УДК 255:29.1

ДОСЛІДЖЕННЯ ВПЛИВУ ПАРАМЕТРІВ ГЕНЕРАТОРА ГОЛЛМАННА НА СТАТИСТИЧНІ ХАРАКТЕРИСТИКИ ВИХІДНОГО СИГНАЛУ

М. М. Мандрона, В. М. Максимович, Ю. М. Костів, О. І. Гарасимчук
Національний університет «Львівська політехніка»
вул. Степана Бандери, 12, м. Львів, 79013, Україна. E-mail: mandrona27@gmail.com
Львівський державний університет безпеки життєдіяльності
вул. Клепарівська, 35, м. Львів, 79007, Україна.

Проводиться дослідження роботи генераторів Голлманна з різними значеннями степенів твірного поліному при сталій кількості базових генераторів М-послідовності. Розглянуто методику побудови статистичного портрету генераторів. Оцінено якість статистичних характеристик за допомогою набору тестів NIST. Побудовано статистичні портрети генераторів псевдовипадкових послідовностей з позначенням довірчого інтервалу. Здійснений підрахунок кількості структурних елементів дав можливість зробити висновок, що для побудови якісного генератора псевдовипадкових послідовностей достатньо лише 75 структурних елементів. У роботі було виявлено покращення якості генератора при збільшенні кількості степенів твірного поліному. Наведені у статті результати дозволили запропонувати параметри оптимізації при побудові якісних генераторів псевдовипадкових послідовностей, які можуть використовуватись як у засобах обчислювальної і вимірювальної техніки, так і у системах захисту інформації.

Ключові слова: генератор псевдовипадкових послідовностей, статистичні тести NIST, статистичний портрет.

ИССЛЕДОВАНИЕ ВЛИЯНИЯ ПАРАМЕТРОВ ГЕНЕРАТОРА ГОЛЛМАННА НА СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ ВЫХОДНОГО СИГНАЛА

М. М. Мандрона, В. М. Максымовыч, Ю. М. Костив, О. І. Гарасимчук
Национальный университет «Львовская политехника»
ул. Степана Бандеры, 12, г. Львов, 79013, Украина. E-mail: mandrona27@gmail.com
Львовский государственный университет безопасности жизнедеятельности
ул. Клепаровская, 35, г. Львов, 79007, Украина.

Проводится исследование работы генераторов Голлманна с различными значениями степеней образующей поленома при постоянном количестве базовых генераторов М-последовательности. Рассмотрена методика построения статистического портрета генераторов. Оценено качество статистических характеристик с помощью набора тестов NIST. Построены статистические портреты генераторов псевдослучайных последовательностей с обозначением доверительного интервала. Проведенный подсчет количества структурных элементов позволил сделать вывод, что для построения качественного генератора псевдослучайных последовательностей достаточно лишь 75 структурных элементов. В работе были выявлены улучшения качества генератора при увеличении количества степеней образующей полинома. Приведенные в статье результаты позволили предложить параметры оптимизации при построении качественных генераторов торов псевдослучайных последовательностей, которые могут использоваться как в средствах вычислительной и измерительной техники, так и в системах защиты информации.

Ключевые слова: генератор псевдослучайных последовательностей, статистические тесты NIST, статистический портрет.

АКТУАЛЬНІСТЬ РОБОТИ. Зважаючи на швидкий розвиток інформаційних технологій, засобів обчислювальної і вимірювальної техніки значно розширилась сфера застосування генераторів випадкових і псевдовипадкових послідовностей, а тому висуваються нові вимоги до їх проектування та методів оцінки якості.

Однією з переваг генераторів псевдовипадкових послідовностей є те, що на виходах таких генераторів отримується результат, який можна повторити нескінченну кількість разів, при заданні однакових початкових умов і параметрів [1].

Визначення якості та надійності роботи генераторів випадкових і псевдовипадкових послідовностей відноситься до одного з основних завдань сучасної прикладної та теоретичної криптографії, тому що вони широко використовуються для генерації ключів та інших випадкових параметрів криптосистем, а також у сфері технічного захисту інформації для пригнічення електромагнітного випромінювання, зашумлення приміщення, при побудові генераторів шуму. Існують спеціальні системи статистичного тестування та оцінювання якості випадкових послідовностей, зокрема тести Д. Кнута, DIEHART, CRYPT-S, FIPS. Проте найвідомішим серед них є набір статистичний тестів NIST, який використовується багатьма криптоаналітиками світу.

