх використання в системах передавання інформації.

На основі аналізу літературних джерел за тематикою роботи сформульовано завдання дисертаційних досліджень.

Другий розділ присвячений питанням аналізу та синтезу ГПВП на основі НДС, з метою уможливлення їх застосування у пристроях формування та оброблення інформаційних сигналів.

Загальновідомо, що детермінований хаос має місце в аналогових системах. При реалізації систем генерування на базі ПЛІС втрачається «хаотичність» внаслідок зменшення множини можливих станів. Розв'язання проблеми повторюваності псевдохаосу можливе шляхом збільшення середньої довжини циклу

та тривалості перехідного процесу за рахунок підвищення прецизійності обчислень та введення псевдовипадкових періодичних збурень, а також переходом до багатовимірних систем. Розглянемо це на прикладі логістичного відображення, що задається ітераційною залежністю:

$$x_{n+1} = r x_n (1 - x_n), \tag{1}$$

де r — параметр керування, n – номер ітерації, x_{n+1} – змінна, яка може приймати значення з діапазону [0; 1]. У випадку, якщо тривалість циклу хаотичної системи становить одну ітерацію, то збурення з періодом повторення, більшим за середню тривалість перехідного процесу є недоцільними, оскільки при цьому має місце періодичне повторення частини однієї і тієї ж траєкторії. У результаті повторення колапсу системи (1) під впливом випадкового періодичного збурення через кожні 50 ітерацій (рис. 1) при реалізації у арифметиці Q12.9 має місце короткотривалий перехідний процес, після якого система колапсує або виходить на періодичну орбіту.

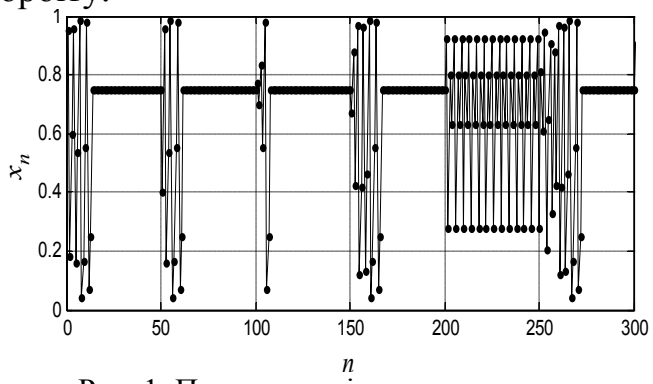


Рис. 1. Повторюваність колапсу при випадкових періодичних збуреннях через кожні 50 ітерацій

Особливістю хаотичних систем є дробове значення фрактальних розмірностей. Внаслідок відвідування їх траєкторіями областей фазового простору з різними частотами розподіл значень послідовностей, генерованих такими системами є нерівномірним. Розглянемо особивості бітового представлення чисел при розрахунках з фіксованою та плаваючою комою. Задамо послідовність ітерацій матрицею розмірності $n \times m$:

$$\begin{cases} l_{11} \; . \; l_{12} \; \ldots \; l_{1,\,m} \\ l_{21} \; . \; l_{22} \; \ldots \; l_{2,\,m} \\ \quad . \quad . \quad \ldots \quad . \\ l_{n,1} \; . \; l_{n,2} \; \ldots \; l_{n,\,m} \end{cases}, \tag{2}$$

де n – номер ітерації x_n, а m – порядковий номер біта в бінарному представленні дійсного числа.

Для кожного стовпця матриці (2) обчислюється кількість нулів “0” - N_0 та одиниць “1” - N_1, $(N_0 + N_1 = N)$. Залежність відносної різниці між кількостями «0» і «1» від номера двійкового символа у числі при реалізації логістичного відображення на ПЛІС приведено на рис. 2. Відхилення в пропорції «0» і «1» для значущих бітів обумовлене нерівномірним розподілом значень хаотичних коливань генерованих логістичним відображенням.

Під простором ключів у системах передавання інформації на базі нелінійних динамічних систем розуміють множину значень параметрів керування та початкових умов, за яких мають місце хаотичні режими. При зміні параметрів системи хаотичні коливання можуть переходити в періодичні, зокрема для логістичного рівняння вони матимуть місце при $r \geq 3{,}57$. З біфуркаційної діаграми

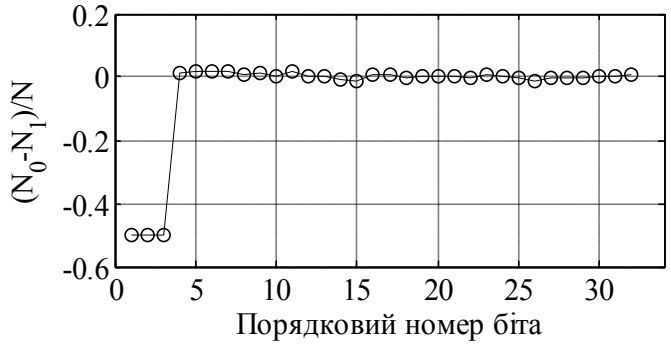


Рис. 2. Збалансованість послідовностей для логістичного рівняння при r = 3.999, за умов використання арифметики Q3.29.

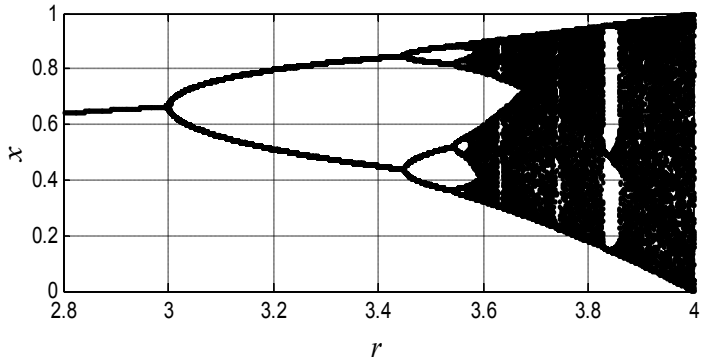


Рис. 3. Біфуркаційна діаграма (1).

(рис. 3) випливає, що при деяких значеннях параметру r існують вікна періодичності, внаслідок чого точна оцінка простору ключів унеможливлена. Тому при виборі хаотичних систем перевагу слід надавати таким, що характеризуються суцільною діаграмою біфуркацій без вікон періодичності. Використання всієї множини початкових умов з області притягування атрактора при виборі простору ключів є некоректним і призводить до неправильної оцінки його обсягу. Для системи (1) допустимі значення початкових умов належать діапазону (0, 1) і не залежать від значень параметру r.

Розмах хаотичних реалізацій після закінчення перехідного процесу не виходитиме за межі інтервалу $[x_{min}, x_{max}]$(рис 4). При зміні параметру r буде змінюватися розмах реалізацій та обсяг ключового простору початкових умов.

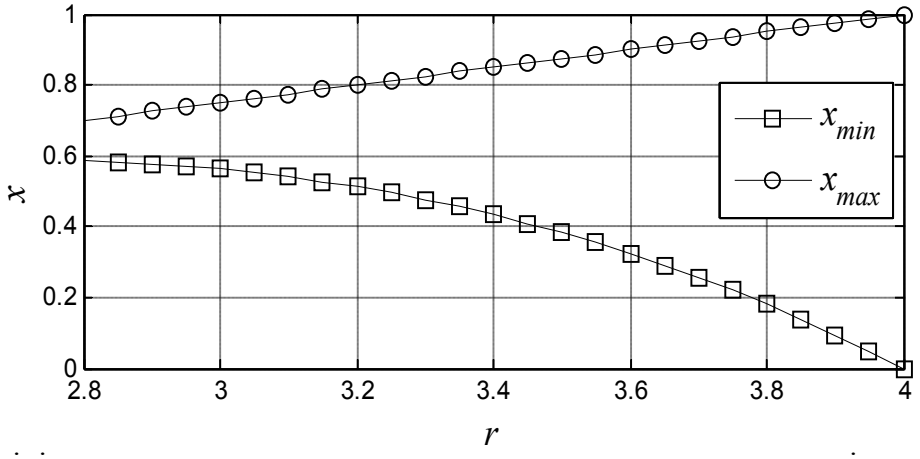


Рис. 4. Залежність мінімальних та максимальних значень хаотичних коливань, які реалізуються на основі логістичного рівняння від значень його параметра r.

