https://doi.org/10.31891/2219-9365-2023-73-1-24
УДК 004.056

Володимир КОРЧИНСЬКИЙ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-3972-0585
e-mail: vkadkorchin@ukr.net
Олександр РЯБУХА
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0001-7402-0395
e-mail: ryabukha@gmail.com
Аль-Файюмі ХАЛЕД
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0003-4624-2569
e-mail: khaled@alfaiomi.com
Сергій ГАВЕЛЬ
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0000-0002-0484-5620
e-mail: arkominer@gmail.com
Володимир МІНЕНКО
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0009-5727-5877
e-mail: minenko.od@gmail.com
Зураб КРИШТАФОР
Державний університет інтелектуальних технологій і зв'язку
https://orcid.org/0009-0004-5287-6589
e-mail: zurab929@gmail.com

ДОСЛІДЖЕННЯ ВАРІАЦІЙНИХ МОЖЛИВОСТЕЙ ГЕНЕРАТОРІВ ХАОСУ ПО ФОРМУВАННЮ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

В роботі проведено дослідження варіаційних можливостей генераторів хаосу по формуванню псевдовипадкових послідовностей, які можна використовувати в системах потокового шифрування. У криптографічних системах найчастіше застосовуються лінійно-конгруентні генератори або апаратні генератори із зворотними зв'язками. Недоліками таких генераторів є невеликий період формування псевдовипадкових числових послідовностей, а також обмежена кількість можливих комбінацій. З цієї причини доцільним є дослідження властивостей генераторів хаосу, період формування вибірки чисел для яких залежить від розміру розрядної сітки використовуваної обчислювальної системи. Вочевидь, що якість генераторів хаосу потрібно оцінювати за допомогою системи тестів NIST. Тобто, для практичного застосування генераторів хаосу в криптографічних системах необхідна ретельна оцінка їх статистичних характеристик. Також на основі хаотичних послідовностей розробляються різні методи модуляції, за допомогою яких забезпечується структурна та енергетична прихованість сигнальних конструкцій. Передумовами для всього цього стали властивості динамічного хаосу: рух детермінованої динамічної системи при певних умовах має всі властивості шумового сигналу; наявність нелінійності і неперіодичності процесу. Характерною особливістю генераторів хаосу є те, що незначні зміни початкових параметрів хаотичного процесу призводять до суттєвої зміни значень генеруючих коливань. Це дає можливість формувати різні траєкторії хаотичного процесу, на основі яких можна створювати практично необмежену кількість комбінацій псевдовипадкових послідовностей (ПВП) заданої довжини. Однак реальне впровадження динамічного хаосу для систем шифрування та модуляції вимагає пошуку методів, за допомогою яких можна формувати початкові параметри генератора на основі, наприклад, введеного пароля. З цього приводу доцільним є оцінка варіаційних можливостей генераторів хаосу для завдання формування псевдовипадкових послідовностей з необхідними кореляційними властивостями. На жаль, у відомих наукових працях цьому питанню приділено недостатню увагу, тому перспективність дослідження в даному напрямку визначає актуальність роботи. Метою цієї роботи є дослідження варіаційних можливостей генераторів хаосу для формування псевдовипадкових послідовностей із заданими кореляційними властивостями.

Ключові слова: генератор, хаос, криптографія, тест, послідовність, період, якість, прихованість, розширення спектра

Volodymyr KORCHYNSKYI, Oleksandr RIABUKHA, Khaled ALFAION,
Sergey HAVEL, Volodymyr MINENKO, Zurab KRYSHTAFOR
State University of Intellectual Technologies and Communications

RESEARCH OF VARIATIONAL OPPORTUNITIES OF CHAOS GENERATORS FOR THE FORMATION OF PSEUDONANDOM SEQUENCES

In the article was researched the variational opportunities of chaos generators in the formation of pseudo-random sequences that can be used as gamma in stream encryption systems. In cryptographic systems, linear congruential generators or hardware generators with feedback are most often used. The disadvantages of such generators are a short period of formation of pseudo-random numerical sequences, and a limited number of possible combinations. For this reason, it is advisable to research the

properties of chaos generators, the period of formation of a sample numbers for which depends on the size of the bit grid of the used computer system.