Мета роботи – дослідити якість генератора Голлманна змінюючи його параметри, а саме значення степенів твірного поліному і використовуючи набір

статистичних тестів NIST визначити оптимальні параметри генератора.

МАТЕРІАЛ І РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ. Генератор Голлманна складається з кількох послідовно з'єднаних генераторів М-послідовностей (регістрів зсуву), тактування кожного з яких керується попереднім генератором. Вихід останнього генератора М-послідовностей є виходом генератора. У роботі [2] детально описано принцип роботи та наведено структурну схему генератора Голлманна.

У цій роботі для генераторії псевдовипадкових послідовностей використовуються п'ять генераторів Голлманна, які побудовані на основі трьох генераторів М-послідовності, твірні поліномами яких подані у табл. 1.

Таблиця 1 – Генератори Голлманна, які досліджуються у роботі

Номер генератора ПВП	Рівняння функціонування генератора Голлманна
1	$\Phi(x)= 1 \oplus x^6 \oplus x^7$
2	$\Phi(x)= 1 \oplus x^{12} \oplus x^{17}$
3	$\Phi(x)= 1 \oplus x^{18} \oplus x^{25}$
4	$\Phi(x)= 1 \oplus x^{18} \oplus x^{31}$
5	$\Phi(x)= 1 \oplus x^{42} \oplus x^{47}$

У першу чергу необхідно перевірити, чи псевдовипадкові послідовності, які згенеровані мають хороші статистичні властивості відносно випадковості розподілу і взаємозалежності між елементами. Для цього використаємо набір статистичних тестів NIST.

Статистичні тести NIST використовуються для визначення якісних і кількісних ознак випадкових послідовностей [3–6].

До складу набору NIST входять 15 статистичних тестів. Але, при тестуванні обчислюється 188 значень імовірності P, які можна розглядати як результат роботи окремих тестів.

На підставі результатів тестування приймається або відхиляється гіпотеза про те, що дана послідовність є випадковою.

Результатом виконання кожного тесту є так зване значення P, яке лежить в діапазоні [0, 1]. Для кожного тесту вибирається рівень значущості α. Якщо значення імовірності $P \geq \alpha$, то послідовність є випадковою, якщо значення імовірності $P < \alpha$ – не є випадковою [4, 5]. Значення α вибирається в інтервалі [0.001, 0.01].

Кожну послідовність перевіряють з використанням пакету NIST. Внаслідок такої перевірки формується портрет генератора.

Статистичний портрет – це матриця розміром m x q, де m – кількість двійкових послідовностей, які перевіряються, а q – кількість статистичних тестів [5].

№ тесту j		№ послідовності i		
	1	2	…	q
S_1	$P_{1,1}$	$P_{1,2}$	…	$P_{1,q}$
S_2	$P_{2,1}$	$P_{2,2}$	…	$P_{2,q}$
…	…	…	…	…
S_m	$P_{m,1}$	$P_{m,2}$	…	$P_{m,q}$

$$\begin{pmatrix} P_{11} & P_{12} & \dots & P_{1q} \\ P_{21} & P_{22} & \dots & P_{1q} \\ \dots & \dots & \dots & \dots \\ P_{m1} & P_{m2} & \dots & P_{mq} \end{pmatrix} \quad (1)$$

За отриманим статистичним портретом визначають частку послідовностей, що пройшли кожен статистичний тест. Для цього задають рівень значущості α та здійснюють підрахунок значень імовірності P, що перевищують встановлений рівень α для кожного з q тестів, тобто визначають коефіцієнт

$$\tilde{\tilde{R}} = \{\overline{R}_i = \{r_{ij} = \frac{1}{m}\begin{cases} p_{ij}, якщо\ p_{ij} \geq \alpha \\ 0, якщо\ p_{ij} < \alpha \end{cases}, j = \overline{1,q}\}, i = \overline{1,m}\} \quad (2)$$

У результаті формується вектор коефіцієнтів $\overline{R}_i = \{r_{ij}, j = \overline{1,q}\}$, елементи якого характеризують у відсотках проходження послідовності S_i всіх статистичних тестів.