Легко показати, що послідовність розв'язків системи (1) з довільними початковими умовами $x \in (0,1)$, в залежності від параметру керування r, обмежиться діапазоном $x \in \left[\frac{r^2}{4}\left(1-\frac{r}{4}\right), \frac{r}{4}\right]$. Залежність потужності множини значень хаотичних реалізацій від параметра керування системи ускладнює оцінювання надійності генератора псевдовипадкових послідовностей.

Слід зауважити, що при комп'ютерних обчисленнях різні початкові умови призводять до однакових циклів. Це означає, що при кодуванні великих обсягів інформації, початкові умови є слабшим ключем, ніж значення параметру керування.

Період повторення послідовностей, генерованих логістичним рівнянням (1) є суттєво меншим за максимально можливий. Для значення $r = 3{,}99$ після закінчення перехідного процесу при m = 32 кількість різних послідовностей, що можуть бути згенеровані системою (1) обмежена і не залежить від початкових умов. Максимальна довжина перехідного процесу становила 16775 ітерацій. Потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів і становить 24797 $\approx 2^{14}$ при використані арифметики із фіксованою комою Q3.29. Залежність потужності простору можливих станів системи від кількості ітерацій приведена на рис. 5.

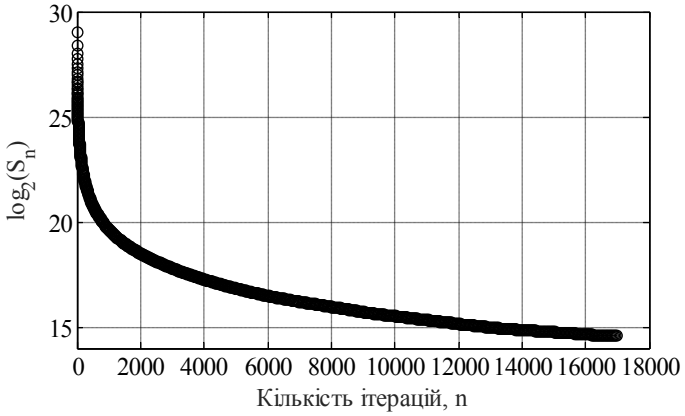


Рис. 5. Залежність потужності множини станів логістичного рівняння від кількості ітерацій

Використання багатовимірних систем для розв'язання проблеми циклічності є найбільш доцільним, оскільки середні тривалості циклу та перехідного процесу при виході траєкторії на цикл залежать від кореляційної розмірності d, наступним чином:

$$\langle L \rangle \sim \varepsilon^{-\frac{d}{2}}, \tag{3}$$

де $\langle L \rangle$ - середнє значення тривалості циклу, ε - точність обчислень, що становить 2^{-29} для арифметики з фіксованою комою Q3.29.

Із (3) випливає, що єдиним способом збільшення середньої тривалості циклу є збільшення кореляційної розмірності хаотичної системи, що не перевищує розмірності її фазового простору. Тому збільшення періоду повторення послідовності можливе шляхом збільшення розмірності фазового простору хаотичної системи.

Багатовимірне логістичне відображення із кільцевим зв'язком описується такою системою рівнянь:

$$\begin{cases} x_{n+1}^{(1)} = e * r * x_n^{(1)}(1 - x_n^{(1)}) + (1-e) * x_n^{(p)} \\ x_{n+1}^{(2)} = e * r * x_n^{(2)}(1 - x_n^{(2)}) + (1-e) * x_n^{(1)} \\ \cdots \\ x_{n+1}^{(p)} = e * r * x_n^{(p)}(1 - x_n^{(p)}) + (1-e) * x_n^{(p-1)} \end{cases}, \tag{4}$$

де p – розмірність системи, а e – коефіцієнт зв'язку.

Залежність значень кореляційної розмірності d від розмірності системи p на основі багатовимірного логістичного відображення з кільцевим зв'язком (4) приведено в табл. 1.

Табл. 1. Залежність кореляційної розмірності від розмірності фазового простору системи (4)

Розмірність системи, p	2	4	6	8	10	12	14	16	18	20
Кореляційна розмірність, d	1.75	3.5	5.06	6.23	7.86	8.88	9.97	11.41	12.42	14.47
Середнє значення тривалості періоду повторення $\langle L \rangle$ при $\varepsilon = 2^{-29}$	2^{25}	2^{50}	2^{73}	2^{90}	2^{113}	2^{128}	2^{144}	2^{165}	2^{179}	2^{209}

Хаотичними системами для яких можливе довільне збільшення їх розмірності є сімейство систем Лоці та гіперхаотична система Тратаса. Багатовимірне відображення Лоці із кільцевим зв'язком, в загальному випадку описується системою рівнянь:

$$\begin{cases} x_{n+1}^{(1)} = 1 - r_1 \left| x_n^{(1)} \right| + k_1 \left(\left| x_n^{(2)} \right| - (x_n^{(1)})^2 \right) \\ x_{n+1}^{(2)} = 1 - r_2 \left| x_n^{(2)} \right| + k_2 \left(\left| x_n^{(3)} \right| - (x_n^{(2)})^2 \right) \\ \qquad\qquad \dots \\ x_{n+1}^{(p)} = 1 - r_p \left| x_n^{(p)} \right| + k_p \left(\left| x_n^{(1)} \right| - (x_n^{(p)})^2 \right) \end{cases} \tag{5}$$

де r і k параметри керування, $r, k \in [1, 2]$, p – розмірність системи, $i = [1 \dots p]$, $\left| x_n^{(i)} \right|$ – абсолютне значення $x_n^{(i)}$. Для рівноймовірного та щільного відвідування усіх областей фазового простору траєкторіями $x_n^{(i)}$ необхідно використовувати наступний механізм рандомізації:

$$\begin{array}{ll} якщо\ 1 - r \left| x_n^{(i)} \right| + r \left(\left| x^{(i-1)} \right| - (x_n^{(i)})^2 \right) < -1 & тоді\ \ x_{n+1}^{(i)} = x_{n+1}^{(i)} + 2 \\ якщо\ 1 - r \left| x_n^{(i)} \right| + r \left(\left| x^{(i-1)} \right| - (x_n^{(i)})^2 \right) > 1 & тоді\ \ x_{n+1}^{(i)} = x_{n+1}^{(i)} - 2 \end{array}, \tag{6}$$

Такий механізм дозволяє, отримати рівномірний розподіл генерованих часових рядів (рис. 6).

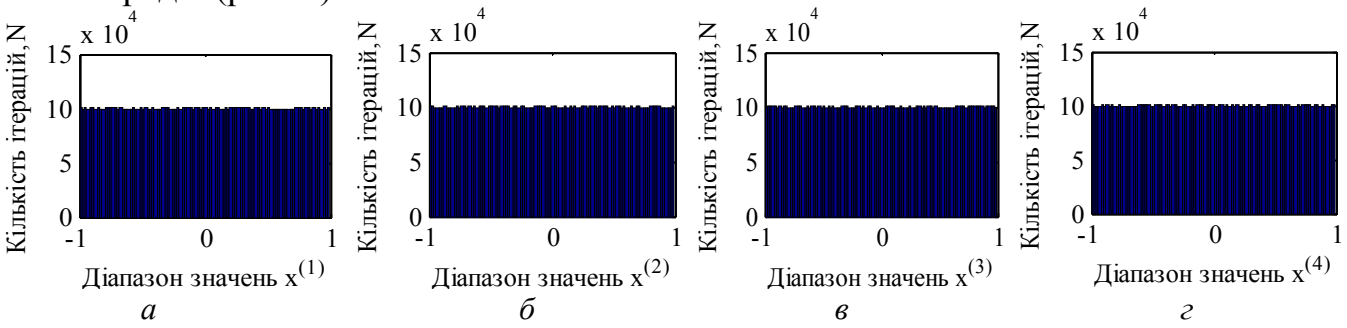


Рис. 6. Гістограма розподілу значень: *а* – канал $x^{(1)}$, *б* – канал $x^{(2)}$, *в* – канал $x^{(3)}$, *г* – канал $x^{(4)}$.

