***Гресь Олександр Володимирович**, кандидат технічних наук,*
асистент кафедри радіотехніки та інформаційної безпеки,
Чернівецький національний університет
імені Юрія Федьковича, м. Чернівці
ORCID: 0000-0002-8465-193X

***Косован Василь Михайлович**, кандидат фізико-математичних наук,*
викладач інформатики, Чернівецький ліцей № 1, м. Чернівці

ПРОГРАМНІ ЗАСОБИ ДЛЯ ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ДИСКРЕТНОГО ВІДОБРАЖЕННЯ

Інтернет-адреса публікації на сайті:
http://www.konferenciaonline.org.ua/ua/article/id-1243/

На сьогоднішній день актуальною задачею є забезпечення захисту інформації в системах обміну інформацією, для вирішення якої застосовують різні методи. Одним із методів забезпечення захисту інформації є її криптографічний захист з використанням генераторів псевдовипадкових послідовностей.

На даний час відомі багато алгоритмів генерування криптостійких псевдовипадкових послідовностей (ПВП), зокрема: на основі еліптичних кривих, клітинних автоматів, теорії детермінованого хаосу [1-3]. Основною особливістю генераторів ПВП, які реалізовані на основі дискретних відображень, є висока чутливість до зміни початкових умов [1-3].

В даній роботі проведемо дослідження криптостійкості та чутливості одного із найпоширеніших генераторів ПВП, а саме генератора на основі логістичного відображення [3].

Логістичне відображення описується формулою:

$$x_{n+1} = \lambda \cdot x_n (1 - x_n) \qquad (1)$$

де: λ – параметр керування, x_0 – початкова умова для генерування послідовностей. Значення параметру керування для генерування хаотичних послідовностей знаходиться в межах $\lambda \in [3, 56 - 4]$.

Для реалізації генератора псевдовипадкових послідовностей на основі дискретних відображень (логістичного, кубічного та інших) було розроблене програмне забезпечення, інтерфейс якого приведений на рисунку 1.

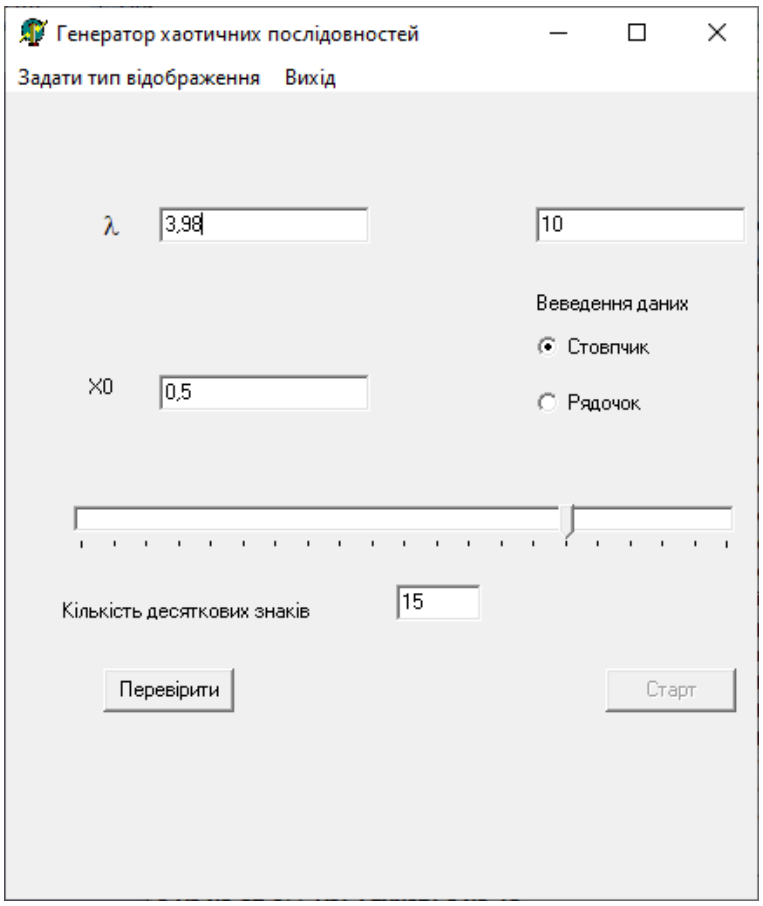

Рис. 1. Інтерфейс програми для генерування псевдовипадкових послідовностей на основі дискретних відображень

Результати досліджень статистичних характеристик генератора на основі логістичного відображення з використанням пакету тестів NIST STS 2.1.2 показали, що послідовності генеровані на основі логістичного відображення мають задовільні статистичні характеристики в діапазоні значень параметру керування $\lambda \in [3{,}8 - 4]$ (масив для дослідження становив 10^9 бітів).

