

УДК 621.391

О. В. ГРЕСЬ,

Чернівецький національний університет імені Юрія Федьковича;

Г. М. РОЗОРІНОВ, доктор техн. наук, професор,

Державний університет телекомунікацій, Київ;

М. М. ІВАНЧУК, канд. техн. наук, інженер-конструктор,

ПП «АРТОН», Чернівці;

Р. Л. ПОЛІТАНСЬКИЙ, канд. фіз.-мат. наук, доцент;

А. Д. ВЕРИГА, канд. техн. наук,

Чернівецький національний університет імені Юрія Федьковича

АПАРАТНА РЕАЛІЗАЦІЯ ГЕНЕРАТОРА ХАОТИЧНИХ СИГНАЛІВ НА ОСНОВІ ДИСКРЕТНИХ ВІДОБРАЖЕНЬ

Запропоновано модель і апаратну реалізацію генератора хаотичних сигналів на основі дискретних відображень. Роботу відповідного пристрою досліджено в режимі генерування хаотичних сигналів при різних значеннях параметра керування. Результати, здобуті при моделюванні та експериментальних дослідженнях, засвідчують можливість використання мікроконтролерів для реалізації генераторів хаотичних коливань.

Ключові слова: хаотична послідовність; логістичне відображення; мікроконтролер; генератор.

Вступ

Сучасні телекомунікаційні системи вимагають забезпечення високої прихованості та конфіденційності зв'язку. Для захисту інформації в таких системах використовують її шифрування за допомогою псевдовипадкових послідовностей. У спеціальних джерелах описано багато методів генерування двійкових псевдовипадкових послідовностей. Один із найпоширеніших методів полягає в генеруванні зазначеної послідовності на основі певного рекурентного співвідношення, що пов'язує між собою деякі цілі або дійсні числа. Тоді черговий біт двійкової послідовності отримують, визначаючи, чи належить відповідний її член одній із двох підмножин усіх можливих значень [1–4].

Основна частина

1. Моделювання генератора хаотичних сигналів

Як одну з найпростіших систем, що уможливають генерування хаотичних сигналів (коливань), слід розглядати логістичне відображення [5; 6]. Моделювання логістичного відображення було здійснено в середовищі LabView 2010. Блок-схему генератора хаотичних коливань на основі логістичного рівняння зображено на рис. 1.