Вважається, що генератор пройшов тестування j-им тестом, якщо значення коефіцієнта r_{ij} знаходиться у межах [r_{max}, r_{min}]. Межі довірчого інтервалу визначаються за таким виразом [5].

$$r_{max(min)} = p \pm 3\sqrt{\frac{p(1-\alpha)}{m}}, \text{ де } p = 1 - \alpha \quad (3)$$

Підставивши відповідні значення, а саме α = 0,01 і m = 1000 отримаємо

$$r_{min} = (1 - \alpha) - 3\sqrt{\frac{(1-\alpha)\alpha}{m}} = 0.980561$$

$$r_{max} = (1 - \alpha) + 3\sqrt{\frac{(1-\alpha)\alpha}{m}} = 0.999439$$

За результатами обчислень визначено межі довірчого інтервалу, якщо результат виконання тесту потравляє у межі 0,999439–0,0980561, то робимо висновок, що тест успішно пройдено, якщо не потрапляє – не пройдено. На усіх рисунках довірчий інтервал позначено широкими пунктирними лініями.

Тестування проводилося при рівні значущості α = 0,01, який рекомендований розробниками НІСТ [3]. У даному випадку статистичний портрет генератора має вигляд матриці розміром 1000×188, елементами якої є 188000 значень відповідних імовірностей.

Результати статистичних досліджень генераторів Голлмана подано на рис. 1–5. По вісі абсцис відкладено номер тесту NIST, по вісі ординат – імовірність проходження тесту.

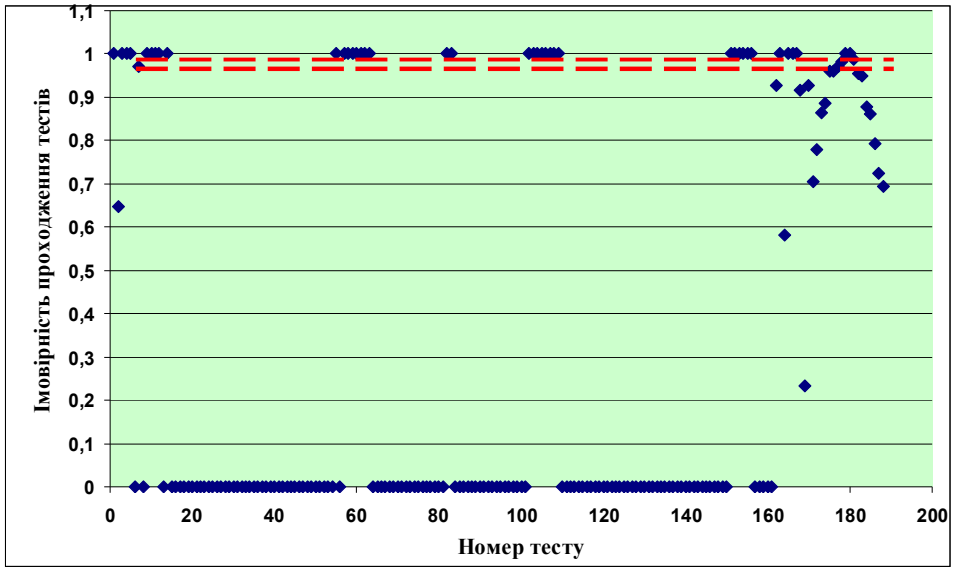

Рисунок 1 – Статистичний портрет генератора № 1

З рис. 1 видно, що генератор твірного поліному сьомого ступеня має погані статистичні характеристики. Практично всі результати тестування знаходяться за межами довірчого інтервалу. Спробуємо покращити якість генератора Голлманна, змінюючи значення ступеня поліному та проводити подальше оцінювання за допомогою пакету тестів NIST.