Ще одною ключовою особливістю даного генератора, яка забезпечує великий масив генерованих вихідних послідовностей, а відповідно, і стійкість генератора, є висока чутливість до зміни початкових параметрів. Проведемо дослідження логістичного відображення на чутливість до зміни початкових умов та параметру керування λ. Для дослідження чутливості генератора на основі логістичного відображення було розроблене програмне забезпечення, інтерфейс якого представлений на рисунку 2.

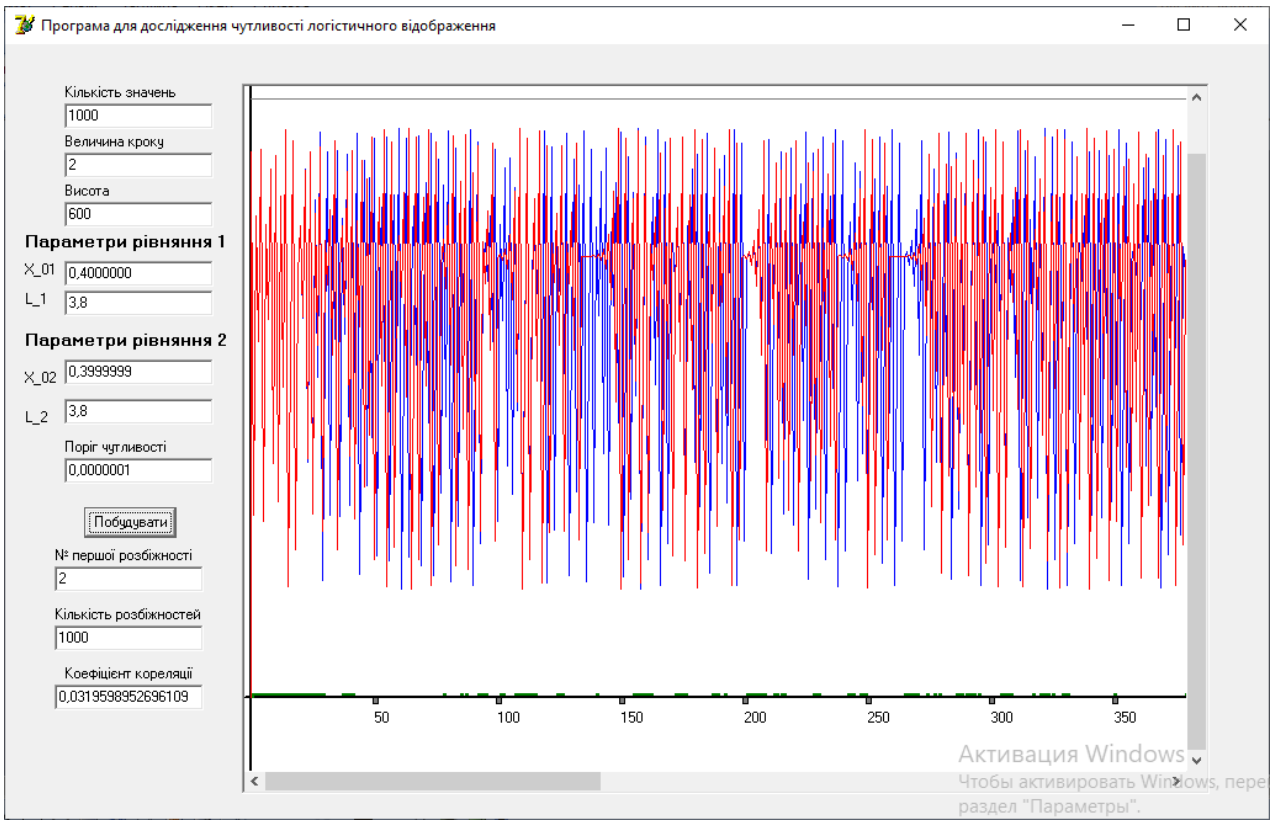

Рис. 2. Інтерфейс програми для дослідження чутливості логістичного відображення

Для дослідження було обрано 1000 значень генерованих послідовностей. Дослідження проводились при невеликій різниці між значеннями параметрів при різних порогах чутливості.

