В роботі представлено алгоритм генерування ключа шифрування інформації для телекомунікаційних систем зв'язку з використанням двох динамічних систем, на основі яких формується послідовність бітів, що формує ключову послідовність для шифрування інформації. Також проведено моделювання роботи основних елементів генератора ключа в середовищах LabView та Matlab. Досліджена оцінка захищеності згенерованого ключа шифрування

Ключові слова: криптографія, шифрування, алгоритм, ключ, одномірне відображення, хаотична динамічна система

В работе представлен алгоритм генерирования ключа шифрования информации для телекоммуникационных систем связи с использованием двух динамических систем, на основе которых формируется последовательность битов, которая формирует ключевую последовательность для шифрования информации. Также было проведено моделирование работы основных элементов генератора ключа в средах LabView и Matlab. Исследована оценка защищенности сгенерированного ключа шифрования

Ключевые слова: криптография, шифрование, алгоритм, ключ, одномерное отображение, хаотическая динамическая система

УДК 621.391.7

МОДЕЛЮВАННЯ АЛГОРИТМУ ГЕНЕРУВАННЯ КЛЮЧА ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ДИНАМІЧНИХ СИСТЕМ

Г. В. Косован
Аспірант*
E-mail: spell1985@mail.ru
М. Я. Кушнір
Кандидат фізико-математичних наук, доцент*
E-mail: kushnirnick@gmail.com
Л. Ф. Політанський
Доктор технічних наук, професор*
E-mail: politansky@ukr.net
*Кафедра радіотехніки та інформаційної безпеки
Чернівецький національний університет імені Юрія Федьковича
вул. Коцюбинського, 2, м. Чернівці, Україна, 58000

1. Вступ

З розвитком інформаційних технологій, комп'ютерної техніки та засобів перехоплення інформації гостро постало питання захисту передавання інформаційних повідомлень від несанкціонованого доступу по телекомунікаційних системах зв'язку. Найбільш ефективним засобом захисту інформації є криптографічні алгоритми шифрування інформації, але традиційні методи шифрування інформації є добре відомими, а деякі з них вважаються зламаними.

Тому існує потреба в розробленні нових алгоритмів шифрування на основі теорії хаосу [1].

Значна частина теорії нелінійних динамічних систем відома як теорія хаосу. Хаос є довготривалою непередбачуваною поведінкою детермінованих динамічних систем, обумовленою їх чутливістю до початкових умов [1 – 3].

Використовуючи ці властивості дослідники намагаються створити нові криптографічні алгоритми [2], тобто підібрати відповідні хаотичні моделі, що задовільняють умовам криптографічної захищеності інформації. В даній роботі розроблений алгоритм генерування ключа шифрування інформації для телекомунікаційних систем зв'язку, проведено моделювання роботи генератора ключа в середовищах LabView та Matlab, а також досліджені його властивості.

2. Загальна схема криптографічної системи

Криптографія в цілому є процесом закриття інформації, що полягає в унеможливленні несанкціонованого доступу до конфіденційної інформації [4]. Прикладом найпростішої реалізації потокового алгоритму шифрування з секретним ключем є схема приведена на рис. 1.

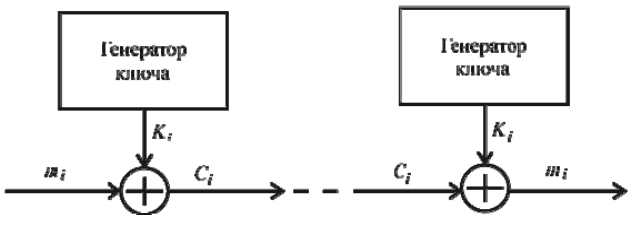

Рис. 1. Структурна схема найпростішого прикладу реалізації потокового шифру

Основним елементом алгоритму шифрування є генератор ключа, що генерує потік бітів $K_0, K_1, K_2, \ldots, K_{m-1}$, у вигляі послідовностей логічних нулів та одиниць.