However, the quality of chaos generators should be evaluated using NIST test system. That is, for the practical application of chaos generators in cryptographic systems, a thorough assessment of their statistical characteristics is necessary. Also, based on chaotic sequences are developed various modulation methods, with the help of which is ensured the structural and energy secrecy of signal constructions. The prerequisites for all this were the characteristics of dynamic chaos: the motion of a deterministic dynamic system, under certain criteria, it has all the qualities of a noise signal; the presence of non-linearity and non-periodicity of the process. A characteristic feature of chaos generators is that minor changes in the initial parameters of the process lead to a significant change in the values of generating fluctuations. It allows to form various trajectories of a chaotic process, based on which it can create an almost unlimited number of combinations of pseudo-random sequences of given length. However, the actual implementation of dynamic chaos for encryption systems or modulation systems requires the search for methods, that can be used to form the initial parameters of the generator based, for example, on the entered password.

On this occasion, it is advisable to evaluate the variational capabilities of chaos generators to set the formation of pseudorandom sequences with the necessary correlation properties. Unfortunately, insufficient attention has been paid to this issue in well-known scientific works, therefore, the prospects of research in this direction determine the relevance of the article. The aim of this article is to research the variational possibilities of chaos generators for the formation of pseudorandom sequences

Keywords: generator, chaos, cryptography, test, sequence, period, quality, stealth, spread spectrum, noise-like signals

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Відомо [1-3], що класична криптографія заснована на різних положеннях і до кінця 20 століття явище динамічного хаосу не застосовувалось для створення будь-яких систем захисту інформації. Проте в 21-му столітті криптографія набула нові напрямки розвитку, в яких хаотичні послідовності, що можуть формуватися за допомогою програмних та апаратних генераторів хаосу, становляться основою для створення різних механізмів в системах шифрування. Також на основі хаотичних послідовностей розробляються різні методи модуляції [4-8], що забезпечують структурну та енергетичну прихованість сигнальних конструкцій [9]. Передумовами для всього цього стали властивості динамічного хаосу: рух детермінованої динамічної системи [4] при певних умовах має всі властивості шумового сигналу; наявність нелінійності і неперіодичності процесу.

Вочевидь, що до генераторів хаосу пред'являються особливі вимоги щодо якості формування послідовності чисел [4,9]. Характерною особливістю таких генераторів є те, що незначні зміни початкових параметрів процесу призводять до суттєвих відхилень значень генеруючих коливань. Це дає можливість формувати різні траєкторії хаотичного процесу, на основі яких можна створювати практично необмежену кількість комбінацій псевдовипадкових послідовностей заданої довжини. Однак реальне впровадження явища динамічного хаосу для систем шифрування та систем модуляції вимагає пошуку методів, за допомогою яких можна формувати початкові параметри генератора на основі, наприклад, введеного пароля. З цього приводу доцільним є дослідження варіаційних можливостей генераторів хаосу для завдання формування псевдовипадкових послідовностей з необхідними кореляційними властивостями.

Аналіз досліджень та публікацій

Динамічний хаос [4] це деякий нерегулярний та аперіодичний процес зміни стану нелінійної динамічної системи. Для нього характерні основні властивості випадкового процесу. Для завдання дослідження розглянемо програмний генератор хаосу [5-8], який є детермінованим пристроєм. Сформована за певним алгоритмом послідовність чисел також є детермінованою. В процесі дослідження потрібно з'ясувати, як впливає на структуру послідовності чисел найменша зміна початкових параметрів генератора хаосу. Очікуваним результатом повинна бути суттєва зміна структури послідовності чисел, що забезпечить можливість формувати різні траєкторії хаотичного процесу. Це особливо важливо для створення великої кількості гама послідовностей для системи потокового шифрування або завдання розширення спектра сигналу в системах з кодовим розділенням каналів.

На жаль, у відомих дослідженнях [7-9] питанню дослідження варіаційних можливостей генераторів хаосу для завдання формування псевдовипадкових послідовностей з необхідними кореляційними властивостями приділено недостатню увагу. Перспективність дослідження в даному напрямку, яке пов'язане з дослідженням властивостей програмних генераторів хаосу, визначає актуальність роботи. Це стало приводом для подальшого дослідження в цьому напрямку, тому метою цієї роботи є дослідження варіаційних можливостей генераторів хаосу для формування псевдовипадкових послідовностей.