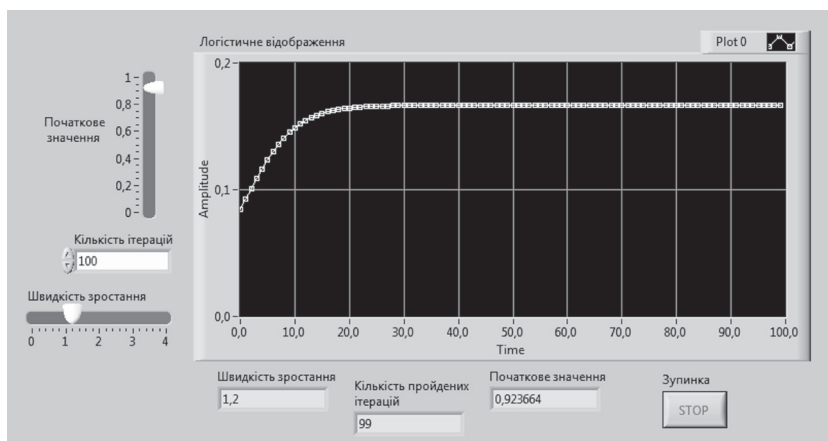


Рис. 1. Блок-схема генератора хаотичних коливань

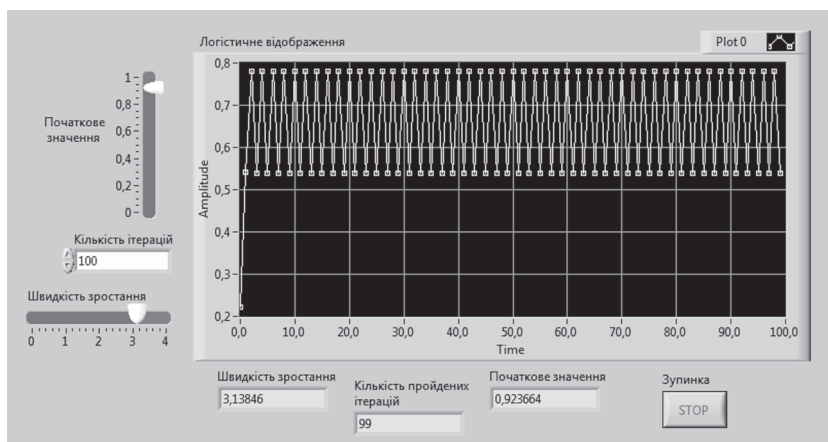
Моделювання роботи генератора було виконано при різних значеннях параметра керування (далі — параметр λ). Результати моделювання наведено на рис. 2.

Як впливає з рис. 2, при значеннях параметра λ , змінюваних від нуля до одиниці, коливань у системі немає. При $1 < \lambda < 2$ спостерігається вихід на стаціонарні значення (рис. 2, а), а з поступовим збільшенням параметра λ період коливань зростає (рис. 2, б). Зокрема, якщо λ міститься між 3,45 і 3,54, то виникають коливання між чотирма числовими значеннями. Коли $\lambda \geq 3,54$, коливання відбуваються послідовно вісьмома, шістнадцятьма, тридцятьма двома, ..., тобто щоразу подвоєною кількістю числових значень. При $\lambda \geq 3,57$ (рис. 2, в, г) каскад подвоєнь закінчується і процес набуває хаотичності: невеликі зміни в початкових умовах призводять надалі до невідповідного поведінки системи [6].

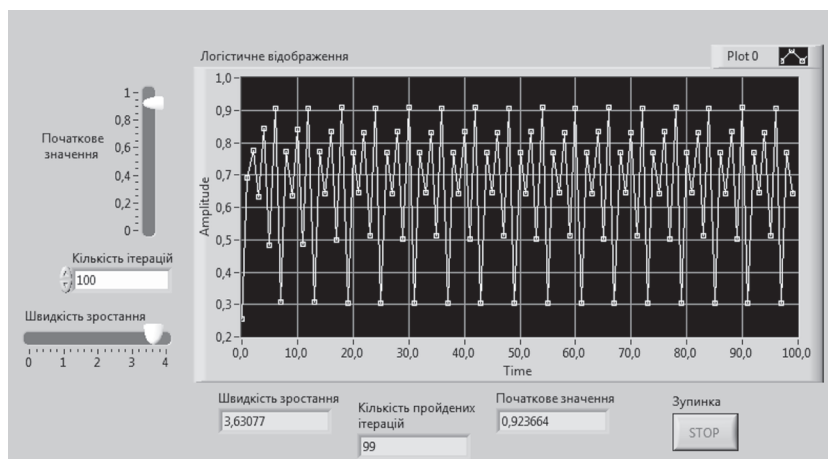
а



б



в



г

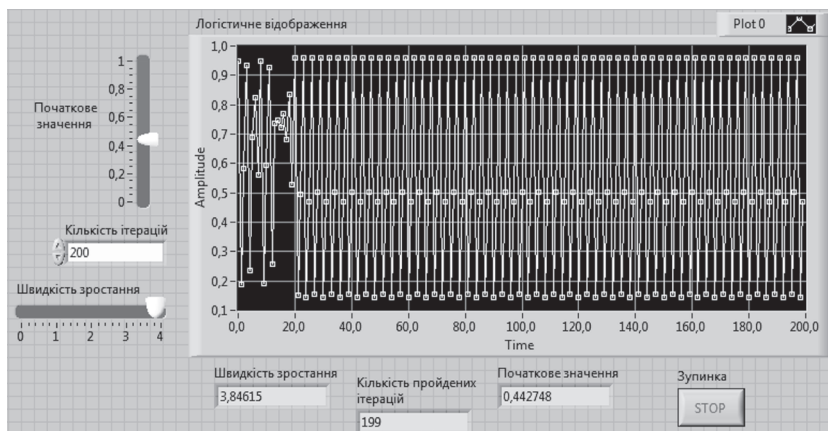


Рис. 2. Моделювання системи при різних значеннях параметра λ : а — $\lambda = 1,2$; б — $\lambda = 3,13$; в — $\lambda = 3,63$; г — $\lambda = 3,84$