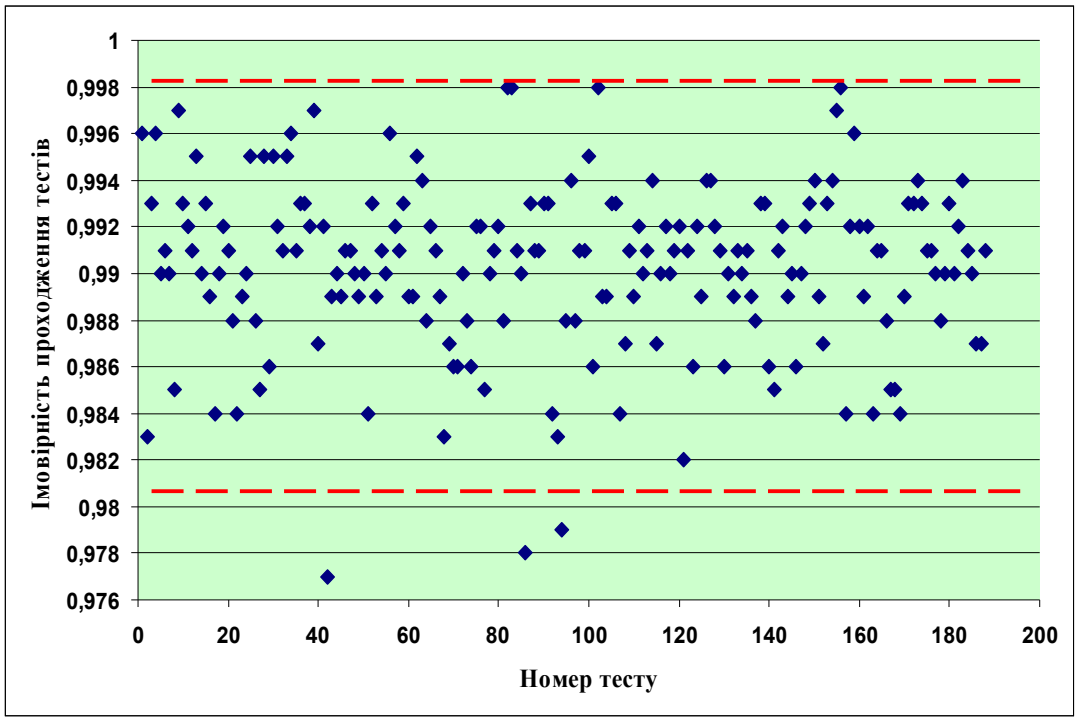

Рисунок 2 – Статистичний портрет генератора № 2

Як бачимо, генератор з твірним поліномом 17-го ступеня не пройшов лише три тести, що суттєво відрізняє його від попереднього генератора.

Спробуємо ще збільшити число ступеня, щоб порівняти статистичні характеристики досліджуваного генератора.