Дослідження варіаційних можливостей генераторів хаосу по формуванню вибірок

Програмні генератори хаосу визначаються видом функції відображення x_i й значеннями керуючих параметрів [7]:

$$x_{i+1} = f\left(x_0; x_i; a\right), \tag{1}$$

де $f(\cdot)$ − нелінійна функція відображення; a − керуючий параметр; x_0, x_i, x_{i+1} − початкові значення процесу.

Генератори хаосу мають рівномірний закон розподілу чисел [6-8] в інтервалі]0…1[і реалізуються за певним алгоритмом, згідно з яким кожне наступне псевдовипадкове число обчислюється з попереднього. Детермінований спосіб формування послідовності має наступні переваги:

а) попередній відбір вибірки чисел із заздалегідь перевіреними статистичними властивостями, що забезпечує необхідну стабільність генерації чисел і не вимагає регулярного тестування послідовності;

б) багаторазове відтворення числової послідовності з потрібної позиції;

в) мінімальну кількість операцій, яка необхідна для формування кожного значення числової послідовності;

г) обчислювальний процес не займає великий обсяг пам'яті;

д) період послідовності повинен бути не менше, ніж заданий процес.

Для завдання експерименту розглянемо генератор хаосу логістичного відображення [7]:

$$x_{i+1} = ax_i(1-x_i). \tag{2}$$

Вхідними параметрами для такого генератора є початкове число послідовності x_0 і $a = 3{,}9$. Відомо [7], що зміна параметра a може бути в дуже обмеженому діапазоні значень. Проведемо дослідження впливу параметра a на процес хаотичного коливання.

На рис. 1 для різних значень $a = 2{,}6; 2{,}9; 3{,}2, 3{,}5; 3{,}7; 3{,}86; 3{,}9$ побудовані діаграми, з яких можна побачити зміну траєкторій хаотичного коливання. При значенні $a = 2{,}6$ логічне відображення вироджується на самому початку свого існування. Аналогічний результат ми отримуємо при значенні $a = 2{,}7$. При $a = 3{,}2$ отримуємо регулярне гармонійне коливання, що зовсім не є хаотичним коливанням. Регулярне коливання з двома різними амплітудами отримуємо при значенні $a = 3{,}5$.

Коливання «дивного» процесу отримуємо при значенні $a = 3{,}86$, при якому певне коливання змінюється на фрагменти коливань з суттєвим зменшенням амплітуди. Дійсне хаотичне коливання отримуємо при $a = 3{,}9$.

Подальше дослідження можливого відхилення значень $a = 3{,}9$ дає підтвердження, що це можливо. Наприклад, при незначному відхиленні параметру a ($a = 3{,}9001$ або $a = 3{,}90011$) є можливість створювати нові послідовності, відмінність яких можна оцінити за допомогою коефіцієнту кореляції.

В табл. 1 надано результати дослідження порівняння двох двійкових ПВП $X_j(a_j, x_j)$ і $X_i(a_i, x_i)$, що згенеровані на основі логістичного відображення генератора хаосу з кількістю чисел $N = 50000$. З таблиці бачимо, що отриманий коефіцієнт кореляції між послідовностями свідчить про їх незначний зв'язок, тому що $k_{ji} \to 0$. Це означає, що на основі генератора хаосу можна отримати велику кількість двійкових ПВП шляхом зміни початкових значень x_j та параметру a.