2. Практична реалізація генератора хаотичних коливань

Апаратну реалізацію генератора хаотичних коливань було виконано за допомогою дискретних хаотичних відображень із використанням сучасної елементної бази (мікроконтролерів, програмованих логічних інтегральних схем тощо), завдяки якій вдалося забезпечити поліпшення масогабаритних показників генератора, розширення його функціональних можливостей, а також підвищення швидкості обробки даних [4; 7; 8].

Структурну схему розробленого генератора наведено на рис. 3.



Рис. 3. Структурна схема генератора хаотичних коливань

Основу цього пристрою становить мікроконтролер DD1 (PIC18F2550), який виконує функції апаратного програмованого ядра для генерування послідовностей за певним алгоритмом.

Принципову схему генератора подано на рис. 4.

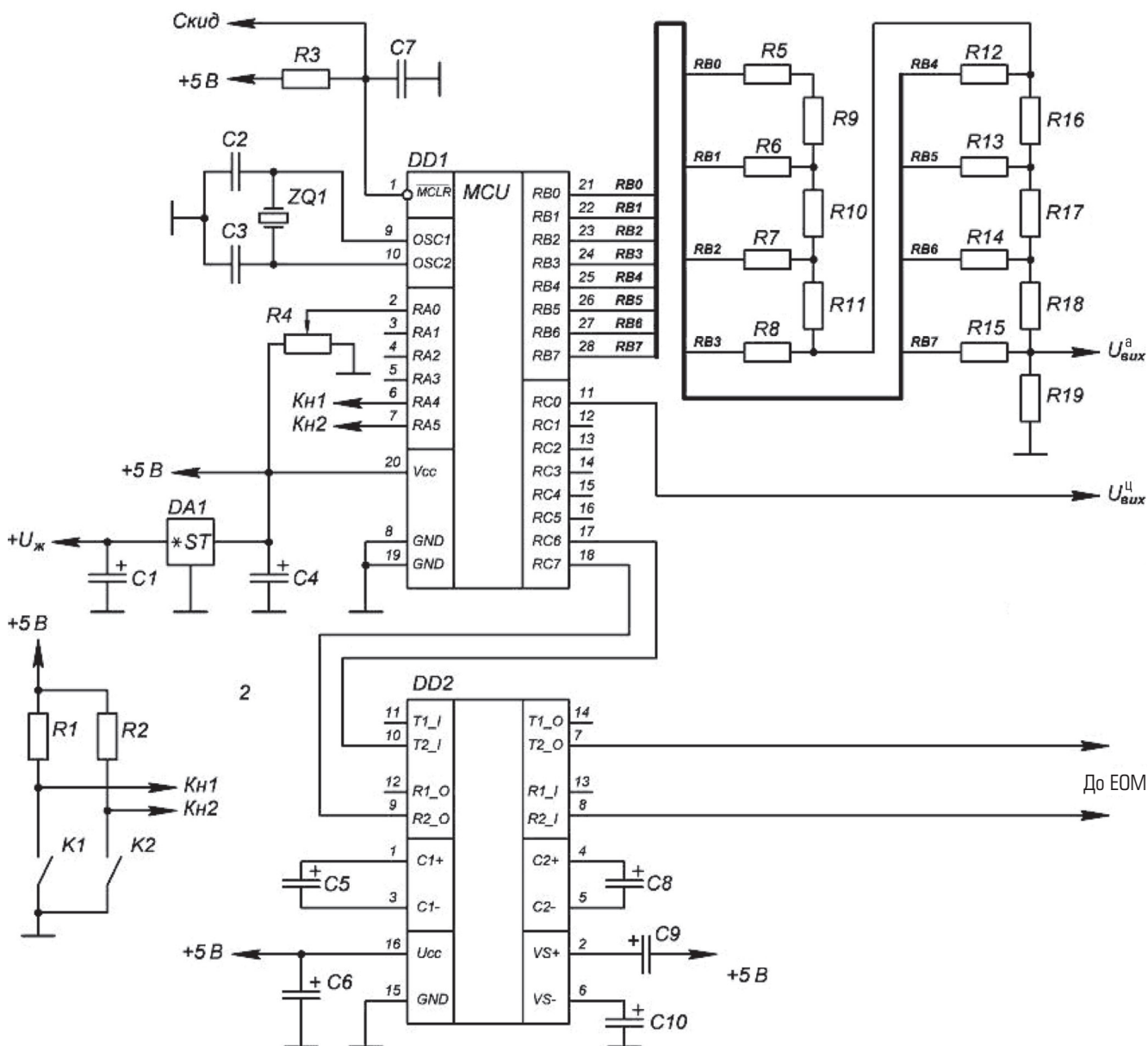


Рис. 4. Принципова електрична схема генератора хаотичних коливань

Для генерування цифрових хаотичних коливань (послідовностей) використовується дискретне відображення, відоме як *логістичне відображення (рівняння)* [1–6]:

$$x_{n+1} = \lambda x_n (1 - x_n), n = 0, 1, 2, \dots, \quad (1)$$

де λ — параметр керування, x_0 — початкова умова для генерування послідовностей.

Залежно від значення параметра λ генеровані коливання можуть бути періодичні, квазіперіодичні чи хаотичні. Генерування хаотичної послідовності згідно з логістичним рівнянням (1) відбувається, коли значення параметра $\lambda \in [3,56; 4]$ [1–6].

Значення початкової умови x_0 і параметра λ задаються при програмуванні мікроконтролера. Генерування послідовностей здійснюється на програмному рівні. Програму для мікроконтролера написано мовою програмування C. Алгоритм роботи програми подано на рис. 5.

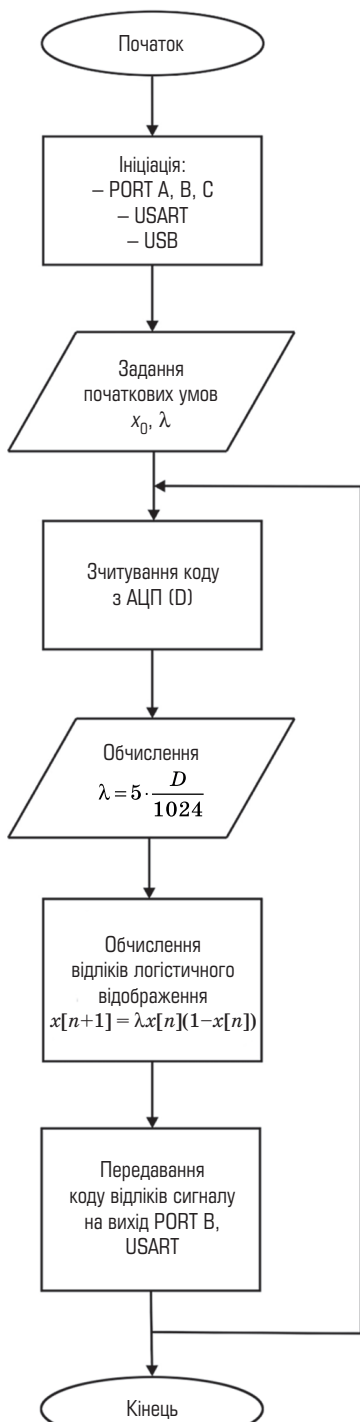


Рис. 5. Алгоритм роботи програми

Пристрій узгодження інтерфейсу RS-232, виконаний на мікросхемі DD2 (MAX232), призначено для зв'язку генератора з ЕОМ, що має здійснювати керування (із можливістю завантаження керуючої програми мікроконтролера за допомогою завантажувача «bootloader»).