З метою отримання зашифрованого потоку даних вхідна інформація $M = \{0,1,\ldots,m-1\}$, де m - порядковий номер біту, шумується з ключовою послідовністю за операцією XOR для отримання зашифрованого потоку даних C:

$m_i \oplus K_i = C_i$.

Дешифрування інформації здійснюється у зворотному порядку:

$C_i \oplus K_i = (m_i \oplus K_i) \oplus K_i = m_i$.

Захищеність такої системи залежить в цілому від особливостей побудови псевдовипадкового генератора ключа.

3. Опис хаотичних динамічних систем

Генератор ключа в алгоритмі шифрування будується за допомогою динамічних систем: динамічної системи Лоренца та одномірного логістичного відображення, що описуються рівняннями (1) та (2) відповідно.

Система Лоренца, траєкторія стану якої приведена на рис. 2 є найбільш відомим прикладом динамічної системи з трьох диференційних рівнянь (1) [4 – 8]:

$$\begin{aligned} \dot{x} &= -a(x-y) \\ \dot{y} &= cx - y - xz, \\ \dot{z} &= bz + xy \end{aligned} \qquad (1)$$

де x, y та z - динамічні змінні, a, b, c - параметри системи Лоренца, що зазвичай приймають значення $a=10$, $b=8/3$ та $c=28$.

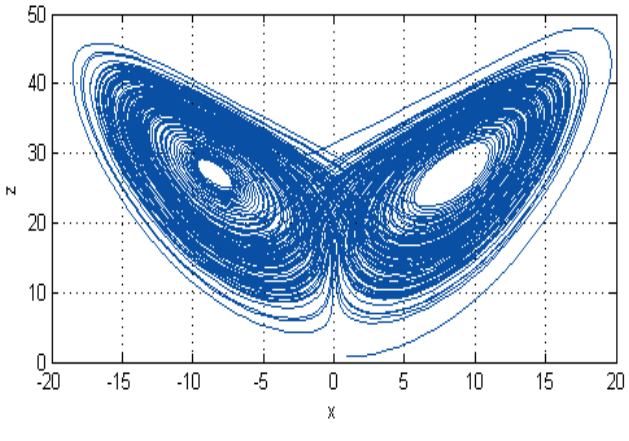

Рис. 2. Траєкторія стану системи Лоренца в фазовому просторі

Другою динамічною системою є одномірне логістичне відображення (2), (одна із найпростіших дискретних хаотичних систем [7, 9]) наступного вигляду:

$$v_{n+1} = r v_n (1 - v_n), \qquad (2)$$

де v_n та r - змінна системи та параметр системи відповідно, n - номер ітерацій. Параметр системи r є значущим елементом рівняння і при значеннях $3.57 < r < 4$ системі притаманна хаотична поведінка. При інших значеннях r хаотична поведінка системи не спостерігається.

Діаграма біфуркацій логістичного відображення приведена на рис. 3.

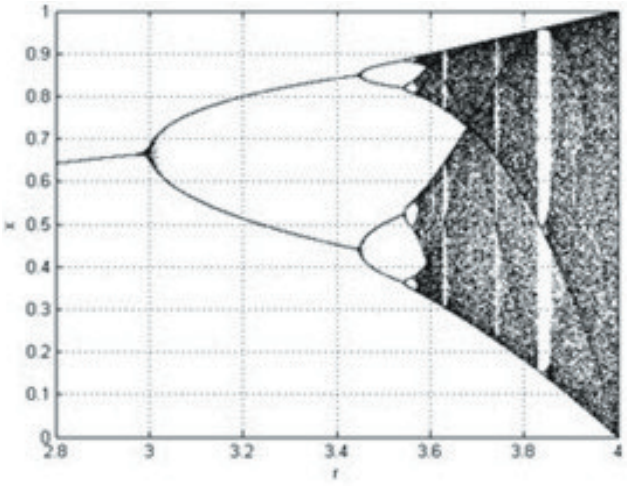

Рис. 3. Діаграма біфуркацій логістичного відображення

4. Опис алгоритму шифрування

Алгоритм шифрування бінарної інформаційної послідовності призначений для шифрування цифрових інформаційних повідомлень будь-якого формату і складається з наступних кроків:

1. На вхід системи шифрування подається цифрове інформаційне повідомлення.