Таблиця 1

Коефіцієнти кореляції двох хаотичних процесів логістичного відображення при кількості двійкових чисел $N = 50000$

x_1	0,5	0,5	0,5	0,2	0,2
x_2	0,5	0,5001	0,75	0,95	0,35
a_1	3,90001	3,9	3,9	3,9	3,9
a_2	3,9	3,9	3,9	3,9	3,9
k_{ji}	-0,00176	-0,00213	-0,0081	-0,00069	-0,00377

Формування двійкових псевдовипадкових послідовностей на основі генератора хаосу

Розглянемо процес формування двійкових псевдовипадкових послідовностей на основі чисел генератора логістичного відображення (2). Для формування двійкової послідовності необхідно виконати наступну послідовність дій:

1) за допомогою генератора хаосу формується достатня велика послідовність в інтервалі $]0; 1[$ з кількістю чисел, наприклад, $N = 10^6$:

$$x_1, x_2, x_3, ..., x_N; \tag{3}$$

2) визначається середнє значення вибірки x_c;

3) інтервал від 0 до 1 розбивається на дві частині з урахуванням значення x_c: один інтервал $]0; x_c[$; другий – $]x_c; 1[$;

4) за умови, що поточне значення послідовності $0 < x_j < x_c$, тоді вибирається логічний нуль «0», якщо $x_c < x_j < 1$, тоді «1»;

5) за пунктом 4 формується певна кількість двійкових ПВП з різними значеннями параметра a або x_j, далі перевіряється коефіцієнт кореляції k_{ji} між послідовностями.

На рис. 2-6 надано залежності коефіцієнта кореляції k_{ji} між двома хаотичними процесами логістичного відображення від кількості двійкових чисел N при різних значеннях: a_1 і x_1 – перша ПВП; a_2 і x_2 – друга ПВП.