Для живлення схеми використано інтегральний стабілізатор DA1 (LM7805), оскільки всі використані в приладі мікросхеми та дискретні

компоненти живляться однополярною напругою +5 В. Режим роботи пристрою можна вибрати за допомогою пари перемикачів К1, К2. Пристрій може працювати в одному з трьох режимів:

- 1) генерування аналогового хаотичного сигналу ($U_{\text{вих}}^a$);
- 2) формування цифрового послідовного коду ($U_{\text{вих}}^n$);
- 3) робота з ЕОМ, із можливістю передавання коду через інтерфейс RS-232.

Необхідне значення параметра λ встановлюється змінним резистором R4.

Моделювання роботи генератора було здійснено в програмному середовищі Proteus 7.2. Результати моделювання роботи генератора при $\lambda = 3,94$ наведено на рис. 6.

Певне уявлення про зовнішній вигляд макета розробленого генератора можна скласти згідно з рис. 7.

Вихідні сигнали генератора, що досліджувались у режимі генерування аналогового хаотичного коливання на виході ЦАП (R-2R матриці) за допомогою цифрового осцилографа Tektronix TDS1012 при різних значеннях параметра керування λ , наведено в таблиці.

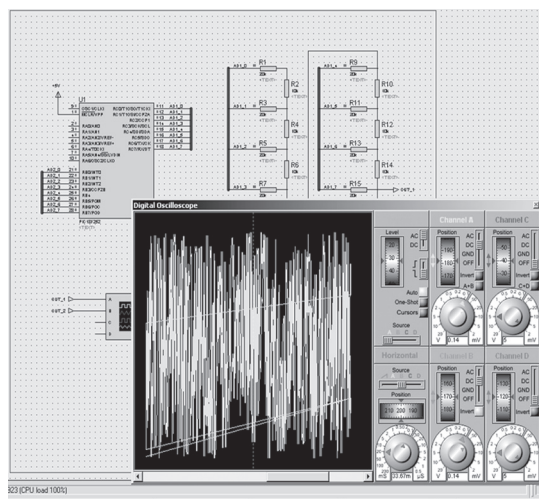


Рис. 6. Вікно моделювання пристрою в середовищі Proteus 7.2

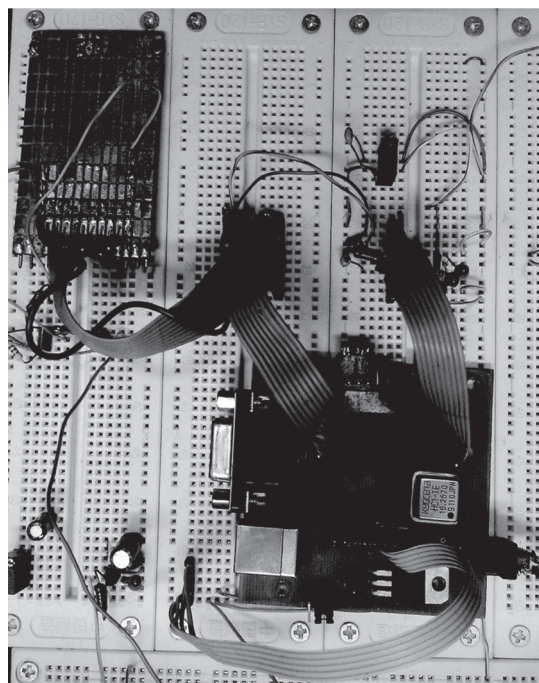
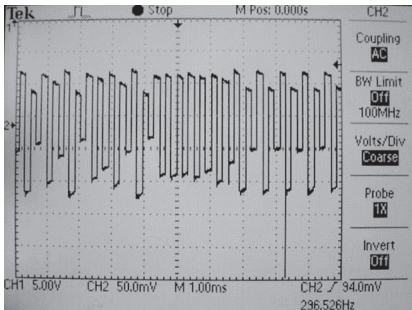
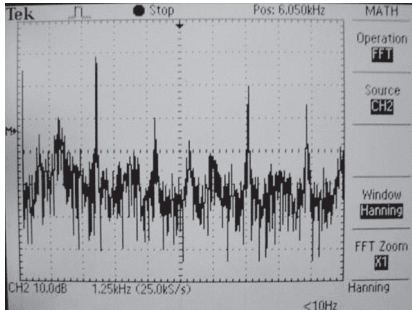
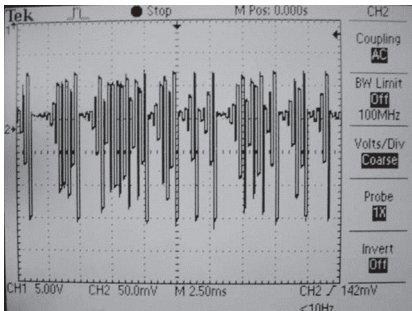
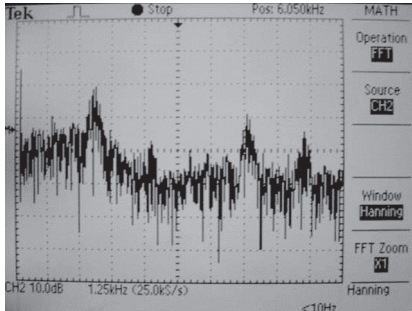
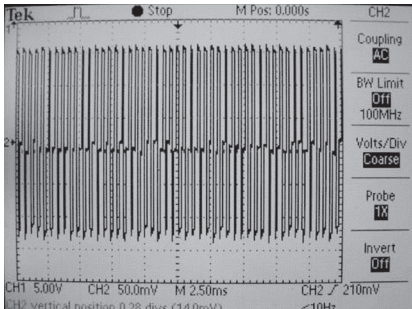
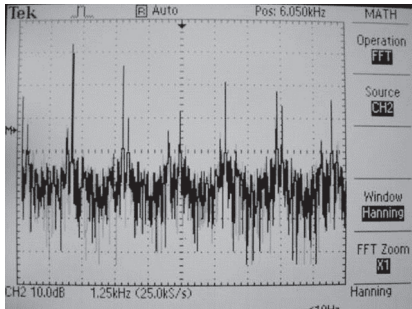
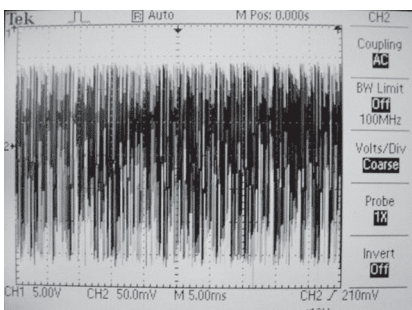
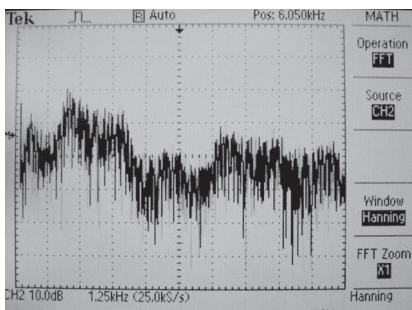
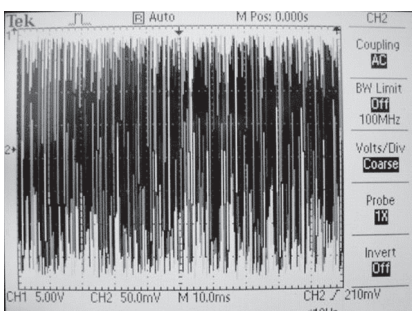
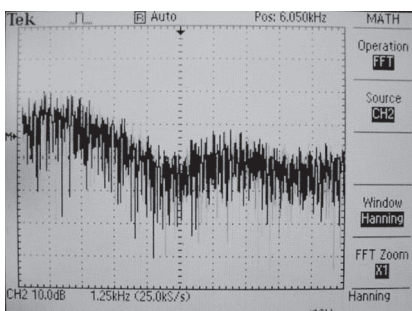


Рис. 7. Зовнішній вигляд макета генератора

Вихідні сигнали генератора при різних значеннях параметра керування

Значення параметра керування	Вигляд генерованого сигналу	Спектральне подання генерованого сигналу
$\lambda = 3,54$		
$\lambda = 3,63$		
$\lambda = 3,79$		
$\lambda = 3,82$		
$\lambda = 3,94$		

Як показують отримані осцилограми й спектрограми, наведені в таблиці, результати моделювання роботи генератора набули експериментального підтвердження.