Із приведеної гістограми розподілу значень $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ і $x^{(4)}$ (рис. 6) випливає, що середнє значення кількості попадань в кожен із 100 піддіапазонів діапазону [-1, 1] становить $\sim 10^5$ для 10^7 ітерацій. Це є суттєвою перевагою, в порівнянні з іншими НДС з нерівномірним розподілом, оскільки їх атрактор сконцентрований тільки в деякій області фазового простору.

Для реалізації генераторів псевдовипадкових послідовностей з великими значеннями їх періоду використовувалися генератори послідовностей на ПЛІС блок-схема яких приведена на рис. 7.

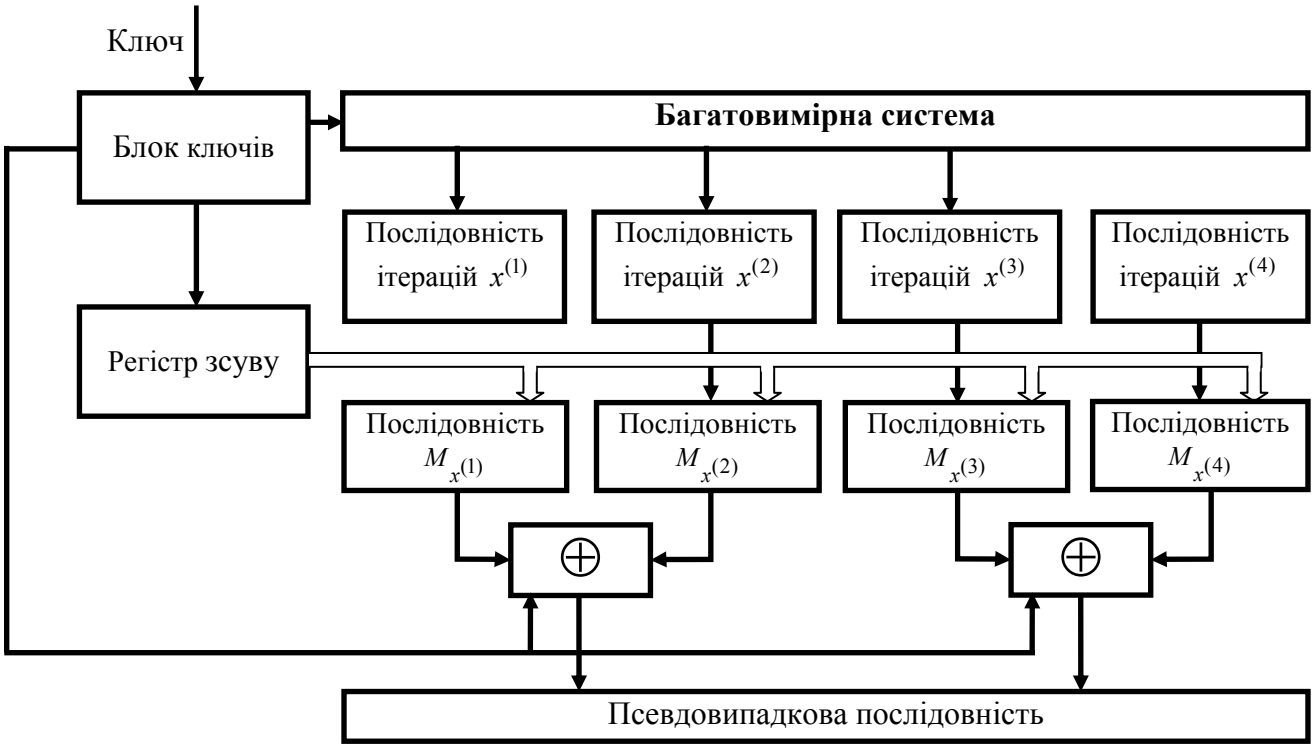


Рис. 7. Блок-схема генератора псевдовипадкових послідовностей на базі чотиривимірних відображень із кільцевим зв'язком

На вхід системи подається ключ, що складається зі значень параметрів системи, початкових умов хаотичної системи та значення параметрів регістра зсуву.

Розв'язки рівнянь системи (4) при $p = 4$ формують чотири різні хаотичні послідовності. Із кожної ітерації вибираються біти з діапазону [0; 31]. Таким чином, формуються чотири блоки по q біт (де q - довжина послідовності $M_{x^{(p)}}$). За одну ітерацію можна отримати послідовність довжиною $4q$ біт. В блоках додавання за модулем 2 виконується побітове додавання наступним чином:

$$\begin{cases} M_{x^{(1)}} \oplus M_{x^{(2)}} \\ M_{x^{(3)}} \oplus M_{x^{(4)}} \end{cases} \tag{7}$$

В результаті додавання отримуємо псевдовипадкову послідовність виду $((M_{x^{(1)}} \oplus M_{x^{(2)}}),\ (M_{x^{(3)}} \oplus M_{x^{(4)}}))$ довжиною $2q$ біт. Регістр зсуву та XOR- блок призначені для ускладнення розкриття параметрів відображення та поточного стану генератора.

У третьому розділі роботи представлено апаратну реалізацію генераторів псевдовипадкових послідовностей на базі багатовимірних хаотичних систем та результати дослідження генерованих ними послідовностей на відповідність критеріям псевдовипадковості згідно набору статистичних тестів NIST. Для генерування послідовностей використана система Лоці (5) зі значеннями p = 4. ГПВП реалізовано на ПЛІС *Altera Cyclone IV EP4CE115*. Simulink блок-схема для обчислення $x_{n+1}^{(1)}$ приведена на рис. 8. Оператори умови (6) реалізовано на базі двох компараторів. У випадку якщо $x_{n+1} > 1$, то сигнал керування ініціалізує підсистему 1, що віднімає 2 від псевдовипадкового значення, а якщо $x_{n+1} < -1$, то сигнал керування ініціалізує підсистему 2, що додає 2 до значення сигналу x_{n+1}.

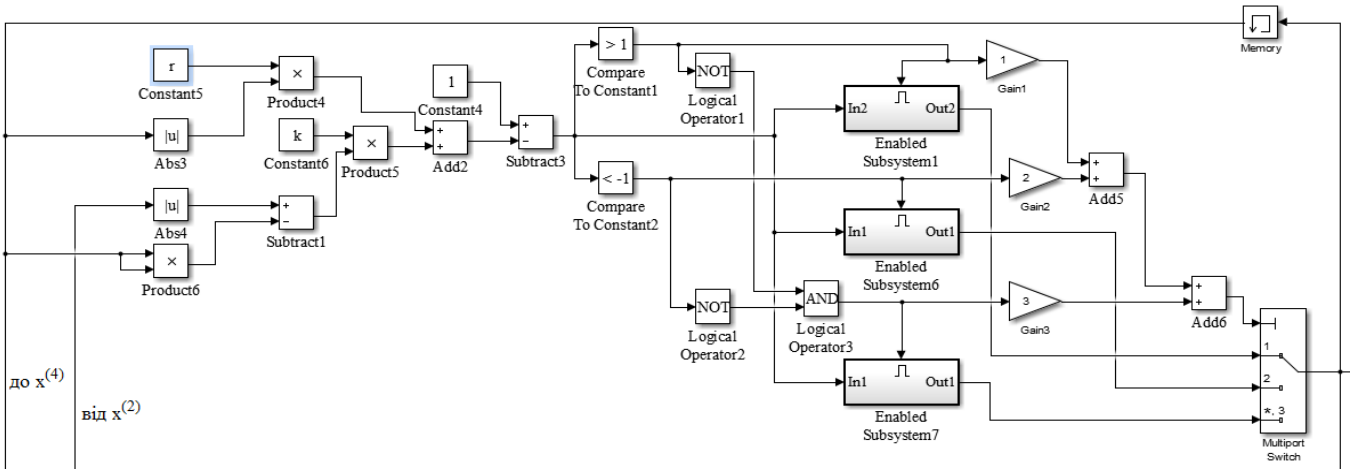


Рис. 8. Simulink-блок-діаграма реалізації $x_{n+1}^{(1)}$.