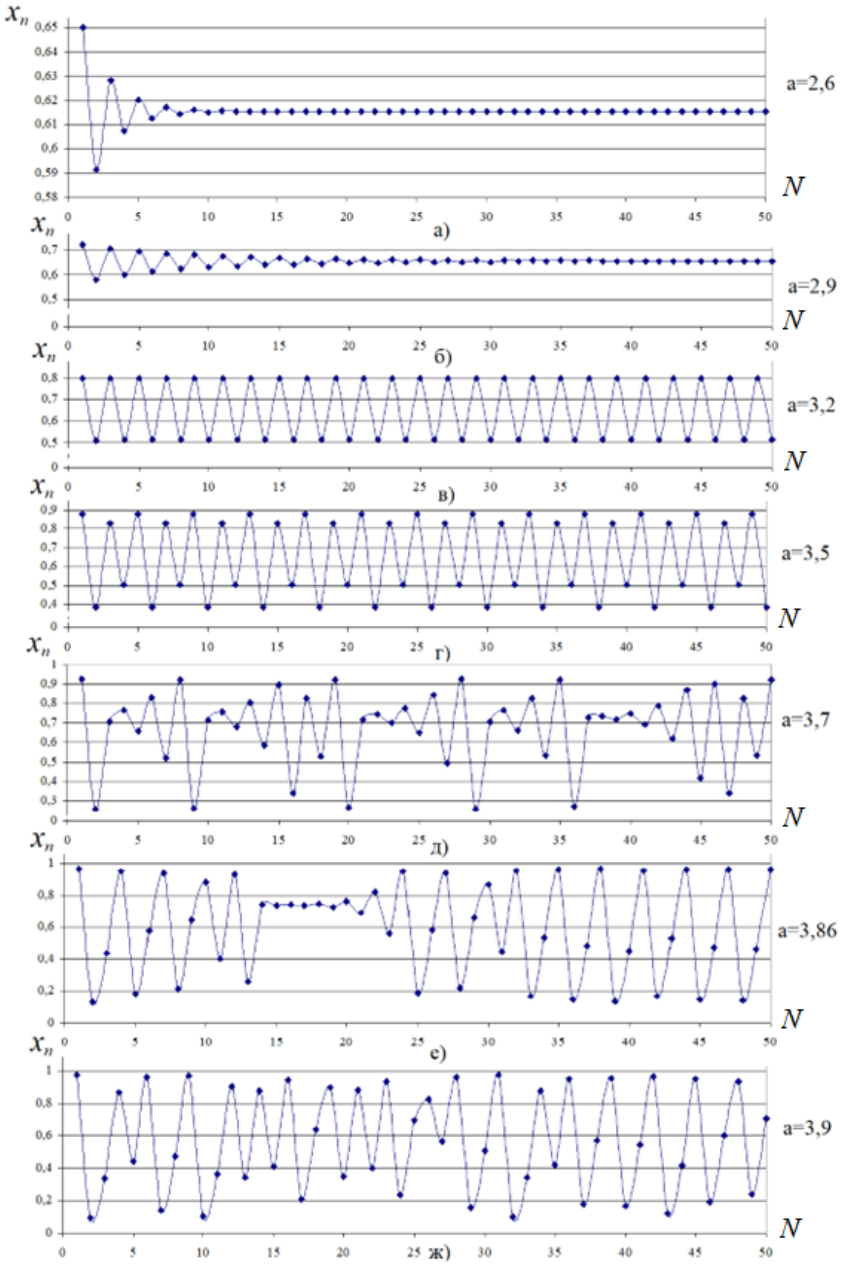

Рис 1. Діаграми хаотичного процесу логістичного відображення при різних значеннях параметру a

На рис. 2 надана залежність коефіцієнта кореляції двох хаотичних процесів для значень: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}90001$ і $x_2 = 0{,}5$ – друга ПВП. При незначній зміні параметра $a_1 = 3{,}9$ і $a_2 = 3{,}90001$ спочатку спостерігається суттєва залежність між числами ($k_{ji} = 0{,}08...0{,}8$), проте при значенні вибірок $N > 300$ коефіцієнт кореляції $k_{ji} \to 0$.

На рис. 3 надана залежність коефіцієнта кореляції двох хаотичних процесів для значень: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}5001$ – друга ПВП. Аналогічно, при незначній зміні початкових значень $x_1 = 0{,}5$ і $x_2 = 0{,}5001$, також спочатку спостерігається суттєва залежність між числами ($k_{ji} = 0{,}08...0{,}7$), проте при значенні вибірок $N > 750$ коефіцієнт кореляції $k_{ji} \to 0$.

На рис. 4 надана залежність коефіцієнта кореляції двох хаотичних процесів логістичного відображення від кількості двійкових чисел при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}75$ – друга ПВП. Для цих процесів спочатку також спостерігається деяка залежність між числами ПВП, проте при значенні вибірок $N > 400$ коефіцієнт кореляції k_{ji} зменшується та повільно прагне до нуля.

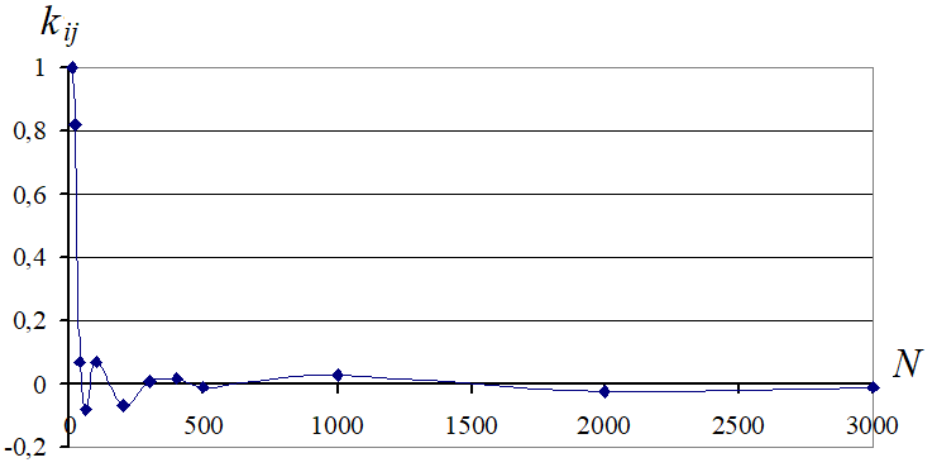

Рис 2. Залежність кореляції двох хаотичних процесів логістичного відображення від N та при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}90001$ і $x_2 = 0{,}5$ – друга ПВП

