УДК 004.056.55, 004.942

ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ХАОТИЧНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ПОБУДОВАНИХ ІЗ ВИКОРИСТАННЯМ НЕЧІТКОЇ ЛОГІКИ

DOI 10.36994/2788-5518-2021-01-01-04[4]

***Кушнір М.Я.**, к.ф.-м.н., доц. Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна.* kushnirnick@gmail.com

***Семенко А.І.,** д.т.н. проф. Відкритий міжнародний університет розвитку людини «УКРАЇНА», Київ, Україна.*

***Косован Г.В.**, к.т.н., Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна. kosovan.gregoriy@gmail.com*

***Крояло П.М.,** Чернівецький національний університет імені Юрія Федьковича, Чернівці, Україна. fredis0629@gmail.com*

***Анотація.** Телекомунікаційні системи із широкосмуговим сигналом мають покращену стійкість до завад. Проте такі системи також потрібно захищати і від перехоплення інформації. Для захисту таких систем використовуються спеціально розроблені генератори бітових послідовностей. Використання відомих псевдовипадкових рівнянь для створення систем не забезпечує їх високої конфіденційності через можливість їх вибору при отриманні сигналу. Значного збільшення конфіденційності системи можна досягти, використовуючи псевдовипадкові послідовності, засновані на використанні хаосу. Метою статті є розробка методики створення псевдовипадкових послідовностей на основі правил нечіткої логіки та одновимірних хаотичних систем, а також аналіз статистичних характеристик псевдовипадкових послідовностей, сформованих таким чином. В результаті аналізу було запропоновано реалізувати генератор на основі двох одновимірних хаотичних систем та перевірити статистичні характеристики послідовностей сформованих таким генератором.*

***Ключові слова:** генератор, хаос, одновимірне відображення, псевдовипадкова послідовність, статистичний тест.*

INVESTIGATION OF PROPERTIES OF CHAOTIC GENERATORS OF PSEUDO-RANDOM SEQUENCES CONSTRUCTED USING FUZZY LOGIC

***Mykola Kushnir,** Ph.D., Docent. Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. kushnirnick@gmail.com*

***Anatolii Semenko** Doctor of Technical Sciences, Professor, Open International University of Human Development "UKRAINE", Kyiv, Ukraine.*

***Hryhorii Kosovan,** Ph.D., Assistant. Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. kosovan.gregoriy@gmail.com*

[4] Кушнір М.Я., Семенко А.І., Косован Г.В., Крояло П.М.

Petro Kroialo, *Ph.D., Postgraduate. Yuriy Fedkovych Chernivtsi National University, Chernivtsi, Ukraine. fredis0629@gmail.com*

Abstract. *Telecommunication systems with a broadband signal spectrum have improved immunity to interference. However, such systems also need to be protected from information interception. Specially designed pseudo-random bit sequence generators are used for this purpose. The use of known pseudo-random equations does not ensure their high confidentiality due to the possibility of their disclosure upon receipt of the signal. A significant increase in system confidentiality can be achieved by using pseudo-random sequences based on the use of chaotic mappings.*

Chaotic signals are essentially pseudo-random, but they are generated by deterministic systems. All computer models of chaos are only an approximation to mathematical chaos. Any analysis of these sequences does not allow them to be reproduced, so they have significant advantages when used to expand the signal spectrum and create a pseudo-noise broadband signal.

The aim of the article is to develop a method of creating pseudo-random sequences based on the rules of fuzzy logic and one-dimensional chaotic systems, as well as to analyze the statistical characteristics of pseudo-random sequences formed in this way. The study used the three most well-known one-dimensional mappings, namely logistic, square and cubic, and presented the results of statistical verification of sequences formed using the rules of fuzzy logic. As a result, a pseudo-random bit generator was proposed and implemented using fuzzy logic rules and two one-dimensional chaotic systems, and the statistical characteristics of the sequences generated by such a generator were verified. The results show that the obtained sequences satisfy most of the tests from the NIST set.

The use of fuzzy logic-based pseudo-random sequences based on the rules of fuzzy logic and deterministic chaos is effective for building broadband telecommunication systems, which will allow them to ensure a high degree of confidentiality in the transmission of information.