Висновки

Запропоновано модель і апаратну реалізацію генератора хаотичних сигналів (коливань) на основі дискретних одновимірних відображень. Роботу пристрою досліджено в режимі генерування хаотичних сигналів при різних значеннях параметра керування. Здобуті результати моделювання та експериментальних досліджень показують, що мікроконтролери цілком придатні для реалізації генераторів хаотичних коливань на основі дискретних відображень. Описаний пристрій можна використовувати для побудови систем передавання інформації, що забезпечують високу прихованість і конфіденційність зв'язку.

Література

1. Kocarev, L. Pseudorandom bits generated by chaotic maps / L. Kocarev, G. Jakimoski // *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions.*— 2003.— № 50(1).— P. 123–126.
2. Стасєв, Ю. В. Інформаційні системи на основі динамічного хаосу / Ю. В. Стасєв, К. С. Васюта, С. В. Женжера // *Системи озброєння і військова техніка.*— 2009.— № 1(17).— С. 134–138.
3. Савельєв, С. В. Счетное множество бинарных последовательностей для широкополосных систем связи на основе системы с динамическим хаосом / III Всерос. конф. «Радиолокация и радиосвязь», 26–29 окт. 2009 г.— С. 488–493.
4. Пристрій генерування хаотичних сигналів на основі дискретних одновимірних відображень / [О. В. Гресь, Р. Л. Політанський, А. Д. Верига, М. М. Іванчук] // *Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки: матеріали IV Міжнар. наук.-практ. конф., 23–25 жовт 2014 р.: тези доп.*— Чернівці, 2014.— С. 83–84.
5. Pareek, N. K. Cryptography using multiple one-dimensional chaotic maps / N. K. Pareek, Vinod Patidar, K. K. Sud // *Commun. Nonlinear Sci. Numer. Simul.*— 2005.— № 10(7).— P. 715–723.
6. Логистическое отображение [Электронный ресурс].— Режим доступа: https://ru.wikipedia.org/wiki/Логистическое_отображение
7. Mao, Y. A Chip Performing Chaotic Stream Encryption / Y. Mao, W. Liu, Z. a. o. // *Studies in Computational Intelligence (SCI).*— 2007.— № 42.— P. 307–332.
8. Апаратна реалізація пристрою шифрування мовної інформації / О. В. Гресь, А. Д. Верига, Р. Л. Політанський, О. В. Дробик // *Сучасний захист інформації.*— 2014.— № 3.— С. 71–77.

А. В. Гресь, Г. Н. Розоринов, М. М. Іванчук, Р. Л. Політанський, А. Д. Верига

АППАРАТНАЯ РЕАЛИЗАЦИЯ ГЕНЕРАТОРА ХАОТИЧЕСКИХ СИГНАЛОВ НА ОСНОВЕ ДИСКРЕТНЫХ ОТОБРАЖЕНИЙ

Предложены модель и аппаратная реализация генератора хаотичных сигналов на основе дискретных отображений. Работа соответствующего устройства исследована в режиме генерации хаотичных сигналов при различных значениях управляющего параметра. Результаты, полученные при моделировании и экспериментальных исследованиях, указывают на возможность использования микроконтроллеров для реализации генераторов хаотических колебаний.

Ключевые слова: хаотичная последовательность; логистическое отображение; микроконтроллер; генератор.

O. V. Hres, G. M. Rozorynov, M. M. Ivanchuk, R. L. Politsansky, A. D. Veriga

HARDWARE IMPLEMENTATION CHAOTIC SIGNAL GENERATOR BASED ON DISCRETE MAPPINGS

In this paper proposed the model of the generator, and the hardware implementation of chaotic signals based on discrete maps. Operation of the device investigated in the mode of generating chaotic signals for different values of the control parameter. The obtained results indicate the possibility of using a microcontroller to implementation generators of chaotic oscillations.

Keywords: chaotic sequence; logistic map; microcontroller; generator.