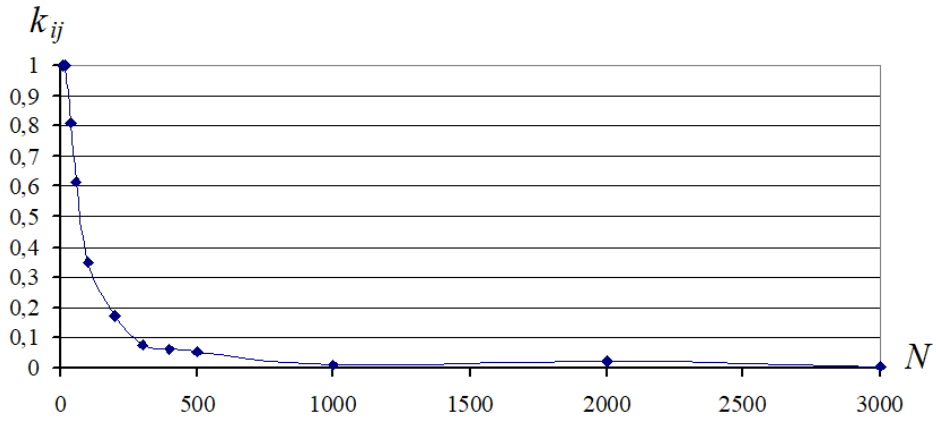

Рис. 3. Залежність кореляції двох хаотичних процессів логістичного відображення від N та при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}5001$ – друга ПВП

На рис. 5 надана залежність коефіцієнта кореляції двох хаотичних процессів логістичного відображення від кількості двійкових чисел при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}2$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}95$ – друга ПВП. З рисунку бачимо, що спочатку спостерігається деяка залежність між числами ПВП з $k_{12} \approx 0{,}1$. При значеннях вибірок $N > 500$ коефіцієнт кореляції зменшується і складає $k_{12} \approx 0{,}05$, що свідчить про наявність деякої залежності цих процесів.

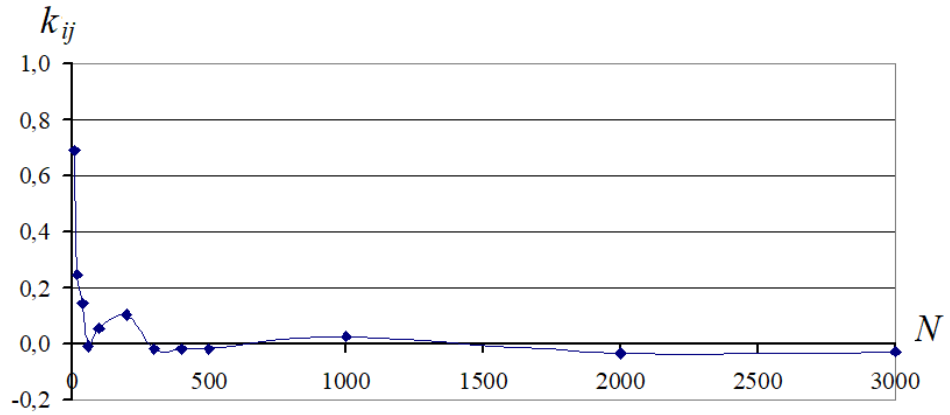

Рис. 4. Залежність кореляції двох хаотичних процессів логістичного відображення від N та при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}5$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}75$ – друга ПВП

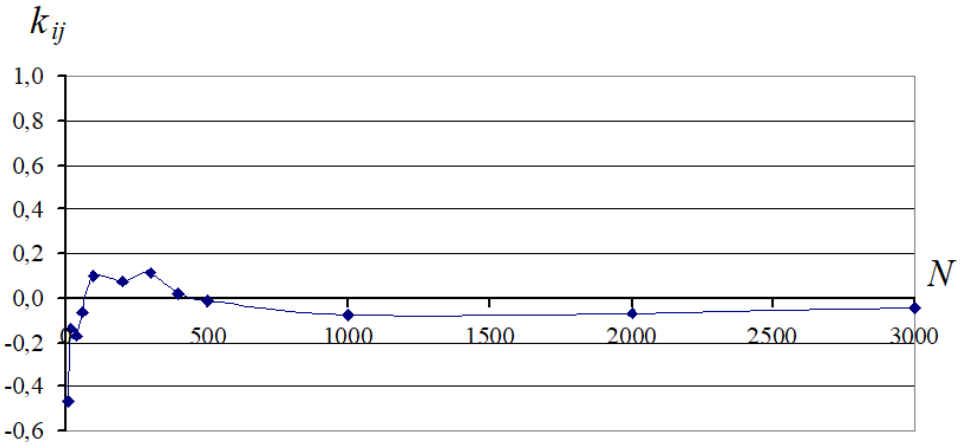

Рис. 5. Залежність кореляції двох хаотичних процессів логістичного відображення від N та при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}2$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}95$ – друга ПВП