Keywords: *generator, chaos, one-dimensional map, pseudo-random sequence, statistical test.*

ИСЛЕДОВАНИЕ СВОЙСТВ ХАОТИЧЕСКИХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ПОСТРОЕНЫХ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОЙ ЛОГИКИ

Кушнир Н.Я.*, к.ф.-м.н., доц. Черновицкий национальный университет имени Юрия Федьковича, Черновци, Украина. kushnirnick@gmail.com*

Семенко А.И., *д.т.н., проф., Открытый международный университет развития человека «УКРАИНА», Киев, Украина.*

Косован Г.В.*, к.т.н. Черновицкий национальный университет имени Юрия Федьковича, Черновци, Украина. kosovan.gregoriy@gmail.com*

Крояло П.М. *Черновицкий национальный университет имени Юрия Федьковича, Черновци, Украина.fredis0629@gmail.com*

Аннотация*. Телекоммуникационные системы с широкополосным сигналом имеют улучшенную устойчивость к помехам. Однако такие системы также нужно защищать и от перехвата информации. Для защиты таких систем используются специально разработанные генераторы битовых последовательностей. Использование известных псевдослучайных уравнений для создания систем не обеспечивает их высокой конфиденциальности из-за возможности их выбора при получении сигнала. Значительное увеличение конфиденциальности системы*

можно достичь, используя псевдослучайные последовательности, основанные на использовании хаоса. Целью статьи является разработка методики создания псевдослучайных последовательностей на основе правил нечеткой логики и одномерных хаотических систем, а также анализ статистических характеристик псевдослучайных последовательностей, сформированных таким образом. В результате анализа было предложено реализовать генератор на основе двух одномерных хаотических систем и проверить статистические характеристики последовательностей сформированных таким генератором.

Ключевые слова: *генератор, хаос, одномерное отображение, псевдослучайная последовательность, статистический тест.*

Вступ

Постійне збільшення залежності від цифрової техніки призводить до пошуку нових та більш досконалих методів захисту інформації. В даний час найбільш велика кількість інформації передається по відкритим каналам зв'язку і в процесі передавання її необхідно захищати. Одним із найбільш ефективних способів захисту інформації являється її шифрування з подальшим передаванням. Шифрування та розшифрування є загальними методами в криптографії, що використовуються для перетворення інформації з явної форми в закриту і навпаки. Проте поряд із розробленням нових методів шифрування і вдосконаленням старих розвиваються методи зламування реалізованих методів шифрування. Тому в наш час вдосконалюються існуючі методи шифрування та розробляються нові на основі альтернативних технік, таких як детермінований хаос.

Хаос широко вивчається багатьма науковцями в області нелінійної динаміки. Використовуючи нестандартний підхід, а саме нелінійної динаміки, було досліджено багато різних варіантів застосувань детермінованого хаосу у реальних системах зв'язку та передачі даних [1].

На початку 1990-х років стало зрозуміло, що одним із потенційних застосувань теорії хаосу є забезпечення захищеного зв'язку. Це ґрунтувалося на відкритті Пекорою та Керолом хаотичних принципів синхронізації. Хаотичні відображення використовуються в різних програмах захисту даних та зображень через таку особливість, як чутливість до початкових значень та параметрів управління. Саме така чутливість робить їх хорошими кандидатами для побудови генераторів псевдовипадкових бітів та криптографічних систем на їх основі [2].

Одним із перспективних напрямків в криптографії є розроблення генераторів псевдовипадкових бітів на основі нечіткої логіки та детермінованих хаотичних систем.

Генератори псевдовипадкових бітів на основі нечіткої логіки та одновимірних відображень

На основі хаотичних систем реалізуються як генератори псевдовипадкових бітів так і методи шифрування на основі математичних перетворень. В літературі відома велика кількість різних генераторів ПВП бітів,

що використовують як порогові методи для формування бітових послідовностей так і формують послідовності шляхом перетворення десяткового значення в бітове представлення [3].

