Технічні науки

УДК 004.056.55

Шевчук Микола Сергійович
аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»
Шевчук Николай Сергеевич
аспирант кафедры безопасности информационных технологий
Национального университета «Львовская политехника»
Shevchuk Mykola
Postgraduate of the
National University "Lviv Polytechnic"

Максимович Володимир Миколайович
доктор технічних наук,
професор кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»
Максимович Владимир Николаевич
доктор технических наук,
профессор кафедры безопасности информационных технологий
Национальный университет «Львовская политехника»
Maksymovych Volodymyr
Doctor of Technical Sciences, Professor
National University "Lviv Polytechnic"

Мандрона Марія Миколаївна
кандидат технічних наук,
доцент кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка»

Мандрона Мария Николаевна
кандидат технических наук,
доцент кафедры безопасности информационных технологий
Национальный университет «Львовская политехника»
Mandrona Maria
Candidate of Technical Sciences, Associate Professor
National University "Lviv Polytechnic"

ДОСЛІДЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ ДЖИФФІ НА ОСНОВІ FCSR
ИССЛЕДОВАНИЕ ГЕНЕРАТОР ПСЕВДОСЛУЧАЙНЫХ БИТОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЖИФФИ НА ОСНОВЕ FCSR
RESEARCH OF THE GIFFY PSEUDORANDOM BIT SEQUENCE GENERATOR BASED ON FCSR

Анотація. *В статті представлені результати дослідження генератора Джиффі при різних базових регістрах FCSR і різній степені їх поліномів, що проводилось з використанням статистичних тестів NIST. Отримані результати дозволяють оптимізувати параметри генератора при заданих параметрах вихідної псевдовипадкової послідовності.*

Ключові слова: *псевдовипадкова бітова послідовність, генератори псевдовипадкових чисел, статистичні характеристики.*

Аннотация. *В статье представлены результаты исследования генератора Джиффи при различных базовых регистрах FCSR и разной степени их полиномов, который проводился с использованием статистических тестов NIST. Полученные результаты позволяют оптимизировать параметры генератора при заданных параметрах исходного псевдослучайной последовательности.*

Ключевые слова: *псевдослучайная битовая последовательность, генераторы псевдослучайных чисел, статистические характеристики.*

Summary. *The article presents the results of Jiffy generator estimation with a different number of basic FCSR generators, and different degrees of their polynomials, carried out with the use of NIST statistical tests. The received results allow to optimize the generator parameters at the given parameters of the output pseudorandom sequence.*

Key words: *pseudorandom generator, protection of information, pseudorandom numbers, statistic characteristics*.

Вступ. Генератори псевдовипадкових чисел (ГПЧ) і псевдовипадкових бітових послідовностей (ГПВБП) часто зустрічається в багатьох областях вимірювальної техніки, зокрема, при проектуванні і налагодженні потокових шифрів, та інформаційних технологій. При цьому вимоги до їх технічних характеристик відрізняються в залежності від мети їхнього застосування.

Генерування псевдовипадкових послідовностей і перевірка на випадковість згенерованої послідовності є одними з найважливіших проблем сучасної криптології. В сучасних криптосистемах генератори псевдовипадкових послідовностей використовуються для створення ключової інформації і забезпечення параметрів цих систем.

Відомо, що при реалізації криптографічних перетворень використовують різні псевдовипадкові послідовності. Звідси випливає, що стійкість криптоперетворень безпосередньо залежить від алгоритму формування псевдовипадкових чисел та послідовностей.

Метою роботи є використання статистичних тестів Національного інституту стандартів і технологій (НІСТ) США для тестування генераторів псевдовипадкових бітових послідовностей на основі генератора Джиффі.

Генератори псевдовипадкових бітових послідовностей на основі генератора Джиффі

Спрощена структурна схема генератора Джиффі наведена на рис. 1 [1]. До його складу входять три регістри FCSR1 – FCSR3 і мультиплексор MUX.