Якщо значення хаотичного коливання знаходиться в межах діапазону [-1, 1], то сигнали керування на компараторах 1 і 2 будуть рівними логічному нулю. Сигнали керування потрапляють на вхід логічного оператора НІ (інвертор). Далі на виході логічних операторів над сигналами виконується логічне множення І, внаслідок чого утворюється сигнал керування підсистемою 3. Дана підсистема передає сигнал без його зміни. Для вибірки шини передавання генерованого хаотичного коливання, що задовольняє одній з умов (6) використано комутатор (Multiport Switch), що керується сигналами керування підсистем. Для розрізнення сигналів керування підсистемами виконується множення на коефіцієнт D_i, що відповідає одному з рівнів входу. Оскільки в даному випадку є три виходи підсистем то D_i =1, 2, 3, а рівень сигналу керування комутатором відповідає одному із виходів підсистем 1-3.

На рис. 9 приведено збалансованість бітів у бінарному представленні генерованих системою Лоці (5) при $p = 4$ значень. Із рис. 9 випливає, що збалансованість бітів має місце для діапазону бітів з порядковим номером від 1 до 29, а біти що належать діапазону від 30 до 32 є незбалансованими, в результаті зсуву розряду числа вліво на один розряд. Тому, для формування псевдовипадкових послідовностей використовувалися біти, що належать діапазону $5 \div 20$. В блоці послідовностей M_x (рис. 7) здійснюється вибірка 16 бітів із кожного часового ряду в діапазоні $5 \div 20$ біт. В результаті після однієї ітерації отримаємо 4*16=64 біти. На виході блоків додавання за модулем 2 отримуємо дві послідовності по 16 біт, що формують послідовність довжиною 32 біти. В табл. 2 приведені результати тестування за набором статистичних тестів NIST SP 800-22 для згенерованої послідовності довжиною 10^9 біт при наступних значеннях параметрів та початкових умов: $x_0^{(1)} = 0.292$, $x_0^{(2)} = -0.90258$, $x_0^{(3)} = 0.0258$, $x_n^{(4)} = 0.990258$, $k^{(i)}, r^{(i)} = 2$.

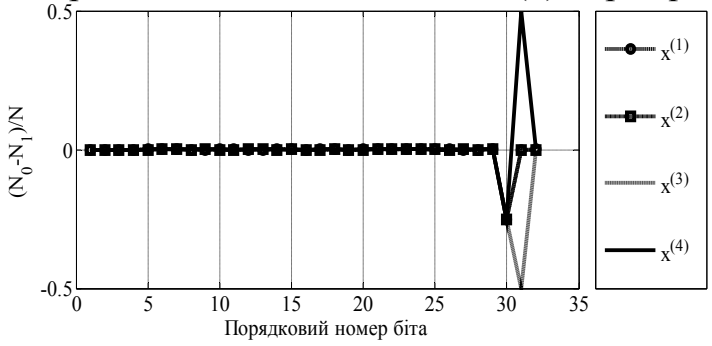


Рис. 9. Збалансованість бітів у бінарному представленні значень, генерованих за системою Лоці (5) при $p = 4$ із урахуванням (6).

Табл. 2. Результати статистичних тестів NIST SP 800-22.

Назва тесту	*P* - значення	Пропорція	Статус
Частотний (монобітний) тест	0.958485	0.989	**Пройдено**
Частотний тест по блокам	0.377007	0.993	**Пройдено**
Тест на послідовність однакових бітів	0.281232	0.986	**Пройдено**
Тест на найдовшу послідовність одиниць в блоці	0.049984	0.993	**Пройдено**
Тест рангу бінарних матриць	0.231956	0.993	**Пройдено**
Тест на основі дискретного перетворення Фур'є	0.137282	0.983	**Пройдено**
Тест на співпадіння з шаблоном без перекриття	0.737915	0.990	**Пройдено**
Тест шаблонів з перекриттям	0.353733	0.993	**Пройдено**
Універсальний статистичний тест Маурера	0.450297	0.992	**Пройдено**
Тест лінійної складності	0.353733	0.983	**Пройдено**
Тест серій	0.056069	0.992	**Пройдено**
Тест на основі апроксимації ентропії	0.132640	0.988	**Пройдено**
Тест накопичених сум	0.672470	0.989	**Пройдено**
Тест випадкових відхилень	0.701024	0.990	**Пройдено**
Тест випадкових відхилень - 2	0.947142	0.992	**Пройдено**

Також за допомогою чисельних методів Ейлера та Рунге-Кути та з використанням арифметики з фіксованою комою Q8.16 досліджено розв'язки нелінійних диференційних рівнянь математичної моделі мемристивної хаотичної системи та встановлено, що середня тривалість циклу знаходиться в межах $10^6 \div 2*10^6$ ітерацій і не залежить від кроку дискретизації Δt, що становить $0,0005 \div 0,02$.

У четвертому розділі дисертації проведені дослідження динамічних режимів роботи та схемотехнічна реалізація генераторів випадкових послідовностей на базі хаотичних систем Тратаса і Лоці. Система Тратаса в загальному вигляді є двомірним відображенням, що описується наступною системою рівнянь:

$$\begin{cases} x(n+1) = a_1 x(n) - b_1 \left| y(n) \right| + 1, \\ y(n+1) = a_2 y(n) - b_2 \left| x(n) \right| + 1, \end{cases} \tag{8}$$

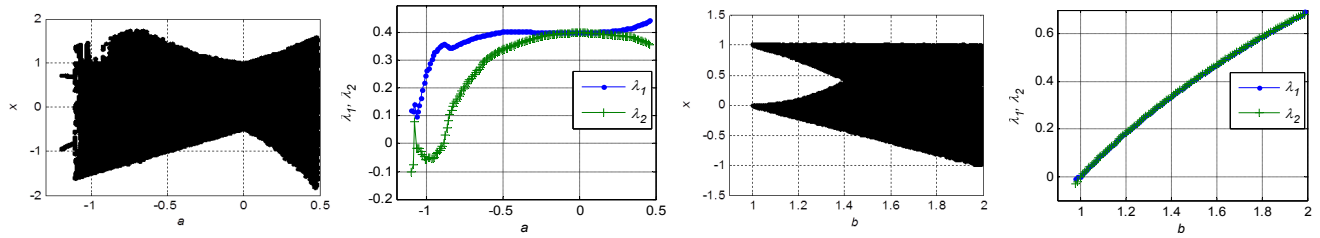
де a_1, a_2, b_1 і b_2 – параметри системи. В залежності від значень параметрів керування, відображення (8) може бути хаотичним або гіперхаотичним. Біфуркаційна діаграма та залежність показників Ляпунова для цієї системи приведені на рис. 10.

Із рис. 10 *а, в* випливає, що гіперхаотичні коливання мають місце в широкому діапазоні значень параметрів керування. Для випадків, якщо $a = [-1;\ 0,48]$ при $b = 1,493$ та $b \in [1,42;\ 1,989]$ при $a = 0,01$ вікна періодичності не виявлено. Розподіл значень реалізацій, генерованих системою (8) є неперервним для всього діапазону хаотичних коливань $x \in [x_{\min}; x_{\max}]$, $y \in [y_{\min}; y_{\max}]$.