В даній роботі запропоновано спосіб генерування ПВП бітів із застосуванням хаотичних систем та нечіткої логіки для формування бітових послідовностей із наступним їх використанням для шифрування зображень. Нечітка логіка в розумінні детермінованого хаосу - це розділ математичної логіки, що призначений для вирішення проблеми прийняття нечітких рішень шляхом призначення певного бітового значення для нечіткого діапазону вихідних значень хаотичної системи, щоб отримати доступний максимально точний результат. Нечітка логіка покликана вирішувати проблему генерування бітів шляхом розгляду всієї наявної інформації і приймаючи найкраще можливе рішення з генерованого вихідного значення хаотичної системи. Після отримання певних бітових послідовностей їх необхідно перевірити на відповідність критеріям статистичних тестів NIST, для підтвердження ефективності застосування генераторів із нечіткою логікою в криптографії.

Для початку нами було обрано три одновимірних хаотичних відображення для генерування ПВП бітів із застосуванням нечіткої логіки, а саме логістичне (1), квадратне (2) та кубічне (3) відображення.

$$x_{n+1} = rx_n\left(1 - x_n\right) \tag{1}$$

$$y_{n+1} = -\mu y_n^2 \tag{2}$$

$$z_{n+1} = a - bz_n + z_n^3 \tag{3}$$

де $x_0 \in (0;1)$, $y_0 \in (-1;1)$ та $z_0 \in (-0,6;1,6)$ – початкові стани хаотичних систем, $r \in \left(3,57;4\right]$, $\mu \in \left(1,4;2\right]$, $a \in \left(\text{-}0,6;0,6\right)$ та $b \in \left(0,8;2,5\right)$ - параметри керування. В залежності від того, яким буде вибраний параметр керування хаотичною системою, отримується різний діапазон вихідних значень та по різному формуватимуться бітові послідовності. Тому для того, щоб можливо було сформувати бітову послідовність, необхідно вказати правила формування послідовності бітів за допомогою нечіткої логіки.

Для реалізації генератору ПВП бітів нами використано наступне правило нечіткої логіки:

1. Спочатку розбиваємо діапазон вихідних значень кожної із хаотичних систем на 10 інтервалів.
2. Кожен із цих інтервалів ділиться на 25 під інтервалів крім останнього, він ділиться на 30.
3. Розмір кожного із інтервалів визначається в залежності від вибраних значень параметрів керування хаотичних систем і для обох систем вони відрізнятимуться між собою.

Наприклад, правило нечіткої логіки для логістичного відображення з значенням параметру керування виглядає наступним чином:

Якщо вхід = 0-0,1, то вихід = 0-25
Якщо вхід = 0,11-0,2, то вихід = 26-50
Якщо вхід = 0,21-0,3, то вихід = 51-75
Якщо вхід = 0,31-0,4, то вихід = 76-100
Якщо вхід = 0,41-0,5, то вихід = 101-125
Якщо вхід = 0,51-0,6, то вихід = 126-150
Якщо вхід = 0,61-0,7, то вихід = 151-175
Якщо вхід = 0,71-0,8, то вихід = 176-200
Якщо вхід = 0,81-0,9, то вихід = 201-225
Якщо вхід = 0,91-1, то вихід = 226-255.

Аналогічним чином розбиваються вихідні діапазони квадратного і кубічного відображення та формуються ПВП бітів. На рис. 1 приведена блок схема генератора ПВП бітів із застосуванням нечіткої логіки та одновимірних хаотичних систем.

В процесі дослідження статистичних характеристик бітових послідовностей, ПВП бітів формувались окремо трьома одновимірними відображеннями з різними початковими умовами та параметрами керування. Результати досліджень ПВП бітів на відповідність критеріїв статистичних тестів, формованих логістичним, квадратним та кубічним одновимірним відображенням, представлені в таблицях 1, 2 та 3.

Таблиця 1

Результати тестування генерованої послідовності, сформованої логістичним відображенням

Тип тесту	Отримане значення P_{value}	Пропорція
Частотний (монобітний тест)	0.616305	0.680
Частотний тест по блоках	0.494392	0.350
Тест серій	0.000000	0.000
Тест найдовшої серії з одиниць	0.000000	0.000
Тест рангу бінарних матриць	0.011791	0.630
Тест на основі дискретного перетворення Фур'є	0.062821	0.110
Тест на збіг з шаблоном без перекриття	0.595549	0.980
Тест шаблона з перекриттям	0.000000	0.000
Універсальний математичний тест Мауера	0.000000	0.000
Тест лінійної складності	0.678686	0.990
Тест серій	0.016717	0.670
Тест на основі апроксимації ентропії	0.000000	0.000
Тест накопичувальних сум	0.249284	0.710
Тест випадкових блукань	0.000000	1.000

