experiment machine is presented. The description of the evolution of a dynamical system in the form of elastic deformed body from the equilibrium to the attractor describing the new steady state, in which the degradation of the material to fracture occurs, is made.

Key words: composite materials, durability, life cycle, fatigue.

УДК 004.3:621.319.5

Доц. В.І. Отенко, канд. техн. наук.; доц. О.І. Гарасимчук, канд. техн. наук; доц. І.М. Журавель, канд. техн. наук; асист. Ю.М. Костів, канд. техн. наук; студ. А.Ю. Пастух – НУ "Львівська політехніка"

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ СТРУКТУРНИХ ЕЛЕМЕНТІВ ГЕНЕРАТОРА ДЖІФФІ

Представлено результати дослідження генератора Джіффі за різної кількості базових генераторів на основі регістрів зсуву з лінійним зворотним зв'язком і різного степеня їх поліномів, що проведено з використанням статистичних тестів NIST. Важливе значення серед генераторів псевдовипадкових послідовностей займає генератор Джіффі, проте його якісні характеристики є малодослідженими. Отримані результати дають змогу оптимізувати параметри генератора за заданих параметрах вихідної імпульсної послідовності. Наведено принципи оптимізації параметрів структурних елементів генератора Джіффі. Якість такої оптимізації підтверджена пакетом статистичних тестів NIST STS.

Ключові слова: генератор псевдовипадкових чисел, статистичні характеристики, генератор Джіффі.

Постановка проблеми. В умовах стрімкого розвитку інформаційних технологій значно розширюється сфера застосування генераторів випадкових і псевдовипадкових послідовностей (ГПВП). На сьогодні існує чимало різноманітних методів і принципів генерування псевдовипадкових послідовностей, кожен з яких має свої переваги та недоліки [1-5]. Важливе значення серед генераторів псевдовипадкових послідовностей займає генератор Джіффі, проте його якісні характеристики є малодослідженими. Тому виникає задача, що полягає у покращенні характеристик генератора Джіффі з метою отримання на його виході послідовностей, що прямо чи опосередковано можна було б застосовувати у вирішенні задач захисту інформації.

Для того, щоб робити висновок про можливість застосування того чи іншого генератора псевдовипадкової послідовності для вирішення конкретних задач, потрібно виконати оцінювання його якості та надійності. Проведення тестування генераторів, особливо тих, що використовуються в системах захисту інформації (зокрема криптографічних додатках), є актуальною теоретичною та практичною задачею. На сьогодні, для тестування псевдовипадкових послідовностей використовують велику кількість різноманітних графічних та оціночних тестів. Також розроблено кілька програмних продуктів, що містять комплекси тестів для перевірки різних статистичних властивостей псевдовипадкових послідовностей, найвідомішим серед таких продуктів є набір статистичний тестів NIST STS [6, 7].

Мета роботи – використовуючи набір статистичних тестів NIST STS визначити оптимальні параметри структурних елементів генератора Джіффі шляхом зміни принципів побудови його базових генераторів.

Виклад основного матеріалу. Генератор Джіффі забезпечує перемішування двох послідовностей x_1 та x_2 з виходів двох генераторів М-послідовностей, які ще називають генераторами на основі регістрів зсуву з лінійними зворотніми зв'язками (LFSR) шляхом керування послідовністю з виходу LFSR 3. Це перемішування здійснюється згідно з функцією

$$F(x_1, x_2, x_3) = x_1\bar{x}_3 + x_2x_3 = x_3 \oplus x_1x_2 \oplus x_2x_3, \quad (1)$$

яка може бути реалізована за допомогою мультиплексора 2→1 (рис. 1) [1].

Генератори М-послідовностей, що є базовими для генератора Джіффі, можуть реалізовуватися різними способами, згідно з рівнянням

$$Q(t+1) = T^rQ(t), \quad (2)$$

де: $Q(t)$ і $Q(t+1)$– стани регістра генератора в моменти часу t і t+1 відповідно (до і після приходу синхроімпульсу); T – квадратна матриця порядку N, де N – степінь примітивного полінома. Тому прийнято рішення за допомогою статистичних тестів та шляхом зміни степеня r (а отже, зміни структури самого генератора) визначити, як це впливатиме на якість вихідної псевдовипадкової послідовності з генератора Джіффі.