При значеннях параметрів керування a=–0,75 і b=1,493 сума показників Ляпунова $\lambda_1 = 0.369$ і $\lambda_2 = -0.21$ є додатною, що вказує на встановлення в системі режиму гіперхаосу (див. рис. 11 *б*). Для додатних значень параметру *a* мають місце гіперхаотичні коливання (див. рис. 11 *в*).

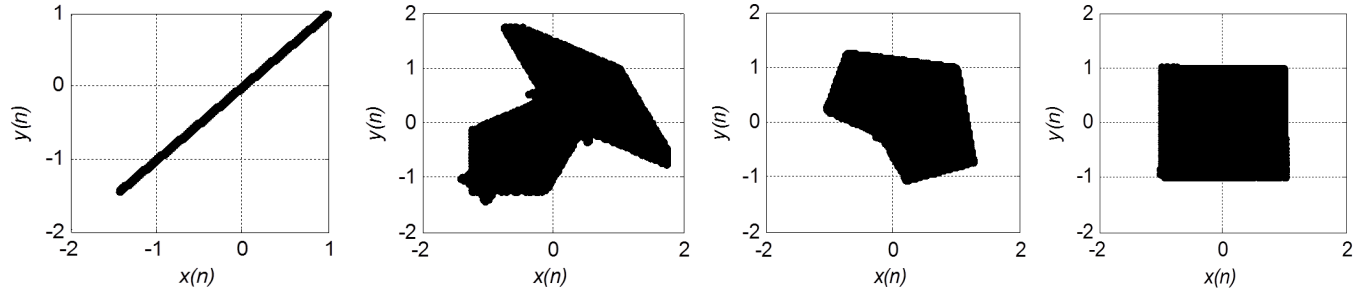
При $a \to 0$, $b = 2 - a \to 2$ обидва показники Ляпунова прямують до максимально можливого значення $\lambda_1, \lambda_2 \to \ln 2$ (рис. 11 *г*), а фазовий портрет має форму квадрату з

рівномірним заповненням, що свідчить про слабку статистичну залежність двох реалізацій $x(n)$ і $y(n)$.



а *б* *в* *г*

Рис. 10. Двовимірне відображення: біфуркаційна діаграма – (*а, в*), залежність показників Ляпунова - від *a* при $b=1,493$ – (*б*); від *b* при $a=0,01$ – (*г*).

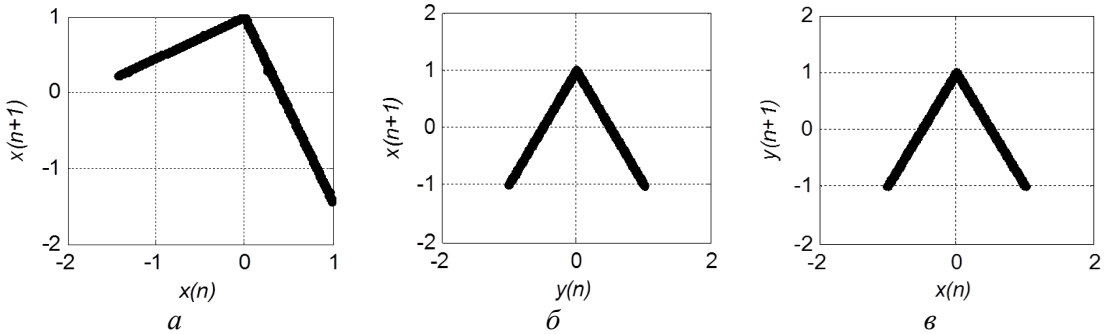


а *б* *в* *г*

Рис. 11. Фазовий портрет системи Тратаса (8): хаотичний режим при $a=-0.95$, $b=1,493$ – (*а*); гіперхаотичний режим при: $a=-0,75$, $b=1,493$ – (*б*); $a=0,23$, $b=1,493$ – (*в*); $a=0,01$, $b=1,98$ – (*г*).

При $a=-0.95$, $b=1,493$ рівняння (8) можна розглядати як такі, що описують ідентичні системи із встановленим між ними режимом повної синхронізації (рис. 11 *а*). Нелінійна функція перетворення $x(n+1)=f[x(n)]$ є кусково-лінійним відображенням, що складається із двох лінійних ділянок (див. рис. 12).

Детальний аналіз ітераційних діаграм (рис. 12 *б, в)* дозволяє зробити висновок, що система (8) за типом функції нелінійного перетворення еквівалентна двом тентовим відображенням, з'єднаним слабким зворотнім зв'язком у формі доданків $ax(n)$ і $ay(n)$.



а *б* *в*

Рис. 12. Графічне представлення функції нелінійного перетворення при $a=-0,95$, $b=1,493$ – (*а*); $a=0,01$, $b=1,98$ – (*б*) і (*в*)

Для схемотехнічної реалізації системи (8) у вигляді електронного кола проводилось перемасштабування змінних наступним чином:

$$\begin{aligned} u(n) &= Ex(n) \\ v(n) &= Ey(n) \end{aligned}, \qquad (9)$$

де $E>0$. Тоді параметри керування *a* та *b* дорівнюватимуть:

$$\begin{aligned} a &= A-1, \quad A>0 \\ b &= B. \end{aligned} \tag{10}$$

Враховуючи (9) і (10) запишемо (8) в наступній формі:

$$\begin{cases} u(n+1) = (A-1)u(n) - B\left|v(n)\right| + E_{кер} \\ v(n+1) = (A-1)v(n) - B\left|u(n)\right| + E_{кер} \end{cases}, \tag{11}$$

де A, B – нові параметри керування системою. Із (11) випливає, що керування амплітудою генерованих сигналів можна здійснювати за допомогою $E_{кер}$. Реалізація електронного кола на основі (11) приведена на рис. 13.