2. Генератором ключа здійснюється генерування ключової послідовності.

3. За допомогою операції XOR, що виконується над відповідними членами інформаційної та ключової послідовності, здійснюється шифрування інформаційного повідомлення.

Особливістю даного алгоритму є спосіб генерації ключової послідовності. Функціональна схема алгоритму шифрування приведена на рис. 4.

Псевдовипадковий генератор бітів (генератор ключової послідовності) побудований з використанням динамічної системи Лоренца (1) та одномірного логістичного відображення (2).

Динамічна система Лоренца описується трьома диференційними рівняннями, що описують її поведінку, що залежить від початкових умов та значень параметрів системи.

Часова діаграма кожної змінної при значеннях параметрів $a=10$, $b=8/3$, $c=28$ та початкових умовах $x=2$, $y=1$ та $z=4$ приведена на рис. 5 а, б, в відповідно.

Система Лоренца неперервно генерує значення змінних, в результаті чого матимемо криву варіації змінних системи протягом часу (рис. 5).

З метою уникнення впливу перехідних процесів у системі відкидаємо перших 1000 згенерованих значень, забезпечуючи тим самим використання тієї частини траєкторії, що відповідає хаотичним процесам в системі.

Кожна генерована точка траєкторії має своє числове значення, що використовується при формуванні ключа шифрування.