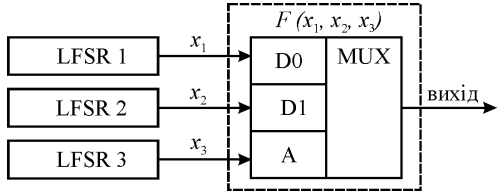


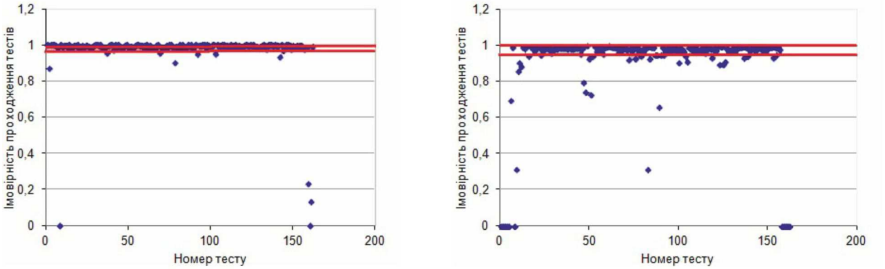
Рис. 1. Генератор Джіффі

Для дослідження якості обирали базові генератори М-послідовностей не тільки з різними степенями твірного поліному, але також змінювали степінь r, до якого підноситься матриця T.

Оцінювання вихідних послідовностей з генератора виконували за допомогою пакету статистичних тестів NIST STS. Результати аналогічних оцінювань генератора Джіффі, на цей час, в літературі відсутні. Для отримання послідовностей з такого генератора розроблено його імітаційні моделі на мові Delphi, що дають змогу одержувати вихідні послідовності залежно від зміни параметрів. Набір тестів NIST STS містить 15 статистичних тестів, розроблених для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що генеруються ГПВП [6].

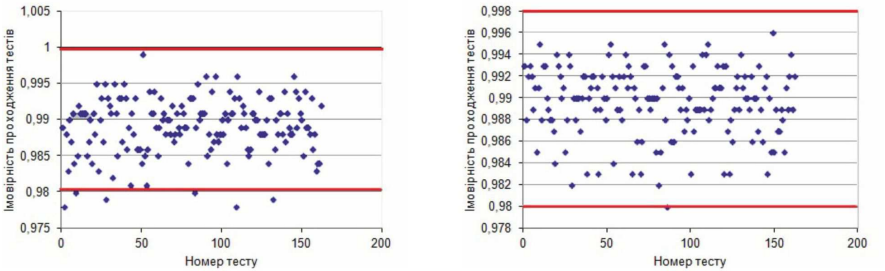
Тест вважається пройденим, коли ймовірність проходження тесту P потрапить у межі від 0,98 до 1,00. Якщо ж імовірність P буде знаходитись нижче 0,98, вважається, що тест не пройдено. За отриманими результатами будуємо статистичний портрет генераторів, який складається з матриці розміром m×q, де m – кількість двійкових послідовностей, які перевіряють, а q – кількість статистичних тестів, які використовуються для тестування кожної послідовності. Кінцеве рішення про випадковість послідовності приймається за результатами сукупності усіх тестів [7].

Тестування проводили за рівня значущості α = 0,01, який рекомендований розробниками NIST STS. Статистичні портрети генераторів (рис. 2 та рис. 3) мають вигляд матриці розміром 1000×188, елементами якої є 188000 значень відповідних ймовірностей. На усіх рисунках довірчий інтервал позначено червоними лініями.



а) *б)*

Рис. 2. Статистичний портрет генератора Джіффі №1: *а) r=1, б) r=5*



а) *б)*

Рис. 3. Статистичний портрет генератора Джіффі №4: *а) r=1, б) r=5*

Досліджено велику кількість генераторів, але оптимізацію параметрів в роботі показано на прикладі кількох комбінацій:

1. Генератор Джіффі №1: LFSR 1 та LFSR 2 на основі полінома $\Phi(x) = 1 \oplus x^{12} + x^{17}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
2. Генератор Джіффі №2: LFSR 1 основі полінома $\Phi(x) = 1 \oplus x^{12} + x^{17}$ та LFSR 2 на основі полінома $\Phi(x) = 1 \oplus x^{18} + x^{25}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
3. Генератор Джіффі №3: LFSR 1 та LFSR 2 на основі полінома $\Phi(x) = 1 \oplus x^{18} + x^{25}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$;
4. Генератор Джіффі №4: LFSR 1 та LFSR 2 на основі полінома $\Phi(x) = 1 \oplus x^{18} + x^{31}$; LFSR 3 – $\Phi(x) = 1 \oplus x^{6} + x^{7}$.

Детальний звіт оцінювання генераторів Джіффі за кожним тестом наведено в таблиці.

Результати здійсненого дослідження свідчать, що із збільшенням степеня r базових генераторів М-послідовностей якість генератора Джіффі покращується, оскільки кількість не пройдених тестів зменшується.