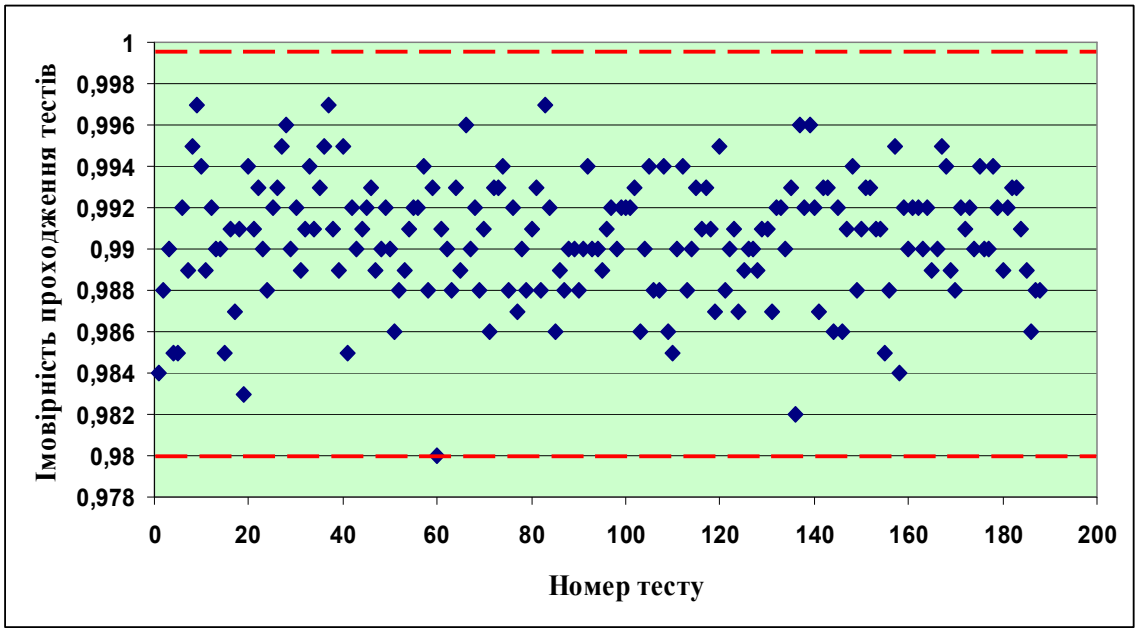

Рисунок 3 – Статистичний портрет генератора № 3

Статистичні характеристики генератора, зображеного на рис. 3, є значно покращеними. Всі тести пройдені, але лише один знаходиться на межі довірчого інтервалу. Спробуємо ще збільшити число ступеня поліному, щоб переконатись у покращенні якості генератора.

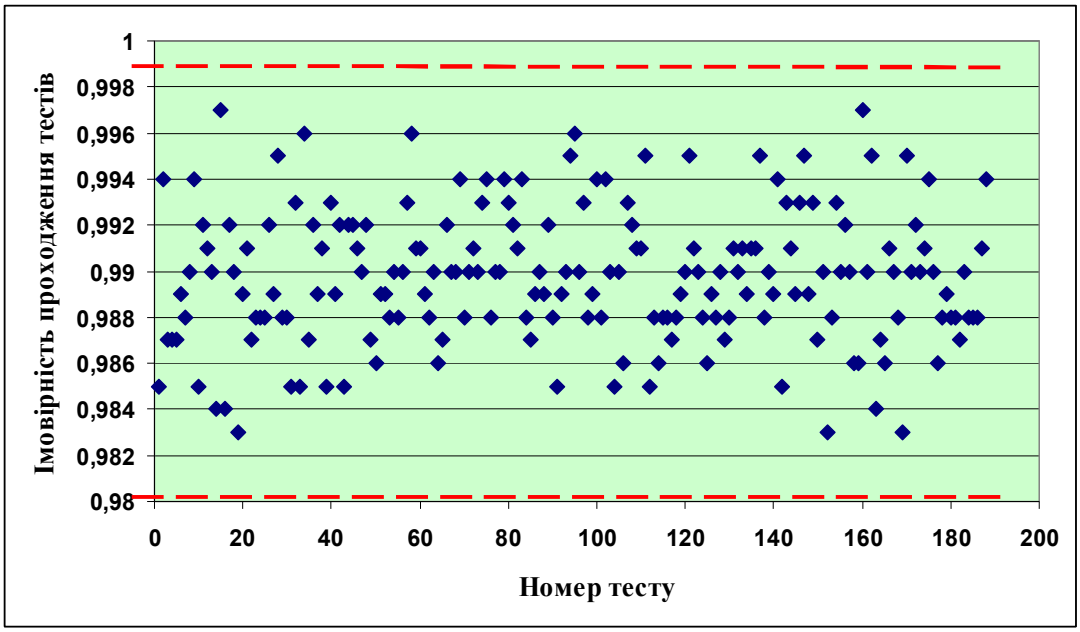

Рисунок 4 – Статистичний портрет генератора № 4

Як бачимо з рисунку 4, розроблений генератор проходить усі тести NIST. Результати трьох тестів знаходяться вище межі 0,983, що є вище довірчого інтервалу 0,98. Згідно з вимогами статистичного оцінювання за допомогою пакету NIST, результати тестування цього генератора свідчать про достатню криптографічну стійкість.