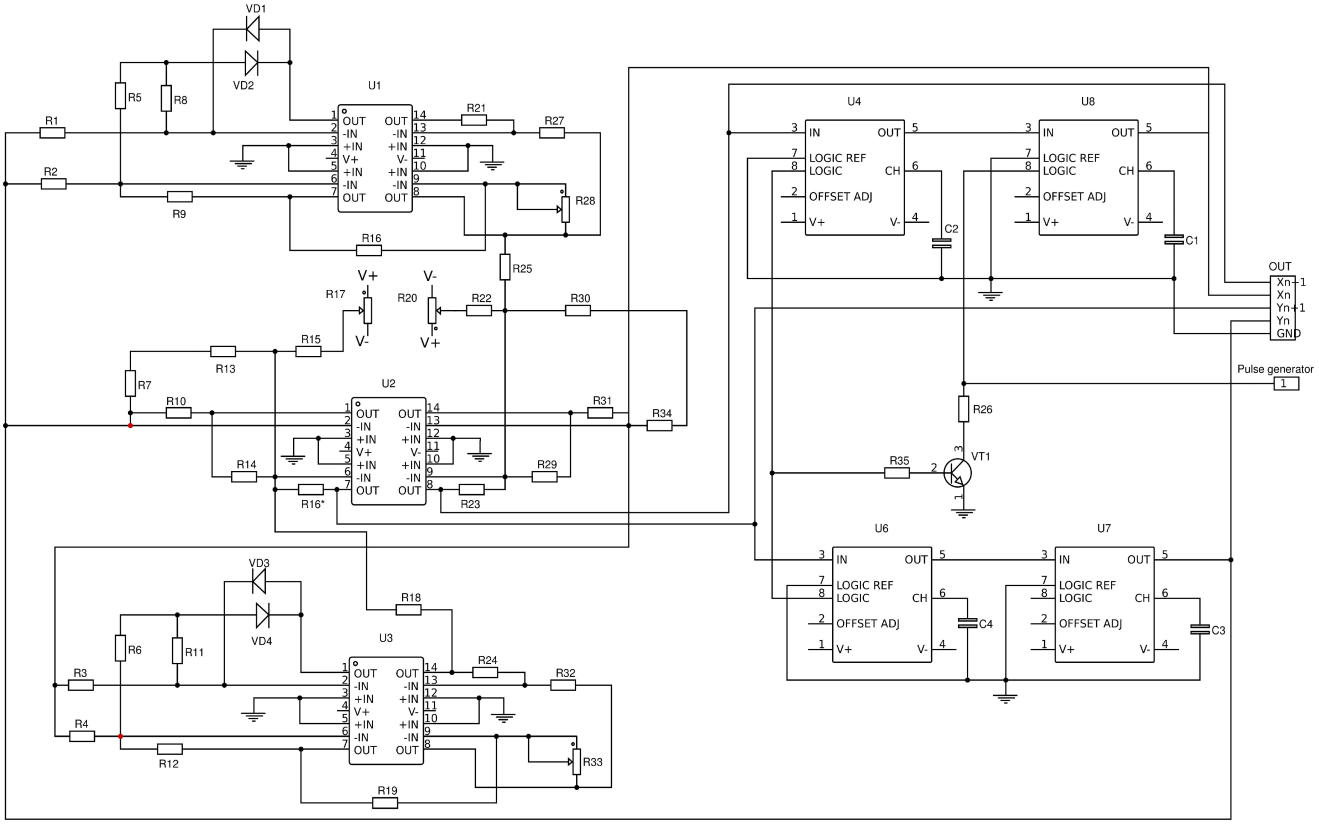


Рис. 13. Схемотехнічна реалізація системи (11).

Встановлення значень сигналу за модулем виконує двонапівперіодний випрямляч на базі операційних підсилювачів та діодів VD1÷VD4. Затримку сигналу на один такт реалізовано на пристроях вибірки і затримки LF398 - U4-7. На мікросхему U6 подається інвертований тактовий сигнал. При цьому на протязі першого напівперіоду заряджаються конденсатори C2 і C4, а значення попередньої ітерації зберігається на C1 і C3. На протязі другого напівперіоду заряджаються конденсатори C1 і C3, а C2 і C4 зберігають значення поточної ітерації. Для експериментального дослідження електронного кола (рис. 13) був розроблений макет, результати дослідження якого приведені на рис. 14. При однакових значеннях параметрів керування для коливань $u(n)$ і $v(n)$ (рис. 14 *а, б, в*) функція нелінійного перетворення є кусково-лінійною (рис. 14 *г, д, е*). Фазові портрети (рис. 14 *ж*, *и*, *к*) відповідають гіперхаотичним режимам.

Для генерованих коливань (рис. 14) значення $E_{кер}$ становить: -2 В (*а, г, ж*); (*б, д, и*); -5,5В (*в, е, к*). Частота тактового сигналу становила 10 кГц.

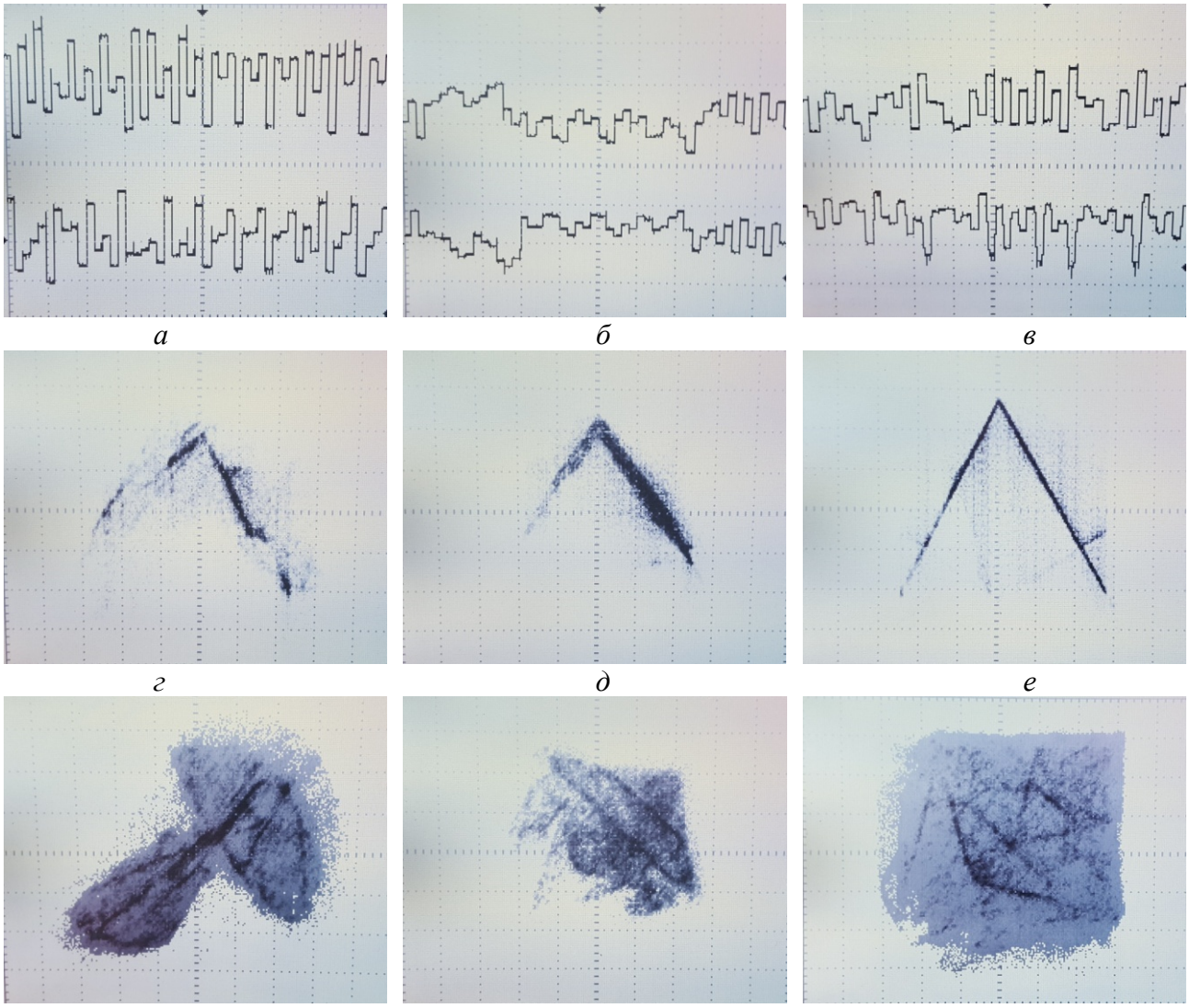


Рис. 14. Гіперхаотичні коливання: сигнали *v(n)* і *u(n)* – (*а, б, в*); функція нелінійного перетворення *u*(*n*+1)=*f*(*u*(*n*)) – (*г, д, е*); фазовий портрет при R17=R22=2.5 кОм, R29=R32=14.93 кОм – (*ж*); R17=R22=12.3 кОм, R29=R32=14.93 кОм – (*и*); R17=R22=0.01 кОм, R29=R32=19.99 кОм – (*к*).

Результати експериментального дослідження корелюють із результатами моделювання. Порівнюючи результати приведені на рис. 14 із рис. 11 і рис. 12 можна зробити висновок про існування розкиду параметрів елементів схеми відносно номінальних значень, оскільки експериментально отримані форми хаотичних коливань є спотвореними.

Також, встановлено що на основі залежності ентропії розподілу діагоналей рекурентної діаграми модифікованої системи Тратаса можливо оцінити нижню межу розмірності фазового простору системи. Це дозволяє здійснювати підбір системи з розмірністю, при якій розкриття параметрів є ускладненим.