Табл. Результати тестування генераторів Джіффі

№	Статистичний тест	Номер досліджуваних генераторів							
		1		2		3		4	
		r=1	r=5	r=1	r=5	r=1	r=5	r=1	r=5
1	Frequency (Monobit) Test	–	–	–	+	–	+	+	+
2	Frequency Test within a Block	–	–	–	+	–	+	–	+
3	Cumulative Sums (Cusum) Test	–	–	–	–	–	+	+	+
4	Runs Test	–	–	+	+	+	+	+	+
5	Test for the Longest Run of Ones in a Block	–	–	+	+	+	+	+	+
6	Binary Matrix Rank Test	+	+	+	+	+	+	+	+
7	Discrete Fourier Transform (Specral) Test	–	–	–	–	–	–	+	+
8	Non-Overlapping Template Matching Test	–	–	+	+	+	+	–	+
9	Overlapping Template Matching Test	–	–	+	+	+	+	+	+
10	Maurer's "Universal Statistical" Test	+	–	+	+	+	+	+	+
11	Approximate Entropy Test	–	–	+	+	+	+	+	+
12	Serial Test	–	–	+	+	+	+	+	+
13	Linear Complexity Test	+	–	+	+	+	+	+	+
14	Random Excursions Test	–	+	+	+	+	+	+	+
15	Random Excursions Variant Test	–	+	+	+	+	+	+	+

Висновки. За допомогою імітаційного моделювання та статистичного тестування доведено, що змінюючи структуру базових генераторів М-послідовностей, а саме збільшуючи значення степеня r та вибираючи твірний поліном більшого степеня, можна значно покращити якість імпульсної послідовності з виходу генератора Джіффі. Дослідження показали, що оптимальним значенням є $r = 5$. Подальше збільшення r для великих степеней твірного поліному не призводить до значного покращення якості вихідної послідовності, але при цьому зростають апаратні затрати на реалізацію такого генератора.

Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М. : Изд-во КУДИЦ – ОБРАЗ, 2001. – 368 с.

2. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М. : Изд-во КУДИЦ – ОБРАЗ, 2003. – 240 с.

3. Гарасимчук О.І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О.І. Гарасимчук, В.М. Максимович // Захист інформації : зб. наук. праць. – К., 2002. – 7 с.

4. Гарасимчук О.І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О.І. Гарасимчук, В.М. Максимович // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні науки та інформаційні технології. – Львів : Вид-во НУ "Львівська політехніка". – 2004. – № 521. – С. 17-23.

5. Rock A. Pseudorandom Number Generators for Criptographic Applications / A. Rock. – Salzbuburg, 2005. – Pp. 57-65.

6. Статистические тесты NIST. [Электронный ресурс]. – Доступный с http://ru.wikipedia.org/wiki/Статестичиские_тесты_NIST.

7. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. [Electronic resource]. – Mode of access http://csrc.nist.gov/publications/nistpubs//SP800-22rev1 a.pdf.

Отенко В.И., Гарасимчук О.И., Журавель И.М., Костив Ю.М., Пастух А.Ю. **Оптимизация параметров структурных элементов генератора Джиффи**

Представлены результаты исследования генератора Джиффи при разном количестве базовых генераторов на основе регистров сдвига с линейным обратной связью и разной степени их полиномов, которое проведено с использованием статистических тестов NIST. Важное значение среди генераторов псевдослучайных последовательностей занимает генератор Джиффи, однако его качественные характеристики являются малоисследованными. Полученные результаты позволяют оптимизировать параметры генератора при заданных параметрах исходной импульсной последовательности.

Приведены принципы оптимизации параметров структурных элементов генератора Джиффи. Качество такой оптимизации подтверждена пакетом статистических тестов NIST STS.

Ключевые слова: генератор псевдослучайных чисел, статистические характеристики, генератор Джиффи.

Otenko V.I., Harasymchuk O.I., Zhuravel I.M., Kostiv Yu.M., Pastukh A.Yu. **The Optimization of Parameters Related to Geffe Generator Structural Elements**

The results of the study of Geffe generator at different base number of generators based on linear feedback shift register and varying degrees of polynomials, conducted using statistical tests NIST, are presented. Geffe generator plays an important role within pseudorandom sequence generators, although its quality characteristics are scarcely explored. The obtained results allow optimizing generator parameters for a given output pulse sequence parameters. Some principles for parameter optimization of structural elements of Geffe generator are provided. The quality of such optimization package was confirmed by statistical NIST STS tests.

Key words: pseudorandom generator, statistic characteristics, Geffe generator.