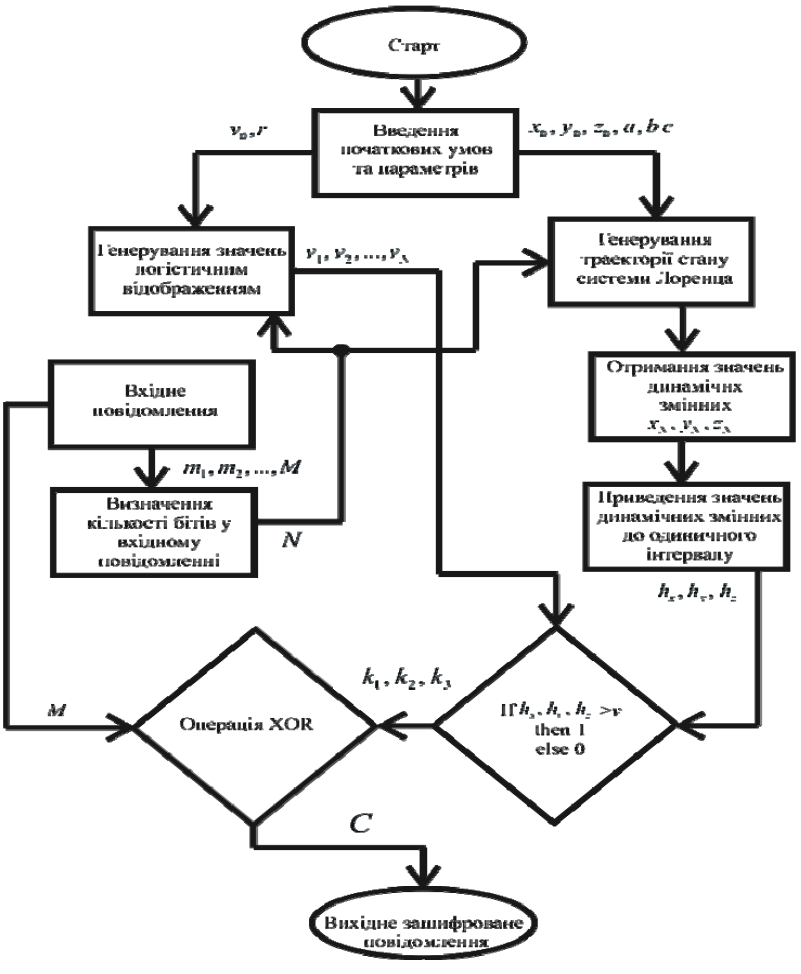

Рис. 4. Функціональна схема алгоритму шифрування інформаційної послідовності

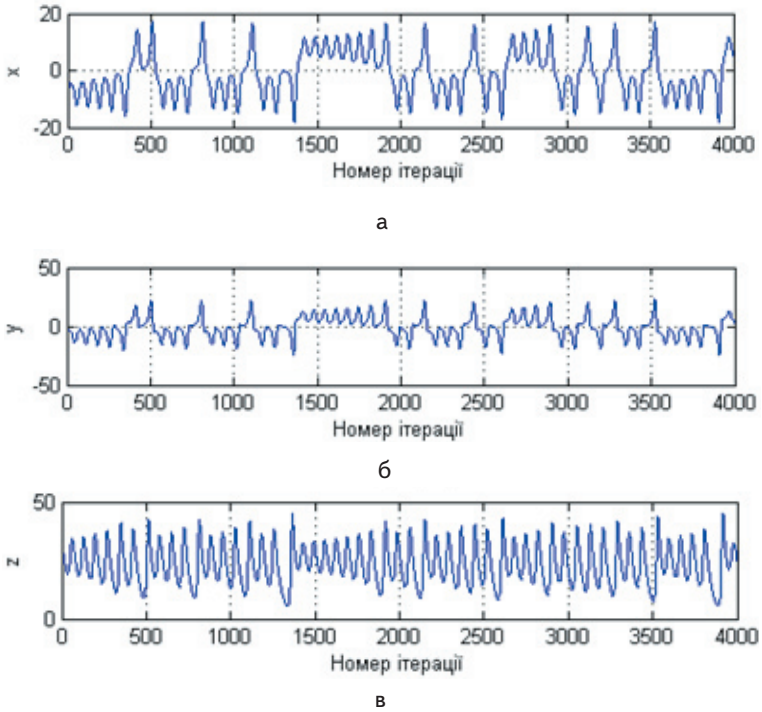

Рис. 5. Варіації змінних системи Лоренца: а - залежність значення змінної x від кількості ітерацій, б - залежність значення змінної y від кількості ітерацій, в - залежність значення змінної z від кількості ітерацій

З метою порівняння розв'язків логістичного відображення зі значеннями змінних системи Лоренца приводимо їх до одиничного інтервалу, в результаті чого значення трьох змінних знаходяться в інтервалі (0; 1]. В результаті порівняння значень системи Лоренца та логістичного відображення при умові $h_x, h_y, h_z \geq \nu$ генерується логічна 1, в іншому випадку – логічний 0, де h_x, h_y, h_z - приведені до одиничного інтервалу значення змінних системи Лоренца та ν - значення, генеровані логістичним відображенням.

Проводячи таку операцію для всіх трьох змінних системи Лоренца, отримаємо три різні бінарні послідовності k_1, k_2, k_3 (рис. 4), що за допомогою операції XOR перемішуються між собою, в результаті чого утворюється загальний ключ шифрування:

$$k_1 \oplus k_2 \oplus k_3 = K.$$

Отриманий загальний ключ шифрування за допомогою операції XOR додається до інформаційної послідовності, в результаті чого утворюється зашифрована інформаційна послідовність.

$$K \oplus M = C.$$

Процес дешифрування є аналогічним до процесу шифрування з використанням тих самих початкових умов та параметрів, що й при шифруванні.

Генерація ключа дешифрування здійснюється так само, як і при шифруванні. В загальному процес дешифрування виглядатиме наступним чином:

$$M = C \oplus K.$$

Робота алгоритму генерування ключа шифрування інформації була модельована в середовищі LabView. Блок-діаграма алгоритму генерації приведена на рис. 6.