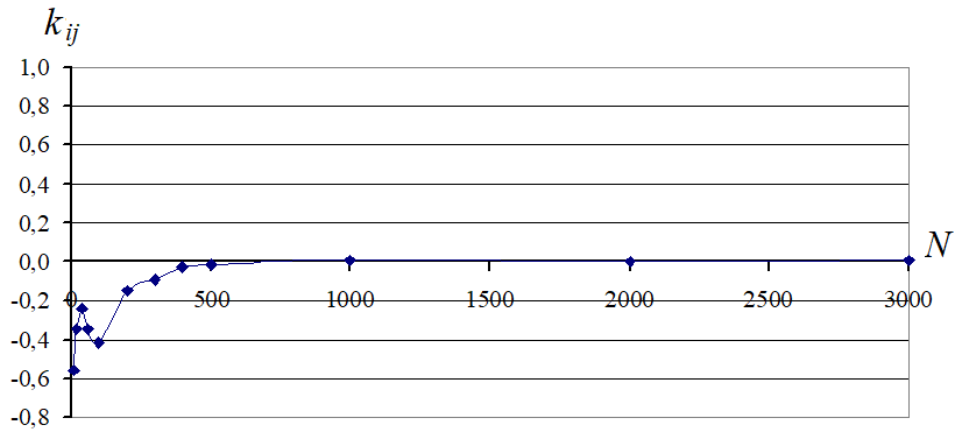

Рис. 6. Залежність кореляції двох хаотичних процессів логістичного відображення від N та при значеннях: $a_1 = 3{,}9$ і $x_1 = 0{,}2$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}35$ – друга ПВП

На рис. 6 надана залежність кореляції двох хаотичних процесів для значень: $a_1 = 3{,}9$ і $x_1 = 0{,}2$ – перша ПВП; $a_2 = 3{,}9$ і $x_2 = 0{,}35$ – друга ПВП. Бачимо, що при значеннях вибірок $N > 500$ коефіцієнт кореляції k_{ji} зменшується та практично дорівнює нулю.

Висновки з даного дослідження
і перспективи подальшого розвитку у даному напрямі

Результати досліджень довели доцільність застосування генераторів хаосу для формування гама послідовностей для потокового шифрування. Використання гамма послідовностей на основі динамічного хаосу обґрунтовується відповідними статистичними властивостями. Встановлено, що незначна зміна початкових параметрів генератора хаосу призводить до суттєвої зміни значень коливання, що дає можливість формувати різні траєкторії хаотичного процесу.

Виявлені властивості є перспективою для створення практично необмеженої кількості комбінацій псевдовипадкових послідовностей різної довжини. Проте, результати досліджень показали, що для виконання умови $k_{ji} \to 0$ потрібно обирати відповідні початкові показники хаотичних послідовностей $X_j(a_j, x_j)$ і $X_i(a_i, x_i)$.

Література

1. Лунтовський А.О. Мультисервісні мобільні платформи / А.О. Лунтовський, М.В. Захарченко, А.І. Семенко – К.: ПВП «Задруга», 2014. – 214 с.

2. Захарченко М.В. Протоколи, термінальне обладнання та інформаційна безпека у мережах наступного покоління : [навч. посібник] / М. В. Захарченко, О. О. Вараксін, В. Г. Кононович, С. О. Вараксін; за ред. М. В. Захарченка. – Одеса: Фенікс, 2008. – 128 с.

3. Банкет В. Л. Защита информации в системах телекоммуникации: Учеб. пособие / В. Л. Банкет, Н. В. Захарченко, А. В. Дырда; Под редакцией Банкет В. Л. – УГАС: Одесса, 1997. – 95 с.

4. Шахтарин Б.И. Генераторы хаотических колебаний / Шахтарин Б.И. – М. : Гелиос АРВ, 2007. – 248 с.