УДК 629.1 ***Доц. В.А. Таземдінов, канд. техн. наук – Черкаський ДТУ***

НЕЙРОМЕРЕЖЕВЕ ПРОГНОЗУВАННЯ РИНКУ НЕРУХОМОСТІ У КРИЗОВИХ УМОВАХ

Здійснено прогнозування ринку нерухомості у кризових умовах за допомогою нейромережі. Для нейромережевого прогнозування ринку нерухомості у кризових умовах створено зведену таблицю з даними про об'єкти нерухомості. Наведено схематичний процес навчання нейромережі. На підставі даних про об'єкти нерухомості проведено навчання нейромережі. Застосовано методи математичної статистики, засновані на сукупності певних правил для точних цифрових даних узагальненого характеру. Загальний прогноз за нейромережевого прогнозування ринку нерухомості у кризових умовах знайдено шляхом множення значення детермінації на кожне індивідуальне значення, отримане на основі результату нейромережевого моделювання.

Ключові слова: нейромережа, навчання, ринок нерухомості, прогнозування, нейрон, комірка.

Постановка проблеми. В умовах сьогодення ринок нерухомості перебуває не у кращому стані. Це є впливом економічної кризи, що склалася у межах держави, нестійким попитом, що є наслідком цього, та нестабільною пропозицією. На сьогодні питання прогнозування ринку нерухомості для багатьох є актуальним питанням, що потребує досліджень та інновацій. Аналітична робота у сфері нерухомості складна та багатогранна, що вимагає дослідження методологій у підходах та правилах інтерпретації даних і алгоритму вироблення рекомендацій.

На сьогодні, в умовах зростання соціальної інфраструктури, ділової активності, потреб забезпеченості житлом, недостатність аналітичних оцінок у

рамках ринку нерухомості є прямим чинником впливу на територіальний розвиток, що, водночас, приводить до більшості криз місцевих громад.

Упродовж останніх кількох років, на основі програми розвитку державного регулювання ринку нерухомості діє методика формування інформаційної бази. В її основу закладено отримання інформації про ринок нерухомості, житловий фонд, ринок будівельних матеріалів та ін. Проте ця методика є доволі складною та потребує вдосконалення. Тому проблема прогнозування ринку нерухомості є актуальною в умовах сьогодення.

Ступінь дослідження в науковій літературі. Фундаментальну основу в розвитку теорії нейрокомп'ютинга і його застосування у фінансовій сфері склали вчені країн Заходу і США. Це насамперед: Д.-Е. Бестенс, Ван ден Берг [1], D.E. Rummelhart, G.E. Hinton, R.G. Williams [2], R.B. Berrens, M. McKee [3], J.B. Ramsey [4], D.F. Specht [5] та ін. До вітчизняних вчених варто віднести: А. Єжова [6], Б. Одинцова, А. Романова, С. Шумського, В.А. Бившего, А.І. Богомолова, В.І. Костюніна [7] та ін., котрі розробляють і впроваджують нейромережеві технології у галузі економіки.

З методологічної точки зору, моделювання динаміки макроекономічних показників у площині статистичного моделювання і прогнозування вивчено вітчизняними авторами, зокрема Г.М. Стерніком [8], Ж.А. Морозовою [9]. Механізм побудови класифікацій методів прогнозування та методик прийняття рішення про вибір оптимального методу прогнозування досліджено у роботах таких науковців, як H. Wittkemper, M. Steiner [10] та ін.

Мета роботи. Здійснити прогнозування ринку нерухомості у кризових умовах за допомогою нейромережі. Навести схематичний процес навчання нейромережі. На підставі даних про об'єкти нерухомості провести навчання нейромережі. Застосувати методи математичної статистики, засновані на сукупності певних правил для точних цифрових даних узагальненого характеру.

Виклад основного матеріалу. На сьогодні, у рамках сформованої ситуації на Сході України, і наслідків, що спричинили крах української економіки, прогнозування ринку нерухомості є досить актуальною проблемою. На основі проведеного дослідження методологічної бази прогнозування ринку нерухомості [8, 9] на перше місце виходить багатофакторне прогнозування – нейронне моделювання. Цей метод моделювання заснований на багатофакторній моделі нейронних мереж. В основу цього методу покладено структурний апарат, що має у своєму складі шість окремих параметрів, які певною мірою взаємопов'язані. Перший – це таблиця, вона містить певний склад індикаторів стану ринку по всіх його сегментах, який визначається на основі даних про об'єкти нерухомості (площа, термін введення в експлуатацію, якість, місце розташування).

Комірка дискретної моделі – це дані по одному конкретному сегменту у локальному ринку нерухомості. Ще одним, не менш важливим параметром, є просторова вісь, що визначає для кожної конкретної комірки її індивідуальне місце розташування або ж його адресу.