На рис. 7 приведено вікно користувача з прикладом роботи даного алгоритму.

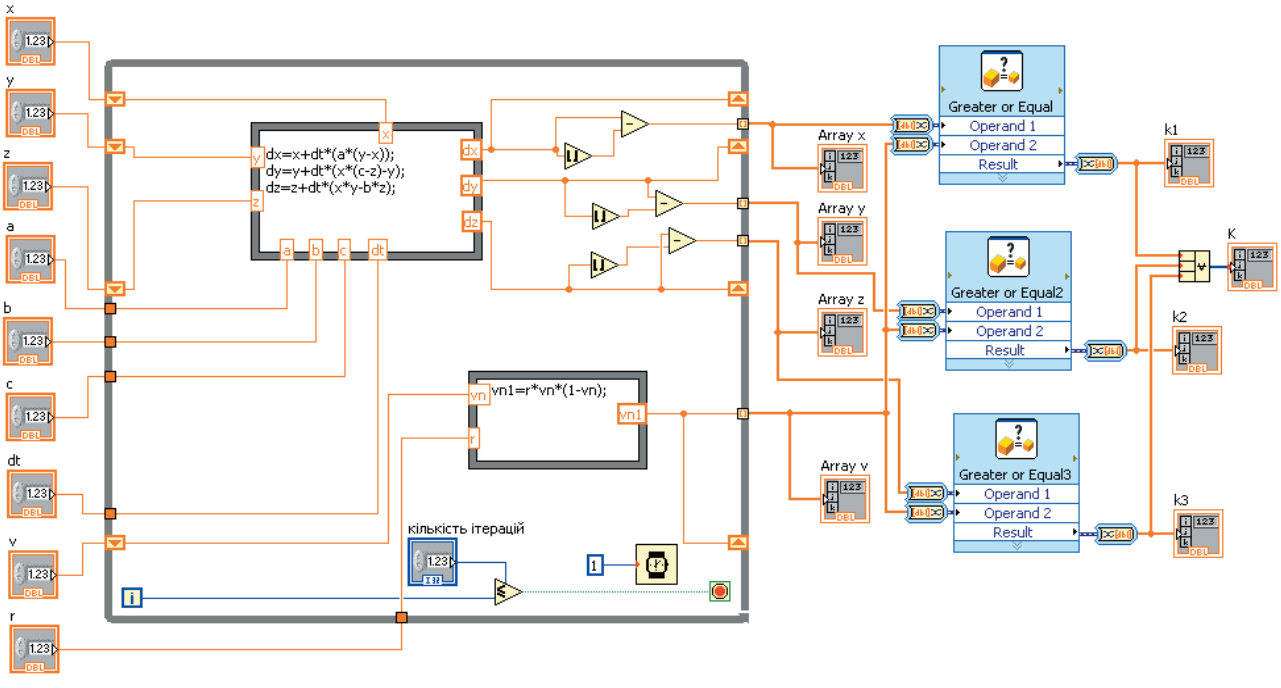

Рис. 6. Блок діаграма генератора ключа шифрування інформації

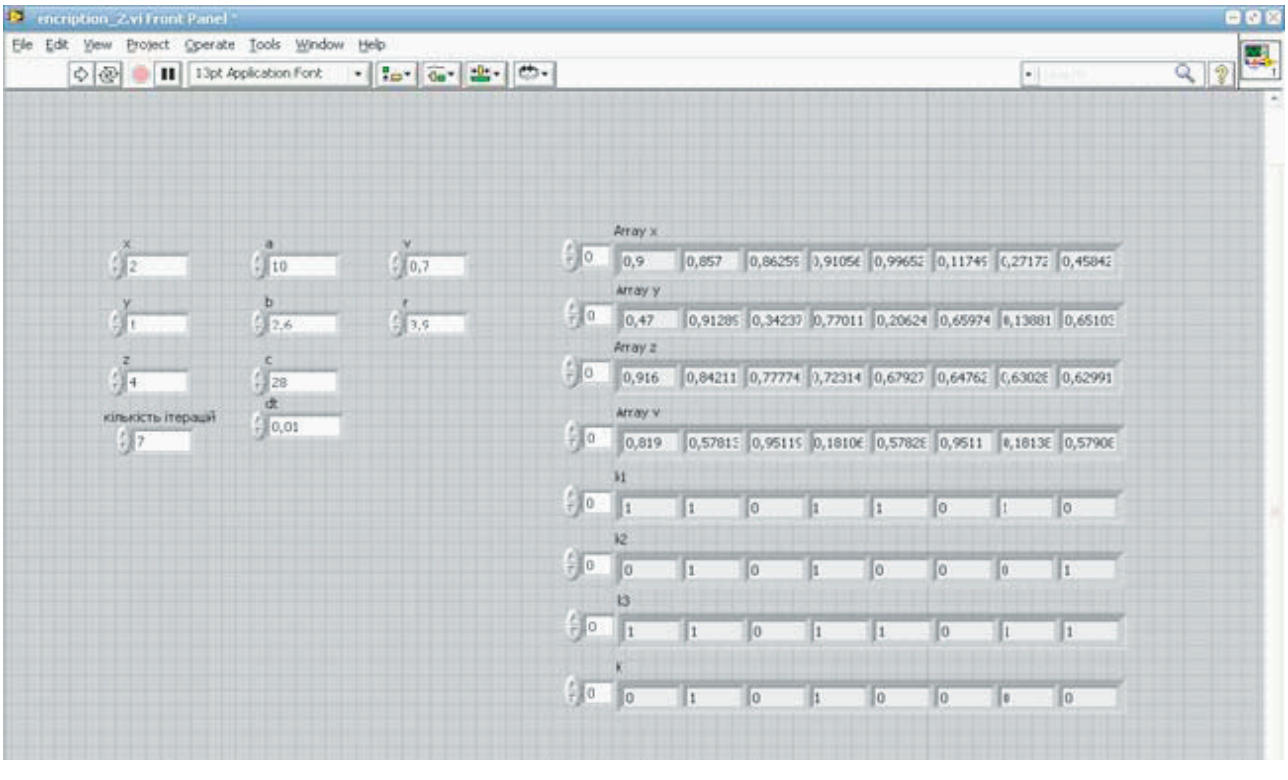

Рис. 7. Вікно користувача змодельованого алгоритму генерації ключа шифрування інформації

5. Аналіз захищеності алгоритму шифрування

Надійна криптосистема повинна володіти наступними властивостями: чутливістю до вхідного повідомлення (зміна вхідного повідомленні утворює інший шифр навіть при одному і тому самому згенерованому ключі), чутливістю до початкових умов та параметрів при генерації ключової послідовності, що використовується для шифрування (зміна хоча б одного з параметрів динамічної системи чи початкової умови приводить до генерації іншої ключової послідовності та утворює цілком інший шифр) [10, 11].

Оскільки криптосистема має справу з бінарними послідовностями (вхідна інформація та ключова послідовність є наборами логічних 0 та 1), генератор ключа неперервно генерує логічні 0 та 1 і формат вихідного зашифрованого повідомлення буде залежати тільки від формату інформації, що підлягає шифруванню.

Алгоритм шифрування поєднує в собі використання двох динамічних систем, одна з яких (система Лоренца) генерує значення динамічних змінних, а інша (логістичне відображення) генерує значення, що використовуються як граничні для визначення згенерований логічний 0 чи 1. Даний елемент алгоритму є оригінальним, оскільки рівень визначення появи логічного 0 чи 1 постійно змінний. Саме зміна рівня ускладнює задачу зламу шифру для криптоаналітика. Поєднання двох динамічних систем обумовлює створення додаткових ключів шифрування.