Тест варіантів випадкових блукань	0.000000	1.000

Таблиця 2:

Результати тестування генерованої послідовності, сформованої квадратним відображенням

Тип тесту	Отримане значення P_{value}	Пропорція
Частотний (монобітний тест)	0.071177	0.770
Частотний тест по блоках	0.000000	0.820
Тест серій	0.000000	0.000
Тест найдовшої серії з одиниць	0.000000	0.000
Тест рангу бінарних матриць	0.000003	0.970
Тест на основі дискретного перетворення Фур'є	0.055361	0.850
Тест на збіг з шаблоном без перекриття	0.181557	0.770
Тест шаблона з перекриттям	0.350485	0.180
Універсальний математичний тест Мауера	0.000000	0.000
Тест лінійної складності	0.419021	0.960
Тест серій	0.000000	0.000
Тест на основі апроксимації ентропії	0.000000	0.000
Тест накопичувальних сум	0.249284	0.140
Тест випадкових блукань	0.350485	0.960
Тест варіантів випадкових блукань	0.000000	0.000

Таблиця 3:

Результати тестування генерованої послідовності, сформованої кубічним відображенням

Тип тесту	Отримане значення P_{value}	Пропорція
Частотний (монобітний тест)	0.935716	0.980
Частотний тест по блоках	0.000123	1.000
Тест серій	0.494392	0.980
Тест найдовшої серії з одиниць	0.000000	0.000
Тест рангу бінарних матриць	0.000000	0.430
Тест на основі дискретного перетворення Фур'є	0.000000	0.790
Тест на збіг з шаблоном без перекриття	0.574903	1.000
Тест шаблона з перекриттям	0.000000	0.490
Універсальний математичний тест Мауера	0.000000	0.000
Тест лінійної складності	0.657933	0.980
Тест серій	0.000000	0.000

Тест на основі апроксимації ентропії	0.000000	0.000
Тест накопичувальних сум	0.171867	0.990
Тест випадкових блукань	0.000000	0.180
Тест варіантів випадкових блукань	0.003712	0.970

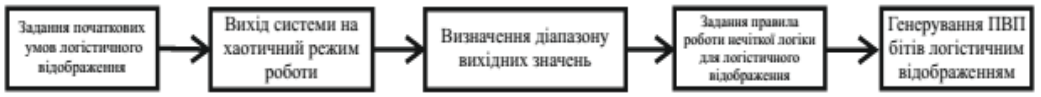

Рис. 1. Блок схема генератора ПВП бітів із застосуванням нечіткої логіки на основі одновимірної хаотичної системи

Мінімальне прохідне значення для кожного статистичного тесту для кожної послідовності, генерованої одновимірним відображенням, за винятком тестів варіантів випадкових блукань, приблизно = 0.960.

З отриманих результатів випливає, що ПВП бітів, сформовані із використанням нечіткої логіки та одновимірних хаотичних систем, задовольняють умовам набору статистичних тестів NIST частково. Тому не достатньо використати лише одне одновимірне хаотичне відображення для формування ПВП бітів.

Для покращення отриманих результатів нами запропоновано використовувати одразу комбінацію з двох одновимірних хаотичних систем для генерування ПВП бітів із застосуванням нечіткої логіки.

Розробка вдосконаленого генератори псевдовипадкових бітів із застосуванням нечіткої логіки та комбінації з двох одновимірних хаотичних відображень

Використання комбінацій з двох одновимірних хаотичних відображень для формування ПВП бітів – це один із можливих шляхів покращення статистичних властивостей бітових послідовностей, генерованих із застосуванням нечіткої логіки. Проте такий крок теж потребує перевірки на відповідність критеріїв статистичних тестів NIST.

Нами запропоновано використати логістичне (1) та кубічне відображення (3) для побудови генератора ПВП бітів із покращеними статистичними властивостями. В запропонованому генераторі кожна із хаотичних систем окремо генерує бітову послідовність із застосуванням нечіткої логіки. Потім обидві послідовності поєднуються між собою шляхом застосування логічної операції □OR для формування остаточної вихідної послідовності бітів [4].