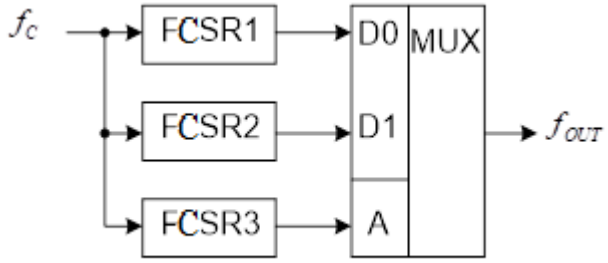


Рис. 1. Спрощена структурна схема генератора Джиффі

Генератор забезпечує перемішування двох імпульсних послідовностей з виходів FCSR1 і FCSR2 під керуванням послідовності з виходу FCSR3. У тому випадку коли значення періодів повторення вихідних послідовностей FCSR1, FCSR2, FCSR3 – T_{1p}, T_{1p}, T_{1p} попарно взаємно прості числа, період результуючою послідовності дорівнює добутку – $T_J = T_{1p} \cdot T_{2p} \cdot T_{3p}$ [1].

Нами були досліджені кілька варіантів побудови генератора Джиффі, при різних структурах FCSR, а саме:

$$F(x) = \begin{cases} x^{12} + x^{10} + x^8 + x^6 + x^5 + x^2 + x^1 + 1 \\ x^{12} + x^{11} + x^9 + x^7 + x^5 + x^3 + x^2 + x^1 + 1 \\ x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^3 + x^2 + x^1 + 1 \end{cases}$$ – варіант А;

$$F(x) = \begin{cases} x^{13} + x^9 + x^7 + x^2 + x^1 + 1 \\ x^{13} + x^{10} + x^6 + x^3 + x^2 + x^1 + 1 \\ x^{13} + x^{10} + x^9 + x^3 + x^2 + x^1 + 1 \end{cases}$$ – варіант Б;

$$F(x) = \begin{cases} x^{13} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + x^1 + 1 \\ x^{13} + x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + x^1 + 1 \\ x^{13} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^3 + x^2 + x^1 + 1 \end{cases}$$ – варіант В;

$$F(x) = \begin{cases} x^{13} + x^{10} + x^8 + x^6 + x^3 + x^2 + x^1 + 1 \\ x^{13} + x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + 1 \\ x^{13} + x^{10} + x^9 + x^7 + x^6 + x^3 + x^2 + x^1 + 1 \end{cases}$$ – варіант Г;

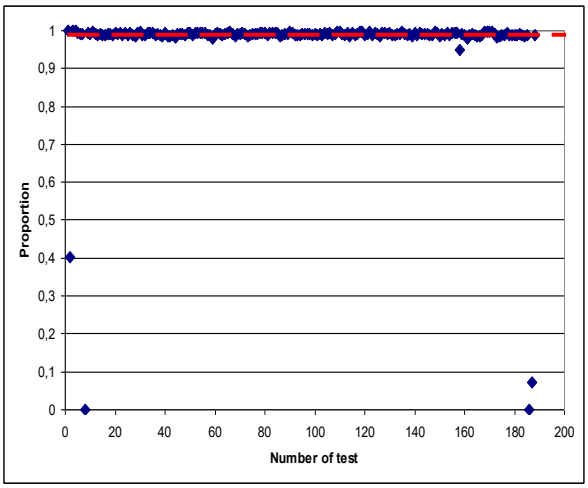
$$F(x) = \begin{cases} x^{32} + x^6 + x^3 + x^2 + 1 \\ x^{32} + x^7 + x^5 + x^2 + 1 \\ x^{32} + x^8 + x^3 + x^2 + 1 \end{cases}$$ – варіант Д;

$$F(x)=\begin{cases}x^{32}+x^{6}+x^{3}+x^{2}+1\\ x^{32}+x^{7}+x^{5}+x^{2}+1\\ x^{32}+x^{23}+x^{8}+x^{2}+1\end{cases}$$ – варіант Е;

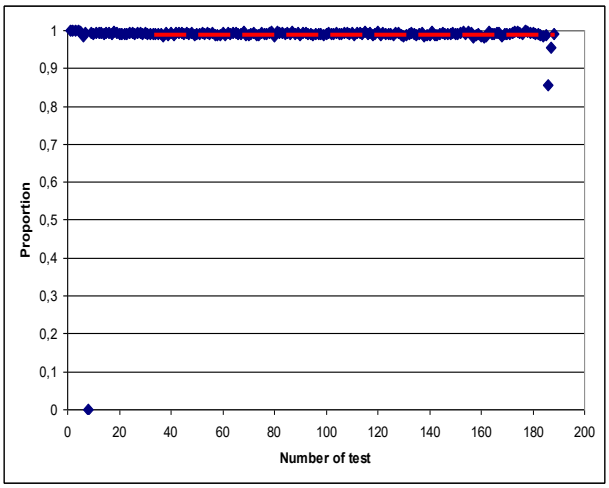
$$F(x)=\begin{cases}x^{32}+x^{7}+x^{5}+x^{2}+1\\ x^{32}+x^{13}+x^{5}+x^{2}+1\\ x^{32}+x^{16}+x^{2}+x^{1}+1\end{cases}$$ – варіант Є.