5 Корчинский В. В. Повышение структурной скрытности передачи систем с хаотическими сигналами / В.В. Корчинский // Восточно-Европейский журнал передовых технологий //научный журнал. – Харьков: Технологический центр, 2013. – № 1/9 (61). – С.53-57.

6. Захарченко Н.В. Метод формирования сигнальных конструкций на основе хаотических и таймерных сигналов в системах передачи конфиденциальной информации / Н.В. Захарченко, В.В. Корчинский, Б.К. Радзимовский // Наукові праці ОНАЗ ім. О. С. Попова. –2011. – № 2. – С. 3–7.

7. Korchynskyi V.V. Increase of stealth transmission based on timer signals and linear frequency modulation / Korchynskyi V.V., Kildishev V.I., Berdnikov A.M., Smazhenko K.O.// Наукові праці ОНАЗ ім.. О.С. Попова, Одеса, 2020 р.

8. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – Р. – 65-69.

9 Корчинський В.В. Оцінка структурної скритності сигнальних конструкцій на основі хаотичних сигналів в системах передачі конфіденційної інформації / В.В. Корчинський // Наукові праці ОНАЗ ім. О.С. Попова, 2012, No 1 - С 77-81.

References

1. Luntovskyi A.O. Multyservisni mobilni platformy / A.O. Luntovskyi, M.V. Zakharchenko, A.I. Semenko – K.: PVP «Zadruha», 2014. – 214 s.

2. Zakharchenko M.V. Protokoly, terminalne obladnannia ta informatsiina bezpeka u merezhakh nastupnoho pokolinnia : [navch. posibnyk] / M. V. Zakharchenko, O. O. Varaksin, V. H. Kononovych, S. O. Varaksin; za red. M. V. Zakharchenka. – Odesa: Feniks, 2008. – 128 s.

3. Banket V. L. Zashchyta ynformatsyy v systemakh telekommunykatsyy: Ucheb. posobye / V. L. Banket, N. V. Zakharchenko, A. V. Dыrda; Pod redaktsyei Banket V. L. – UHAS: Odessa, 1997. – 95 s.

4. Shakhtaryn B.Y. Heneratorы khaotycheskykh kolebanyi / Shakhtaryn B.Y. – M. : Helyos ARV, 2007. – 248 s.

5 Korchynskyi V. V. Povышenye strukturnoi skrытnosty peredachy system s khaotycheskymy syhnalamy / V.V. Korchynskyi // Vostochno-Evropeiskyi zhurnal peredovыkh tekhnolohyi //nauchnыi zhurnal. – Kharkov: Tekhnolohycheskyi tsentr, 2013. – № 1/9 (61). – S.53-57.

6. Zakharchenko N.V. Metod formyrovanyia syhnalnыkh konstruktsyi na osnove khaotycheskykh y taimernыkh syhnalov v systemakh peredachy konfydentsyalnoi ynformatsyy / N.V. Zakharchenko, V.V. Korchynskyi, B.K. Radzymovskyi // Naukovi pratsi ONAZ im. O. S. Popova. –2011. – № 2. – S. 3–7.

7. Korchynskyi V.V. Increase of stealth transmission based on timer signals and linear frequency modulation / Korchynskyi V.V., Kildishev V.I., Berdnikov A.M., Smazhenko K.O.// Наукові праці ОНАЗ ім.. О.С. Попова, Одеса, 2020 р.

8. Korchynskyi V.V. A method for formation parameters of chaos generators based on hash functions / Korchynskyi V.V., Kildishev V.I., K. Alfaion, Smazhenko K.O., Valyhurskyi Y.P., Polishchuk K.V.// Наукові праці ОНАЗ. – Одеса: ОНАЗ, 2020. – № 2, – Р. – 65-69.

9 Korchynskyi V.V. Otsinka strukturnoi skrytnosti syhnalnykh konstruktsii na osnovi khaotychnykh syhnaliv v systemakh peredachi konfidentsiinoi informatsii / V.V. Korchynskyi // Naukovi pratsi ONAZ im. O.S. Popova, 2012, No 1 - S 77-81.