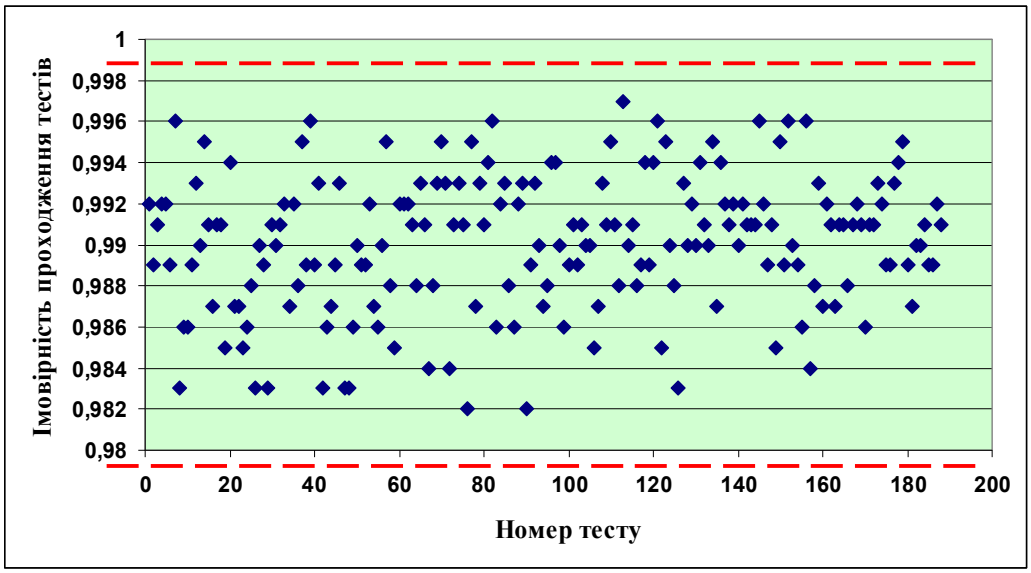

Рисунок 5 – Статистичний портрет генератора №5

На рис. 5. генератор також успішного пройшов тестування, два значення знаходяться на межі 0,982, що є вищим за довірчий інтервал.

Як видно з наведених рисунків, зі збільшенням кількості ступеня твірного поліному якість генератора Голлманна покращується, оскільки кількість непройдених тестів зменшується.

Детальний звіт по оцінюванні генераторів Голлманна за допомогою набору статистичних тестів NIST п'яти вищезгаданих генераторів Голлманна, реалізованих на основі трьох базових генераторів М-послідовності з різними значеннями твірного поліному наведено в табл. 2, у якій вказано, які саме тести успішно пройдено, а які ні.

Таблиця 2 – Результати тестування генератора Голлманна на основі трьох базових генераторів М-послідовності з різними твірними поліномами

Статистичний тест	Номер досліджуваних генераторів				
	1	2	3	4	5
Монобітний (частотний) тест	–	+	+	+	+
Частотний блоковий тест	–	+	+	+	+
Тест накопичених сум	–	+	+	+	+
Тест перевірки серій	–	+	+	+	+
Найдовшої серії одиниць	–	+	+	+	+
Перевірки рангу двійкових матриць	–	+	+	+	+
Тест на основі дискретного пертворення Фур'є	–	+	+	+	+
Тест на відповідність з шаблоном без перекриття	–	–	+	+	+
Тест на відповідність з шаблоном з перекриття	–	+	+	+	+
Універсальний тест Мауера	–	+	+	+	+
Тест на основі апроксимації ентропіїї	–	+	+	+	+
Тест серій	–	+	+	+	+
Тест лінійної складності	–	+	+	+	+
Тест випадкових блокувань	–	+	+	+	+
Тест випадкових блокувань 2	–	+	+	+	+

З усіх рисунків і табл. 2 наглядно видно, що починаючи з генератора № 3 результати тестування позитивні.

Як видно з табл. 3, що для побудови якісного генератора псевдовипадкових чисел достатньо лише 75 структурних елементів, тому що саме генератор № 3 першим успішно пройшов тестування усіма тестами.

Таблиця 3 – Підрахунок кількості структурних елементів для побудови генераторів Голлманна

№	Генератори	Кількість структурних елементів
1.	$\Phi(x)= 1 \oplus x^6 \oplus x^7$	21
2.	$\Phi(x)= 1 \oplus x^{12} \oplus x^{17}$	51
3.	$\Phi(x)= 1 \oplus x^{18} \oplus x^{25}$	75
4.	$\Phi(x)= 1 \oplus x^{18} \oplus x^{31}$	93
5.	$\Phi(x)= 1 \oplus x^{42} \oplus x^{47}$	141

ВИСНОВКИ. У результаті досліджень було виявлено, що при збільшенні кількості ступенів твірного поліному покращується якість генератора. Як видно з результатів тестування п'яти генераторів Голлманна, перший генератор із твірним поліномом сьомого ступеня повністю не пройшов усі тести. Це означає, що в послідовності є близько розташовані один до одного повторювані ділянки, що, в свою чергу, демонструє відхилення від випадкового характеру досліджуваної послідовності. Другий генератор не пройшов лише три тести, а отже даний генератор не можна використовувати у криптографії, проте його можна використати як елемент складнішої криптографічної системи. Всі інші генератори успішно пройшли всі тести, що свідчить про перспективи їх використання у системах захисту інформації. Проведений підрахунок кількості логічних елементів показав, що для побудови якісного генератора ПВП достатньо лише 75 структурних елементів. Отримані результати дають змогу оптимізувати параметри при побудові якісного генератора псевдовипадкових послідовностей.