Для всіх FCSR був вибраний тип матриці T_1 і степінь матриці $r=1$.

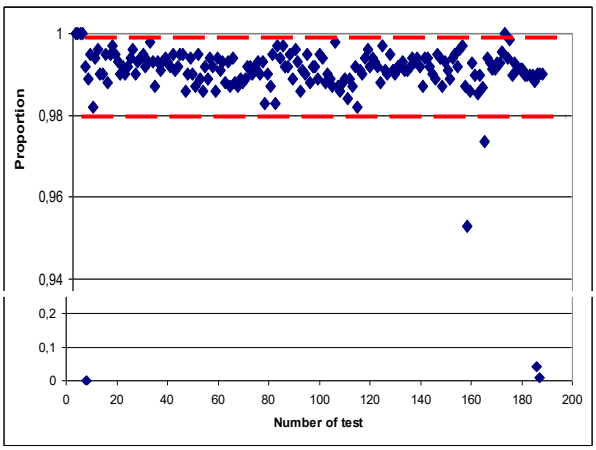
На рис. 2 наведені статистичні портрети вихідної послідовності досліджуваних генераторів Джиффі, отримані при випадково вибраних фіксованих початкових установках регістрів.



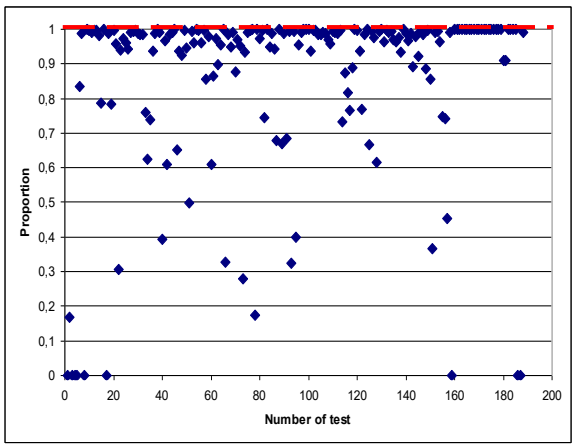
а



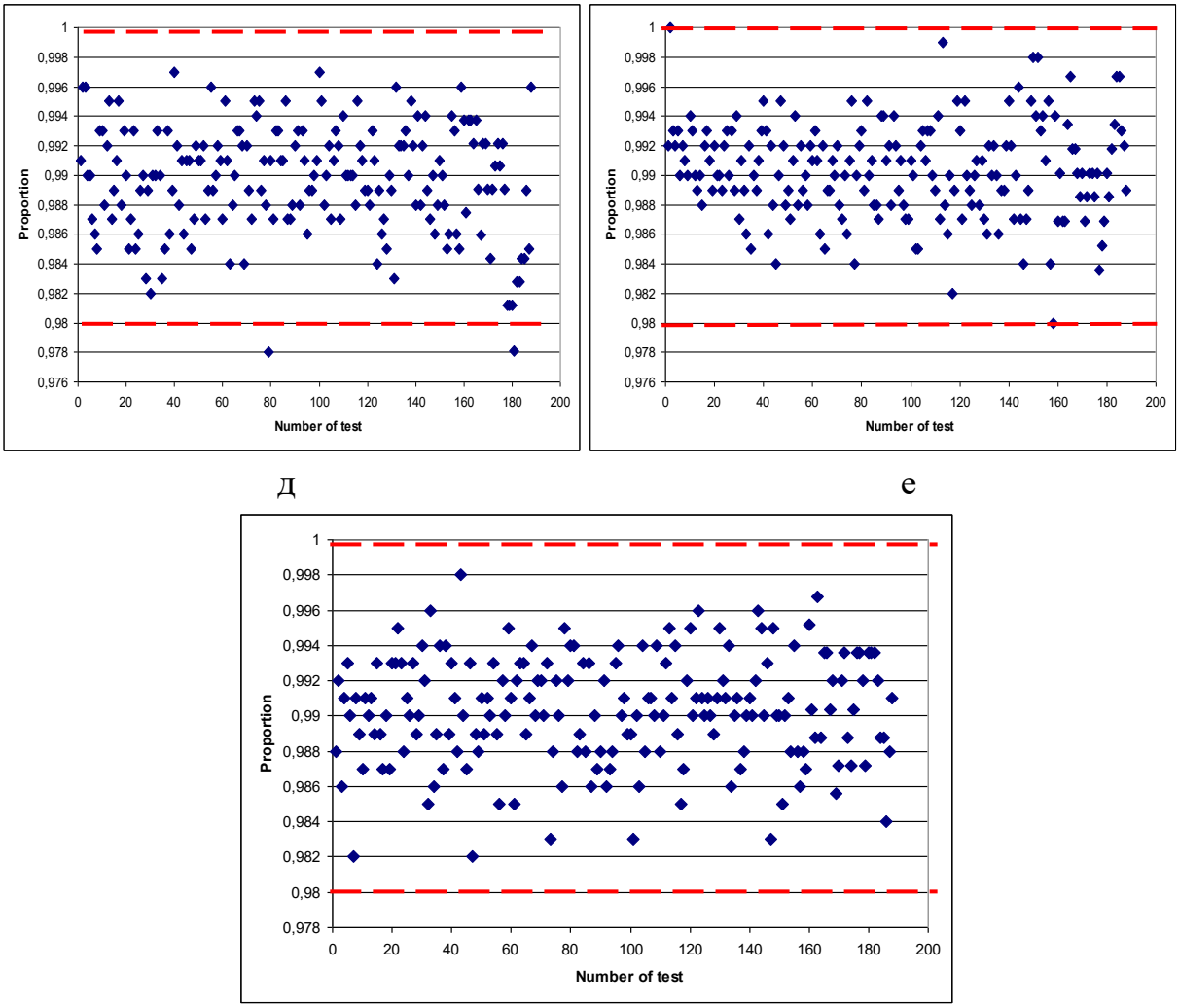
б



в



г



д е

є

Рис. 2. Статистичні портрети генератора Джиффі:
а –варіант А; б – варіант Б; в – варіант В; г – варіант Г;
д – варіант Д; е – варіант Е; є – варіант Є

Отже, у результаті дослідження статистичних характеристик генератора Джиффі, з'ясовано, що при малих степенях поліномів (варіанти А-Г), вихідна псевдовипадкова послідовність не проходить тести NIST. Із збільшенням степеня поліному покращуються статистичні характеристики генератора (рис. 2 д-є). Цікавим є спостереження генераторів варіантів Г і Д, як видно вони відрізняються лише наявності поліному 23 степеня у варіанті Д, при цьому статистичні характеристики відрізняються: варіант Г не пройшов два тести, варіант Д пройшов усі тести, а отже таких генератор відповідає вимогам випадковості і є статистично безпечним [*1]

У процесі імітаційного моделювання було зафіксовано, що період повторення вихідних послідовностей становить $T_J > 10^9$.

Кількість КЛБ, необхідних для побудови ГПВБП на основі генератора Джиффі, визначається сумарною кількістю розрядів усіх трьох FCSR – n_1, n_2, n_3, плюс один КЛБ для побудови мультиплексора[5]:

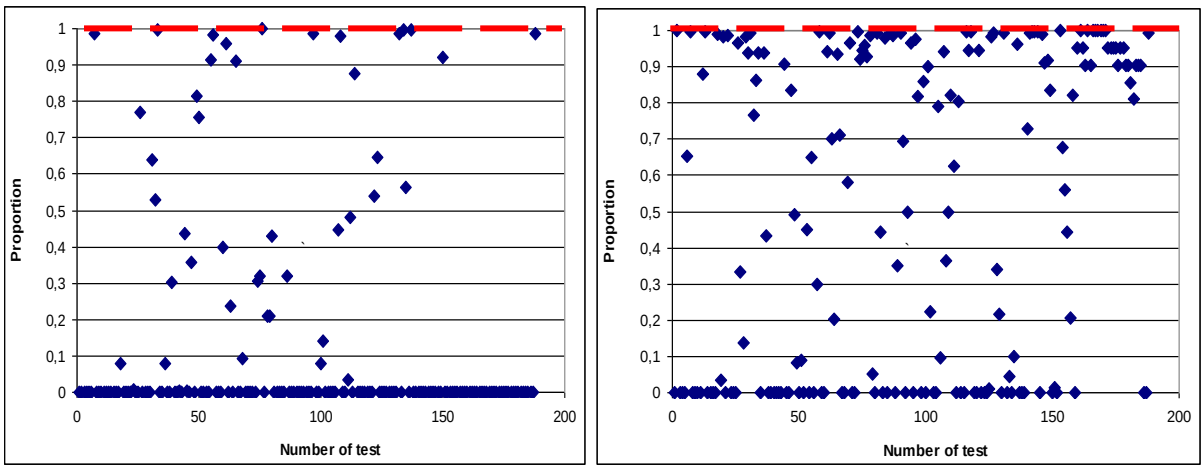
$$A_{JIFFY} = n_1 + n_2 + n_3 + 1. \quad (1)$$

Криптографічним ключем ГПВБП на основі FCSR є початкові стани усіх трьох регістрів[2-3]. Повна множина значень цих станів дорівнює $(2^{n_1} - 1) \cdot (2^{n_2} - 1) \cdot (2^{n_3} - 1)$[6], а довжина ключа визначається таким чином:

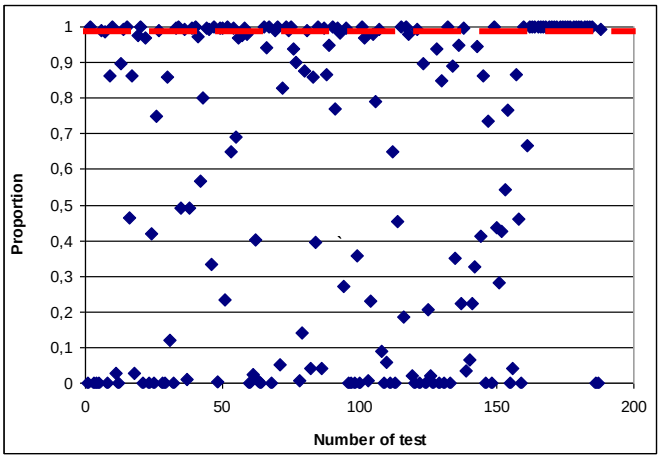
$$C_{JIFFY} = n_1 + n_2 + n_3. \quad (2)$$

В експериментальних цілях проводились дослідження чи має вплив початкових даних на якість вихідної послідовності генератора Джиффі. Для цього ми обрали два генератори, один має невипадкові характеристики (варіант Г), інший – випадковий (варіант Е).

На рис. 3 наведено статистичні портрети генератора Джиффі варіанту Г з такими початковими значеннями а – 000001, б – 100000 і в – 000111.