У п’ятому розділі проведено дослідження криптостійкості методу перестановок пікселів на основі відображення Чирікова. Проаналізовано та визначено недоліки методу шифрування растрових зображень з незалежними етапами дифузії і перестановки та показано можливість розкриття шифру.

Запропоновано спосіб шифрування для якого атака вибраним відкритим текстом є ускладненою.

Для перестановок пікселів пропонується використання дискретизованої за

розмірами зображення $N \times N$ двовимірної хаотичної системи Чирікова. В загальному випадку дискретизоване відображення Чирікова задається системою рівнянь:

$$\begin{cases} x_{j+1} = \left(x_j + y_j \right) mod\, N, \\ y_{j+1} = \left(y_j + K_2 \sin \dfrac{x_{j+1} N}{2\pi} \right) mod\, N, \end{cases} \tag{12}$$

де K – параметр (натуральне число) стандартного відображення; x_{j+1} та y_{j+1} координати $j \in [0; N-1]$ пікселів по ширині або висоті растрового зображення розмірністю $N \times N$. Показано, що простір ключів для змішування пікселів такого відображення становить N^{N-1}.

Для збільшення потужності простору ключів до $(N^2 - 1)!$ для відображення (12) запропоновано ввести нелінійну функцію в змінну x_{j+1}. Тоді модифіковане відображення набуде вигляду:

$$\begin{cases} x_{j+1} = \left(x_j + K_1 \sin \dfrac{y_j N}{2\pi} \right) mod\, N, \\ y_{j+1} = \left(y_j + K_2 \sin \dfrac{x_{j+1} N}{2\pi} \right) mod\, N, \end{cases} \tag{13}$$

де K_1 і K_2 – параметри системи. Значення якобіана системи (13) дорівнює одиниці і не залежить від значень параметрів K_1 і K_2:

$$D = \begin{vmatrix} \dfrac{\partial x}{\partial x} & \dfrac{\partial x}{\partial y} \\ \dfrac{\partial y}{\partial x} & \dfrac{\partial y}{\partial y} \end{vmatrix} = \begin{vmatrix} 1 & \dfrac{K_1 N}{2\pi} \cos \dfrac{yN}{2\pi} \\ \dfrac{K_2 N}{2\pi} \cos \dfrac{\left(x + K_1 sin\, \dfrac{yN}{2\pi} \right) N}{2\pi} & 1 + \dfrac{K_1 K_2 N^2}{(2\pi)^2} \cos \dfrac{\left(x + K_1 sin\, \dfrac{yN}{2\pi} \right) N}{2\pi} \end{vmatrix} = 1.$$

Тому, відображення (13) буде зберігати площу, а отже є придатним для здійснення перестановок. Проте, на практиці використовуючи різні апаратні платформи складно отримати однакові значення функції синуса. Тому необхідно використовувати заздалегідь підготовлені таблиці значень або розробити відображення, що оперує цілими числами та зберігає площу.

Для реалізації хаотичної системи в цілочисельному діапазоні запропоновано замінити нелінійні функції $\sin \dfrac{y_j N}{2\pi}$ та $\sin \dfrac{x_{j+1} N}{2\pi}$ на y_j^2 та x_{j+1}^2, відповідно. Тоді система (13) набуде вигляду:

$$\begin{cases} x_{j+1} = \left(x_j + K_1 y_j^2 \right) mod\, N \\ y_{j+1} = \left(y_j + K_2 x_{j+1}^2 \right) mod\, N \end{cases}, \tag{14}$$

де K_1 і K_2 – параметри системи.

Також розроблено метод захисту зображень на основі перестановок пікселів, що базуються на модифікованому відображенні Чирікова (14) та дифузії кольору пікселів шляхом шифрування бінарними ПВП, генерованими розробленими ГПВП.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

У дисертаційній роботі розв’язано науково-прикладне завдання синтезу та практичної реалізації генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем. Основні результати дисертаційного дослідження викладені у висновках, що зводяться до наступних положень:

1. Проведено ретельний аналіз сучасного стану ГПВП та ГВП на базі нелінійних динамічних систем. Досліджено вплив обмеження точності обчислень на статистичні властивості логістичного відображення при його апаратній реалізації на базі ПЛІС з використанням арифметики з фіксованою комою Q3.29. Встановлено, що потужність множини різних початкових умов після перехідного процесу дорівнює сумі довжин всіх можливих циклів та становить $24797 \approx 2^{14}$. Визначено залежність потужності простору початкових умов для логістичного відображення від кількості ітерацій.

2. Досліджено двовимірну дискретну хаотичну систему Тратаса. Встановлено, що генератор хаотичних сигналів на базі системи Тратаса генерує хаотичні та гіперхаотичні коливання в широкому неперервному діапазоні значень параметрів керування. Запропоновано спосіб отримання випадкових сигналів на основі модифікованої багатовимірної системи Тратаса, що уможливлює формування сигналів із наперед заданим розподілом їх значень.

3. Схемотехнічно реалізовано генератор випадкових сигналів на базі відображення Лоці із кільцевим зв’язком, що може бути використаний для генерування випадкових сигналів із швидкістю 0,84 Мбіт/с при умові використання двовимірної системи та частоти тактового сигналу 30 кГц.

4. Встановлено, що на основі залежності ентропії розподілу діагоналей рекурентної діаграми модифікованої системи Тратаса можливо оцінити нижню межу розмірності фазового простору системи. Це дозволяє здійснювати підбір системи з розмірністю, при якій розкриття параметрів є ускладненим.

5. Запропоновано метод синтезу псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв’язком, з використанням збалансованих найменш значущих бітів. Це ускладнює розкриття параметрів генератора, що дозволяє формувати великі ансамблі послідовностей з наперед заданими наборами довжин.

6. Проведено апаратну реалізацію запропонованих генераторів та показано, що при умові використання чотиривимірної системи потенційна швидкість формування ПВП становитиме до 19,2 Гбіт/с. Розроблена структура генератора уможливлює формування псевдовипадкових послідовностей на основі багатовимірних відображень із кільцевим зв’язком довільної розмірності. Проведено тестування генерованих послідовностей на відповідність критеріям псевдовипадковості згідно набору статистичних тестів NIST SP 800-22.

7. Розроблено апаратне рішення методу генерування псевдохаотичних послідовностей на основі математичних моделей неперервних хаотичних систем з використанням в якості нелінійного елементу мемристивної структури, що забезпечує незалежність середньої тривалості періоду повторення в межах

$10^6 \div 2 * 10^6$ ітерацій від кроку дискретизації, що становить $\Delta t = 0,0005 \div 0,02$ при умові використання арифметики з фіксованою комою Q8.16.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових виданнях України та в іноземних наукових періодичних виданнях, які включені до міжнародних наукометричних баз

1. Галюк С.Д. Аналіз часових рядів генерованих гіперхаотичною системою Тратаса / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 4(251). – С. 187-192. (Наукове фахове видання України; інд. Index Copernicus).
2. Галюк С.Д.Порівняльний аналіз двомірних відображень для перестановок пікселів / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Вісник Хмельницького національного університету серія: Технічні науки. – 2017. – № 1(245). – С. 214-220. (Наукове фахове видання України; інд. Index Copernicus).
3. Krulikovskyi O.V. Image encryption algorithm based on chaotic maps / O.V. Krulikovskyi, P.M. Shpatar, L.F. Politanskyi // Eastern European Scientific Journal. – 2014. – №6. – P. 362-366. (Друковане іноземне наукове періодичне видання з напряму; індексується Index Copernicus).
4. Круліковський О.В. Особливості вибору хаотичних систем для побудови генераторів псевдовипадкових послідовностей / О.В. Круліковський, С.Д. Галюк, Л.Ф. Політанський // Телекомунікаційні та інформаційні технології. – 2017. – №2. – С. 64-67. (Наукове фахове видання України; інд. РИНЦ, Google Scholar).
5. Krulikovskyi O.V. Testing timeseries ring-coupled map generated by on FPGA / O.V. Krulokovskyi, S.D. Haliuk, L.F. Politanskyi // Телекомунікаційні та інформаційні технології. – 2016. – №4(53). – С. 24-29. (Наукове фахове видання України; інд. РИНЦ, Google Scholar).