На рис. 2 приведена блок схема генератора ПВП бітів із нечіткою логікою на основі двох хаотичних систем.

Спочатку для кожного відображення вибирається початкова умова та параметри керування. Далі, для того, щоб правило нечіткої логіки чітко застосовувалось, необхідно спершу визначити діапазон вихідних значень кожного одновимірного відображення:

1. Для цього для виходу на хаотичний режим необхідно спочатку здійснити 100 ітерацій кожною із хаотичних систем.

2. Потім визначити мінімальне та максимальне вихідне значення кожної із хаотичних систем.

3. Отриманий діапазон вихідних значень ділимо за правилом, як показано для логістичного відображення і після формування правил нечіткої логіки генеруємо бітові послідовності.

Результати досліджень ПВП бітів на відповідність критеріїв статистичних тестів, сформованих запропонованим генератором на основі двох хаотичних відображень та нечіткої логіки представлено в таблиці 4.

Рис. 2. Блок схема генератора ПВП бітів із нечіткою логікою на основі двох хаотичних систем

Таблиця 4

Результати тестування генерованої послідовності, сформованої генератором на основі двох хаотичних відображень

Тип тесту	Отримане значення P_{value}	Пропорція (Proportion)
Частотний (монобітний тест)	0.851383	0.980
Частотний тест по блоках	0.383827	0.980
Тест серій	0.816537	0.980
Тест найдовшої серії з одиниць	0.0	0.080
Тест рангу бінарних матриць	0.455937	0.970
Тест на основі дискретного перетворення Фур'є	0.191687	0.980
Тест на збіг з шаблоном без перекриття	0.719747	0.980
Тест шаблона з перекриттям	0.419021	0.970
Універсальний математичний тест Мауера	0.000123	0.970
Тест лінійної складності	0.090936	1.000
Тест серій	0.000000	0.000

Тест на основі апроксимації ентропії	0.366918	0.949
Тест накопичувальних сум	0.825537	0.980
Тест випадкових блукань	0.595549	0.983
Тест варіантів випадкових блукань	0.334538	0.983

З отриманих результатів випливає, що отримана послідовність пройшла практично весь набір статистичних тестів, що свідчить про високу ефективність роботи запропонованого генератора. Крім того результати показали, що мінімальне значення проходження кожного тесту, за винятком Тесту варіантів випадкових блукань складає приблизно 0.960, а мінімальне значення проходження тестів варіантів випадкових блукань складає приблизно 0.949. На рис. 3 також представлена залежність значення рівня пропорції та номеру теста.

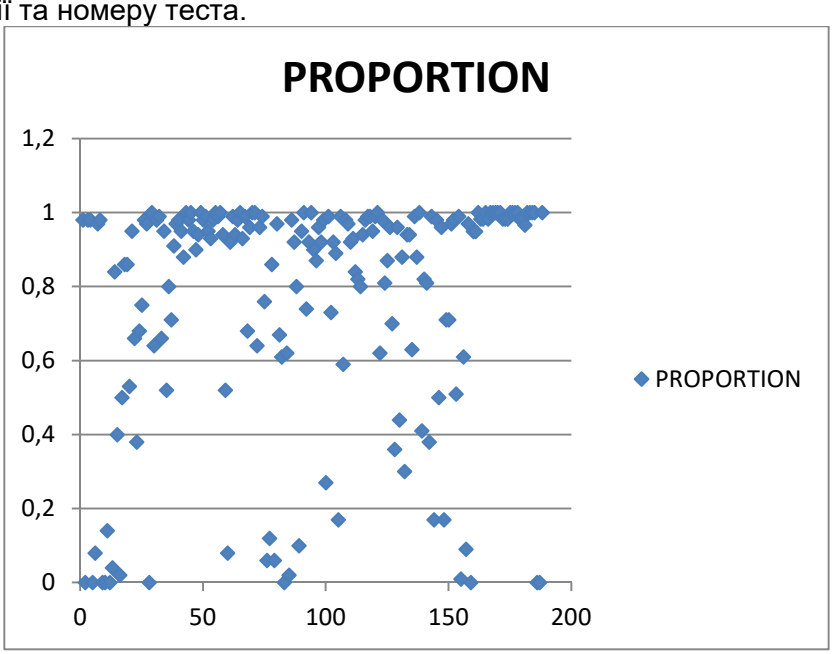

Рис. 3. Залежність значення рівня пропорції та номеру теста для генерованої послідовності бітів