З проведених досліджень встановлено, що розбіжності в генерованих значеннях з'являються вже при зміні параметра керування λ на $1 \cdot 10^{-7}$ при порозі чутливості $1 \cdot 10^{-7}$.

Для більш якісного аналізу також визначимо коефіцієнт кореляції між значеннями функцій. Для розрахунку коефіцієнту кореляції було обрано 1000 значень генерованих послідовностей. Дослідження проводилось при наступних значеннях параметрів: $\lambda_1 = \lambda_2 = 3{,}8$; $x_{01} = 0{,}4$ $x_{02} = 0{,}3999999$ (графік 1) та $\lambda_1 = 3{,}8$; $\lambda_2 = 3{,}7999999$; $x_{01} = x_{02} = 0{,}4$). Залежність коефіцієнта кореляції від кількості значень генерованих послідовностей (для перших 500 генерованих значень) показана на рис. 3.

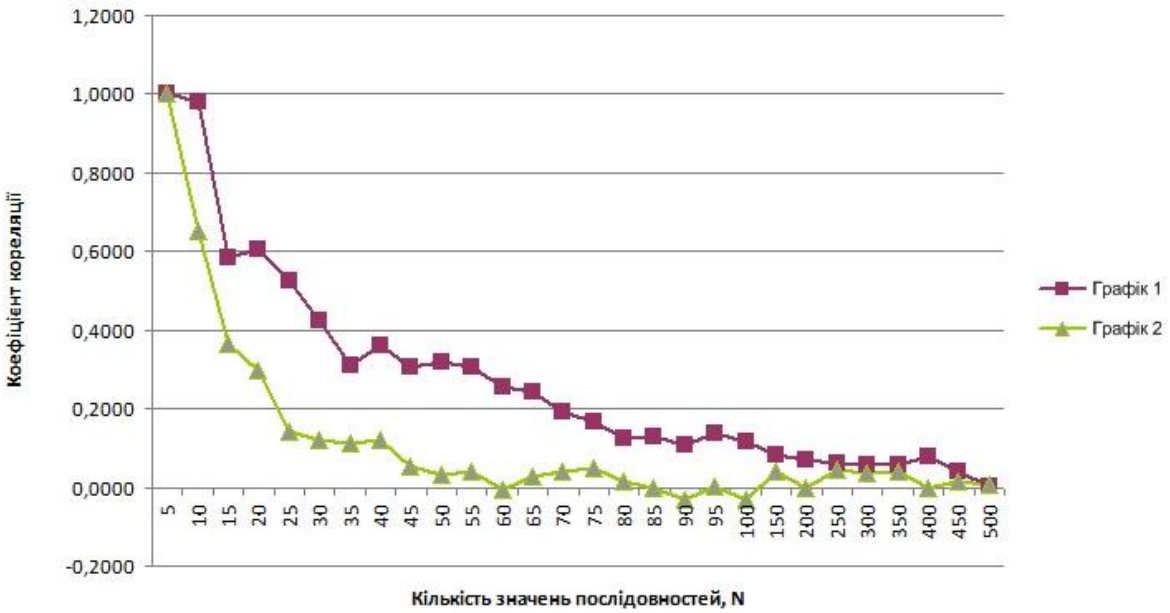

Рис. 3. Графік залежності коефіцієнта кореляції ПВП
від кількості генерованих значень

Отже, з отриманих результатів досліджень можна зробити висновок, що послідовності генеровані на основі логістичного відображення мають задовільні статистичні характеристики в діапазоні значень параметру керування $\lambda \in [3{,}8 - 4]$ та найкращий коефіцієнт кореляції мають генеровані значення послідовностей, починаючи з N-100.

Література:

1. Kocarev L. Pseudorandom bits generated by chaotic maps / Kocarev L., Jakimoski G // Circuits and Systems I: Fundamental Theory and Applications, IEEETransactions – 50(1) – 2003 – Pp. 123-126.

2. Kanso A. Logistic chaotic maps for binary numbers generations. / A. Kanso, N. Smaoui // Chaos, Solitons & Fractals. – 2009 – Vol. 40(5) – pp. 2557-2568.

3. Гресь О. В. Дослідження криптостійкості генераторів бінарних послідовностей на основі дискретних відображень / Гресь О. В., Політанський Р. Л. // Фізико-технологічні проблеми передавання, обробки та зберігання інформації в інфокомунікаційних: Матеріали V Міжнародної науково-практичної конференції, 3-5 листопада 2016р.: тези доп. – Чернівці, 2016. – С. 123.