а б

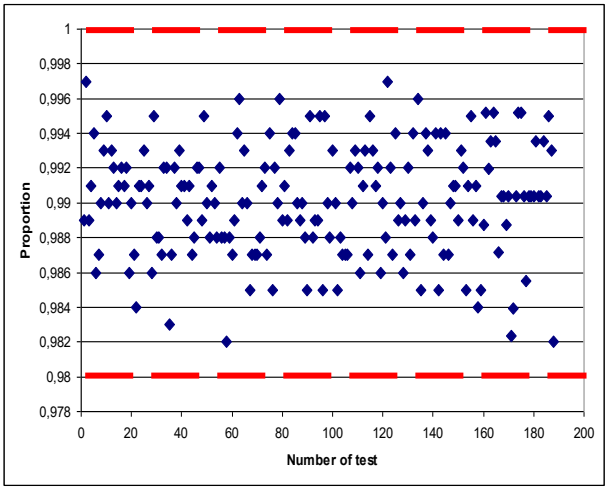


в

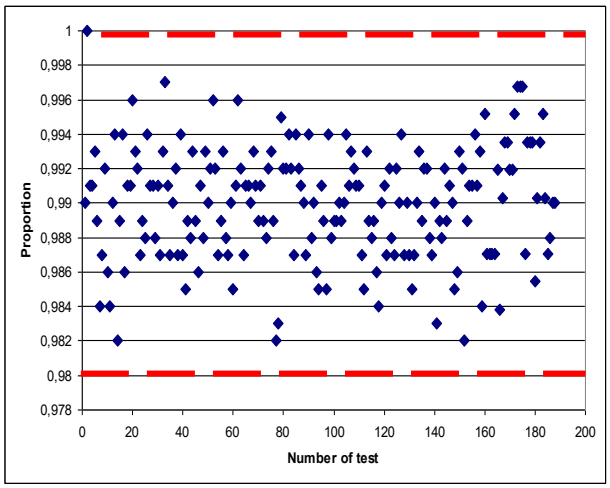
Рис. 3. Статистичні портрети генератора Джиффі (варіант Г) з різними початковими даними

Із рис. 3 наглядно видно, що жоден з протестованих генераторів не пройшов тести NIST, також видно, що зі зміною значень початкових даних не спостерігається динаміка покращення статистичних характеристик.

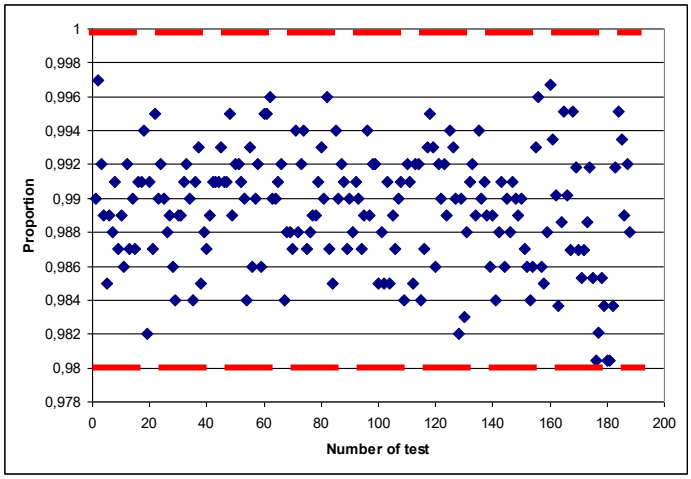
Нижче наведено аналогічні дослідження Джиффі для варіанту Е з такими ж початковими даними (рис. 4).



а



б



В

Рис. 4. Статистичні портрети генератора Джиффі (варіант Е) з різними початковими даними

Як видно із результатів тестування всі тести NIST пройдено. Отже, враховуючи ці та попередні дослідження (рис. 3 і 4), можна зробити висновок, що значення початкових даних не впливають на якість вихідної послідовності генератора Джиффі.

Висновок. Здійснене дослідження ГПВБП на основі генератора Джиффі показало, що навіть, не зважаючи на великий період повторення послідовності, при використанні малих значень степенів твірних поліномів генератори не є повністю статистично безпечними, але із збільшення степенів їх поліномів приводить до підвищення якості генератора. При зафіксованих значеннях цих поліномів ГПВБП Джиффі на основі FCSR проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики і криптостійкість.

Отже, такі генератори можна використовувати у криптографії безпосередньо, проте їх можна використати, як елементи складнішої криптографічної системи.

Література

1. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М.А. Иванова, И.В. Чугунков. – М. : НИЯУ МИФИ, 2012. – 400 с.
2. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы и исходные тексты на языке С / Б. Шнайер. – М. : Триумф, 2002. – 816 с.
3. Гапак О.М. Вісник НТУУ «КПІ» Інформатика, управління та обчислювальна техніка №63: «Оцінка якості генератора Голлманна, реалізованого на основі FCSR» – 2015. – № 63- 119-122 с.
4. NIST SP 800-22rev1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications / National Institute of Standards and Technology Special Publication 800-22rev1a, 2010, 131 p.
5. Гапак О. М. Визначення довжини періоду генераторів псевдовипадкових послідовностей на основі регістрів зсуву зі зворотним зв'язком та перенесення / О. М. Гапак // Моделювання та інформаційні технології – 2014. – №73. – С. 92– 97.
6. Максимович, В.М.; Мандрона, М.М.; Шевчук, М.С. (Національний університет ім. В. Даля, 2017) / Дослідження ГПВБП на основі генератора Джиффі.