Висновки

Отже, підсумовуючи вище викладене, варто відмітити наступні результати досліджень:

В даній роботі запропоновано метод генерування ПВП бітових послідовностей із використанням правил нечіткої логіки та на основі хаотичних одновимірних відображень. В процесі дослідження було використано три найбільш відомі одновимірні відображення, а саме логістичне, квадратне та кубічне. В результаті перевірки було встановлено, що ПВП сформовані такими відображеннями відповідають умовам тестів із набору NIST частково. Тому не

бажано використовувати лише одне одновимірне хаотичне відображення для формування послідовностей бітів із застосуванням правил нечіткої логіки.

Для вирішення цієї проблеми було запропоновано реалізувати генератор ПВП бітів із застосуванням двох одновимірних хаотичних систем, а саме логістичного і кубічного відображень. Перевірка статистичних властивостей послідовностей сформованим таким генератором продемонструвала значно кращі результати, тобто сформовані послідовності відповідають більшості із тестів з набору NIST. Також використання двох хаотичних систем збільшило кількість ключів, що необхідно задати для їх формування і як наслідок зростає і стійкість сформованих послідовностей до різного роду атак [5]. Таким чином ПВП бітів сформовані із застосуванням правила нечіткої логіки та двох хаотичних систем може бути використано для створення захищених телекомунікаційних систем, а також для розробки методів шифрування інформації на їх основі.

Література

1. P. Stavroulakis, Chaos Applications in Telecommunications. London, U.K.: Taylor & Francis, 2005.
2. Kushnir, M., Vovchuk, D., Haliuk, S., Ivaniuk, P., & Politanskyi, R. (2021). Approaches to Building Chaotic Communication System (pp. 207–227). https://doi.org/10.1007/978-3-030-43070-2_11
3. Semenko A.. Kushnir N. Bokla N. Kosovan G. Features of creating based on chaos pseudo-random sequences**.** Modern Problems of Radio Enginiring,Telecommunications, and Computer Sciens . Proceedings of the IIth International Conference TCSET' 2018. Lviv-Slavsco,Ukraine.February 20-24 , 2018.Pp338-342.
4. СеменкоА.І. Спосіб формування широкосмугового псевдошумового, сигналу/ М.Я. Кушнір, Н.І. Бокла // Пат.125337, Україна: ПКН04В.3/60(2006.01), Н04В3/00. № u201711149; заявл. 14.11.2017;опубл.10.05.2018, бюл. № 9.
5. Kocarev L. Chaos-based cryptography: A brief overview / Kocarev L. // IEEE Circuits and Systems Maganize. – 2001. – №1. – P. 6–21.

Reference

1. P. Stavroulakis, Chaos Applications in Telecommunications. London, U.K.: Taylor & Francis, 2005.
2. Kushnir, M., Vovchuk, D., Haliuk, S., Ivaniuk, P., & Politanskyi, R. (2021). Approaches to Building a Chaotic Communication System (pp. 207–227). https://doi.org/10.1007/978-3-030-43070-2_11
3. Semenko A.. Kushnir N. Bokla N. Kosovan G. Features of creating based on chaos pseudo-random sequences**.** Modern Problems of Radio Enginiring,Telecommunications, and Computer Sciens . Proceedings of the IIth International Conference TCSET' 2018. Lviv-Slavsco,Ukraine.February 20-24 , 2018.Pp338-342.
4. Semenko A., Kushnir M, Bokla N. Sposib formuvannia shyrokosmugovogo psevdoshumovogo sygnalu. Patent 125337 Ukraine: МПКН04В. 3/60(2006.01), H04B 3/00. № u201711149; zaiavleno. 14.11.2017 opubl. 10.05.2018,bulet. № 9 (in Ukr).
5. Kocarev L. Chaos-based cryptography: A brief overview / Kocarev L. // IEEE Circuits and Systems Maganize. – 2001. – №1. – P. 6–21.