ЛІТЕРАТУРА

1. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О.І. Гарасимчук, В.М. Максимович // Захист інформації. – К., 2002. – № 3. – С. 29–36.

2. Оцінка якості генератора Голлманна, реалізованого на основі модифікованих генераторів М-послідовностей / О.І. Гарасимчук, Ю.М. Костів, Т.Г. Паршенко // Системи обробки інформації – Харків: ХУПС, 2010. – № 6 (87). – С. 35–38.

3. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М.: КУДИЦ–ОБРАЗ, 2003. – 240 с.

4. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс]. Режим доступу: http://csrc.nist.gov/publications/nistpubs//SP800-22rev1a.pdf

5. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Вид-во «Форт», 2012. – 880 с.

6. Кравцов Г.О. NIST 800-22 українською мовою. Набір статистичних тестів для генераторів випадкових та псевдовипадкових чисел для криптографічних додатків. [Електронний ресурс]. – Режим доступу: http://www.itsway.kiev.ua/pdf/Articles180106.pdf.

IMPACT STUDY OF PARAMETERS OF THE GOLLMANN GENERATOR ON STATISTICAL CHARACTERISTICS OF OUTPUT SIGNAL

M. Mandrona, V. Maksymovych, Yu. Kostiv, O. Harasymchuk
Lviv Polytechnic National University
vul. Stepan Bandera, 12, Lviv, 79013, Ukraine. E-mail: mandrona27@gmail.com
Lviv State University of Life Safety
vul. Kleparivska 35, Lviv, 79007, Ukraine.

In this paper, the authors have presented the research results of operation of the Gollmann generators with the different values of the degree of a polynomial generatrix when the number of M-sequence base generators remains constant. The technique allows creating a generator statistical portrait is described. The quality of the statistical characteristics was proved through the NIST tests. The statistical portraits of pseudorandom sequence generators were constructed with their confidence interval specified. Counting the number of structural elements has led to conclusion that for a high-quality pseudorandom sequence generator to be constructed only 75 structural elements are needed. Also, the operation quality enhancement of the generator is revealed when increasing the degree of a polynomial generatrix. The research results obtained allow for new options of optimizing the construction of high-quality pseudorandom sequence generators, which can be used as for computing and measurement systems, as for information security systems.

Key words: pseudorandom sequence generator, statistical tests NIST, a statistical portrait.

REFERENCES

1. Harasymchuk, O.I., Maksymovych, V.M. (2002), "Pseudo-random number generators and their application, classification, basic architectural methods, and quality assessment", *Ukrainian information security research journal,* Kyiv, no. 3, pp. 29–36.

2. Harasymchuk, O.I., Kostiv, Yu.M., Parshenko, T.G. (2010), "Quality assessment of the Gollmann generator based on modified M-sequence generators", *Systems of information processing,* KhUAF, Kharkiv, no. 6 (87), pp. 35–38.

3. Ivanov, M.A., Chygynkov, I.V., (2003), *Teoriya, primenenie i otsenka kachestva generatorov psevdoslu chaynyih posledovatelnostey* [Theory, application, and evaluation of the quality of pseudorandom sequence generators], KYDUTS-Obraz, Moscow, Russia.

4. NIST SP 800-22. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, [electronic resource], available at: http://csrc.nist.gov/publications /nistpubs//SP800-22rev1a.pdf

5. Gorbenko, I.D., Gorbenko, Yu. I., (2012), *Prykladna kryptolohiya: Teoriya. Praktyka. Zastosuvannya* [The Applied Cryptology: Theory. Practice. Application], Fort, Kharkiv, Ukraine.

Стаття надійшла 03.08.2013.