Статті у наукових фахових виданнях України

6. Krulikovskyi O.V. PRNG based on modified tratas chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Сучасний захист інформації. – 2016. – №2. – С. 69-77.

Опубліковані наукові праці апробаційного характеру

7. Corinto F. Memristor-based chaotic circuit for pseudo-random sequence generators / Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Proceedings of the 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, April 18-20, 2016. (Індексується у Scopus).
8. Haliuk S. Analysis of Pixels Permutations Based on Discretized Chirikov Map / Sergiy Haliuk, Oleg Krulikovskyi, Leonid Politanskyi // Proceedings of the XIIIth International Conference TCSET'2016, Lviv-Slavsko, Ukraine, February 23 – 26, 2016. – pp. 519-521. (Індексується у Scopus).
9. Політанський Л.Ф. Циклічність послідовностей генерованих хаотичною системою / Л.Ф. Політанський, С.Д. Галюк, О.В. Круліковський // II Міжнародна конференція з інформаційно-телекомунікаційних технологій та радіоелектроніки УкрМіКо 2017. – м. Одеса, 11-15 вересня 2017 р. – С. 545-548.

10. Krulikovskyi O. Development features of cryptographic means based on chaotic systems / Krulikovskyi Oleh, Haliuk Serhii // Proceeding of the Vth International Scientific Practical Conference “PREDT 2016”, 3–5 November, 2016, Chernivtsi, Ukraine. - P.125.

11. Krulikovskyi O.V. Using PRNG based on multidimensional discrete hyperchaotic system for image encryption / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // IV Міжнародна науково-практична конференція «Напівпровідникові матеріали, інформаційні технології та фотовольтаїка»: тези доповідей, м. Кременчуг. 26-28 травня, 2016 р. – С. 234-235.

12. Krulikovskyi O.V. PRNG based on discrete hyper chaotic system / O.V. Krulikovskyi, S.D. Haliuk, L.F. Politanskyi // Проблеми інформатики та комп’ютерної техніки: Праці V-ї Міжнародної науково-практичної конференції ПІКТ – 2016, Чернівці, Україна, 21 – 24 травня, 2016. – С. 204.

13. Image encryption algorithm based on one-dimensional and two-dimensional maps / M.Ya. Kushnir, G.V. Kosovan, O.V. Krulikovskyi // Proceeding of the II International Scientific- Practical Conferences “PREDT -2012”. – Chernivtsi, October 25-27, 2012. – p. 90-91.

14. Encryption algorithm based on two-dimensional standard map / O.V. Krulikovskyi , L. F. Politanskyi // Proceeding of the IV International Scientific-Practical Conferences “PREDT -2014”. – Chernivtsi, October 23-25, 2014. – pp. 68-69.

15. Круліковський О.В. Рекурентний аналіз багатовимірних хаотичних систем / С.Д. Галюк, О.В. Круліковський, Л.Ф. Політанський // Міжнародна науково-практична конференція "ОСНП - 2017"- м. Черкаси, 24-26 травня, 2017 р. – С. 94-96.

АНОТАЦІЯ

Круліковський О.В. Синтез генераторів псевдовипадкових послідовностей на основі багатовимірних нелінійних динамічних систем. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій. – Національний університет “Львівська політехніка” Міністерства освіти і науки України, м. Львів, 2018.

Роботу присвячено розв’язанню важливої науково-прикладної задачі синтезу та практичної реалізації генераторів псевдовипадкових та випадкових послідовностей на основі багатовимірних нелінійних динамічних систем.

В результаті досліджень, що виконані у межах дисертаційної роботи показано, що використання багатовимірних систем із кільцевим зв’язком в якості бази генераторів псевдовипадкових послідовностей уможливлює генерування таких послідовностей із великим періодом повторення. Зокрема, проведено апаратну реалізацію запропонованих генераторів на програмованих логікових інтегральних схемах та показано, що генеровані ними послідовності відповідають вимогам статистичних тестів NIST SP 800-22.

На базі гіперхаотичної системи Тратаса та двовимірного відображення Лоці реалізовано генератори випадкових послідовностей. Показано, що неперервний діапазон зміни параметрів керування системи Тратаса і відображення Лоці, в

порівнянні із іншими системами, забезпечує роботу генераторів в хаотичному та гіперхаотичному режимах. Встановлено, що біфуркаційна діаграма системи Тратаса не має вікон періодичності, що є суттєвою перевагою в порівняні із іншими системами такого класу.

Ключові слова: нелінійні динамічні системи, генерування псевдовипадкових послідовностей, відображення із кільцевим зв'язком, перестановки, збалансованість бітів, програмовані логікові інтегральні схеми.

АННОТАЦИЯ

Круликовский О.В. Синтез генераторов псевдослучайных последовательностей на основе многомерных нелинейных динамических систем. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.13 – радиотехнические устройства и средства телекоммуникаций. – Национальный университет "Львовская политехника" Министерства образования и науки Украины, г. Львов, 2018.

Работа посвящена решению важной научно-прикладной задачи синтеза и практической реализации генераторов псевдослучайных и случайных последовательностей на основе многомерных нелинейных динамических систем.

В результате исследований выполненных в рамках диссертационной работы показано, что использование многомерных систем с кольцевой связью в качестве базы генераторов псевдослучайных последовательностей позволяет генерировать последовательности с большим периодом повторения. В частности, проведено аппаратную реализацию предложенных генераторов на программируемых логических интегральных схемах и показано, что генерируемые ими последовательности соответствуют требованиям статистических тестов NIST SP 800-22.

На базе гиперхаотичной системы Тратаса и двумерного отображения Лоци реализовано генераторы случайных последовательностей. Показано, что непрерывный диапазон изменения параметров управления системы Тратаса и отображения Лоци, по сравнению с другими системами, обеспечивает работу генераторов в хаотическом и гиперхаотическом режимах. Установлено, что бифуркационная диаграмма системы Тратаса не имеет окон периодичности, что является существенным преимуществом в сравнении с другими системами такого класса.

Ключевые слова: нелинейные динамические системы, генерирование псевдослучайных последовательностей, отображение с кольцевой связью, перестановки, сбалансированность бит, программируемые логические интегральные схемы.

ABSTRACT

Krulikovskyi O.V. Synthesis of pseudorandom number generators based on multidimensional nonlinear dynamical systems. – On the rights of the manuscript.

A thesis submitted in fulfillment of the Candidate of Science (PhD) degree on specialty 05.12.13 – Radio Engineering Devices and Telecommunication Means. – Lviv Polytechnic National University of Ministry for Education and Science of Ukraine, Lviv, 2018.

The work is devoted to solving an important scientific and practical task of synthesis and practical implementation of pseudorandom and random sequence generators based on multidimensional nonlinear dynamical systems.

As a result of the investagation carried within dissertation, it has been shown that the use of multidimensional ring-coupled maps as a base of pseudorandom sequence generators makes it possible to generate such sequences with a long period, this type generators were implemented in hardware and investigated experimentally. In particular, the hardware implementation of the proposed generators on field-programmable gate array (FPGA) was performed and it was shown that the generated sequences meet to the requirements of the NIST SP 800-22 statistical test siute.

The generators of random sequences are implemented on the basis of the hyperchaotic Tratas system and the two-dimensional Lozi map. It is shown that the continuous range of changes in the control parameters of the Lozi and Tratas systems, in comparison with other systems, provides the operation of generators in chaotic and hyperchaotic modes. It has been established that the Tratas system bifurcation diagram does not have windows of periodicity, that is a significant advantage compared with other systems of this class.

Key words: nonlinear dynamical systems, generation of pseudorandom sequences, ring-coupled maps, permutations, balance of bits, FPGA.