Запропонована криптосистема має вісім секретних ключів, що є параметрами систем та початковими умовами (σ, b, R, x_0, y_0, z_0, ν_0 та r). В результаті чого значно зросте час підбору ключів для криптоаналітика.

Загальна кількість можливих варіантів комбінацій ключів при точності в 10 знаків після коми може сягнути близько 10^{50}.

Використання двох динамічних систем, що формують досить велику кількість ключів та екстремальна чутливість до початкових умов та параметрів забезпечує високу стійкість алгоритму як до статистичних атак, так і грубих атак.

6. Висновки

1. Запропонований генератор ключа побудований на основі двох динамічних хаотичних систем (система Лоренца та логістичне відображення), властивості яких дозволяють генерувати велику кількість ключів шифрування, забезпечуючи високу захищеність хаотичної криптосистеми від статистичних атак та атак грубої сили. При проведенні атаки грубої сили для запропонованої точності в 10 знаків після коми, буде приблизно 10^{50} варіантів ключів і на момент розкриття інформації вона вже може втратити свою актуальність.

2. Особливістю розробленого генератора є те, що логістичне відображення використовується в якості динамічного параметру, за яким отриманий на виході генератора логічна одиниця чи логічний нуль.

3. Моделювання роботи генератора ключа в середовищі LabView підтверджує можливість реалізації запропонованого алгоритму як програмним так і апаратним засобами.

Література

1. Pecora, L. M. Synchronization in chaotic systems [Текст] / L.M. Pecora, T.L. Carroll // Phys. Rev. Lett. - 1990. - Vol. 64. - № 8. - P. 821-824.
2. Птицын, Н.В. Приложение теории детерминированного хаоса в криптографии [Текст] / Птицын Н.В. – М.: Изд. МГТУ им Н.Э Баумана, 2002. – 80 с.
3. Strogatz, S. H. Nonlinear systems and chaos. Perseus Publishing [Текст] / Strogatz Steven H. – 1994.
4. Ali-Pacha, A. Chaotic behaviour for the secrete key of cryptographic system [Текст] / Ali-Pacha A, N. Hadj-Said, B. Belmekki, Belgoraf A. // Chaos, Solitons & Fractals 2005;23:1549–52.
5. Schneier, B. Applied cryptography – protocols, algorithms and source code in C [Текст] / Bruce Schneier // second ed. New York: John Wiley & Sons, Inc.; 1996.
6. González, O. A. Cryptosystem Using a Lorenz Chaotic Oscillator [Текст] / O.A. González, G. Han, J.P. de Gyvez, and Edgar CMOS // Proceedings of the IEEE International Symposium on Circuits and Systems. ISCAS '99. Vol. 5. - PP 442-445.
7. Шахтарин, Б.И. Генераторы хаотических колебаний [Текст] / Б.И. Шахтарин, П.И. Кобылкина, Ю.А. Сидоркина, А.В. Кондратьэв, С.В. Митин – Галилеос АРВ. – Москва. - 2007 – 247 с.
8. Ali-Pacha, A. Lorenz's attractor applied to the stream cipher (Ali-Pacha generator) [Текст] / Adda Ali-Pacha, Naima Hadj-Said, A. M'Hamed, A. Belgoraf // Chaos Solitons and Fractals 33 (2007) 1762–1766.
9. Kocarev, L. Logistic map as a block encryption algorithm [Текст] / L. Kocarev, G. Jakimoski // Physics Letters A, 289 (4-5) 2001 – PP 199–206.
10. Vaidya, P. G. and Angadi, S. Decoding chaotic cryptography without access to the superkey [Текст] / P.G. Vaidya and S. Angadi // Chaos, Solitons and Fractals, 17:379-386, 2003.
11. Solak, E. Cryptanalysis of observer based discrete-time chaotic encryption schemes [Текст] / E. Solak // International Journal of Bifurcation and Chaos, 15(2):653-658, 2005.