Технічні науки

УДК 004.056.55

Шевчук Микола Сергійович

аспірант

Національного університету «Львівська політехніка»

Максимович Володимир Миколайович

доктор технічних наук, професор

Національний університет «Львівська політехніка»

Мандрона Марія Миколаївна

кандидат технічних наук, доцент

Національний університет «Львівська політехніка»

ДОСЛІДЖЕННЯ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ БІТОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КАСКАДІВ ГОЛЛМАНА, ЩО СКЛАДАЄТЬСЯ З LFSR

RESEARCH OF THE PSEUDORANDOM BIT SEQUENCE GENERATOR BASED ON GOLLMAN'S CASCADES WHICH CONTAINES LFSR

Анотація. *В статті представлені результати дослідження генератора на основі каскадів Голлмана при різних базових каскадах з регістрами LFSR 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.*

Summary. *The article presents the results of Gollman cascade generator estimation with a different number of LFSR cascades, 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[1].

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

Каскад Голлмана

Каскад Голлмана (див. 0-й), описаний в [2], являє собою посилену версію генератора "стоп-пішов". Він складається з послідовності LFSR, тактування кожного з яких управляється попереднім LFSR. Якщо виходом LFSR-1 в момент часу t є 1, то тактується LFSR-2. Якщо виходом LFSR-2 в момент часу t є 1, то тактується LFSR-3, і так далі. Вихід останнього LFSR і є виходом генератора. Якщо довжина всіх LFSR і однакова і рівна, лінійна складність системи з k LFSR дорівнює [2]: $n(2^n - 1)^{k-1}$

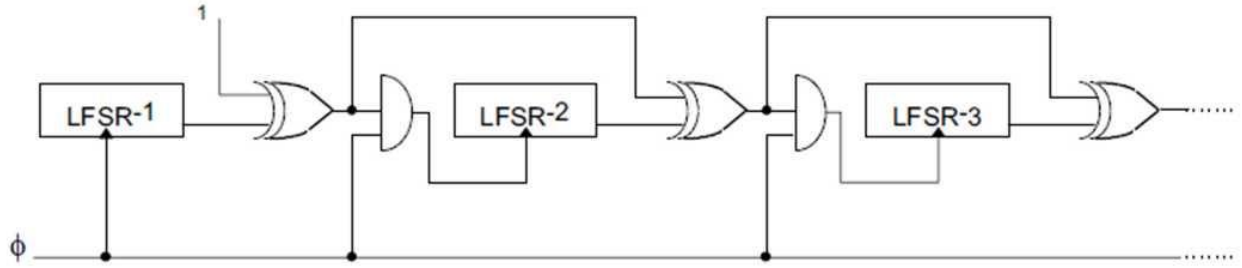

Рис. 1. Каскад Голлмана

Для дослідження ГПВП нами розроблений програмний засіб на мові Java. Цей засіб дозволяє згенерувати ПВП за алгоритмом Голлманна із різною кількістю, порядком та довжиною базових LFSR. Оскільки будь-які послідовності, які породжені ГПВП безпосередньо для криптографічних цілей, підлягають обов'язковому тестуванню, то для проведення оцінки якості генератора Голлманна ми обрали набір статистичних тестів NIST STS. Статистичні тести NIST STS [5] (National Institute of Standards and Technology Statistical Test Suite) використовуються для визначення якісних та кількісних ознак випадковості послідовності чисел. Сьогодні ця методика є найбільш поширеною серед розробників криптографічних засобів захисту інформації [3]. Пакет NIST STS містить 16 статистичних тестів, які розроблені для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, породжуваних ГПВП. Усі тести спрямовані на виявлення різних дефектів випадковості. Кожен тест

подається у розрізі мети, позначення, статистик, опису та правил інтерпретації результатів [4].

Таблиця 1

Результати статистичних тестів NIST для ГПВБП Голлмана при різних твірних поліномах та різній кількості каскадів

Твірні поліноми / Кількість регістрів в каскаді	$x^{12}+x^6+x^4+x^1+1$	$x^{16}+x^5+x^3+x^2+1$	$X^{23}+x^5+1$	$x^{29}+x^2+1$	$x^{35}+x^2+1$
1	-	-	-	-	-
2	-	-	+	+	+
3	-	-	+	+	+
4	-	-	+	+	+
5	-	+	+	+	+
6	-	+	+	+	+
7	+	+	+	+	+
8	+	+	+	+	+

З Табл.1. ми бачимо що зі збільшенням кількості каскадів, статистичні характеристики вихідної бітової послідовності покращуються, до прикладу при 6-и каскадах полінома x12+x6+x4+x1+1 – на рис. 2 ми бачимо його статистичний портрет, який не проходить тести NIST STS, проте при 7-и каскадах ми бачимо позитивний результат тестів (Рис. 3).

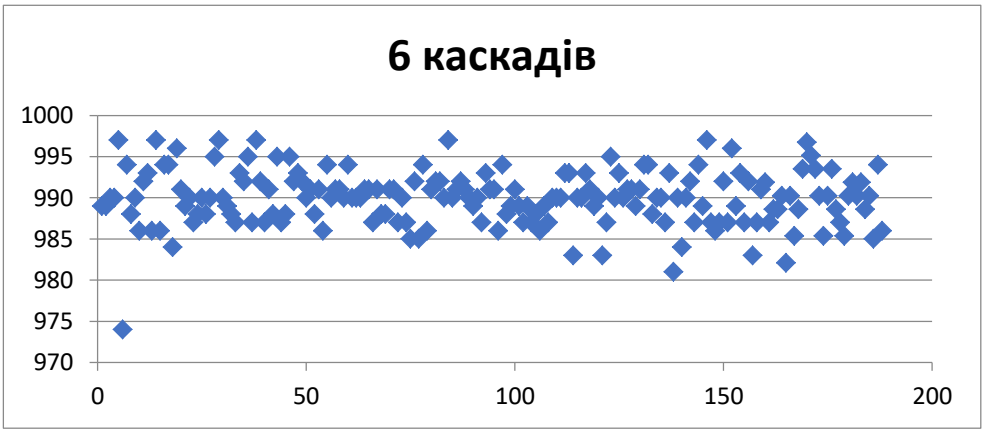

Рис. 2. Статистичний портрет ГПВБП на основі генератора Голлмана при 6-и каскадах і твірних поліномах - $x^{12}+x^6+x^4+x+1$

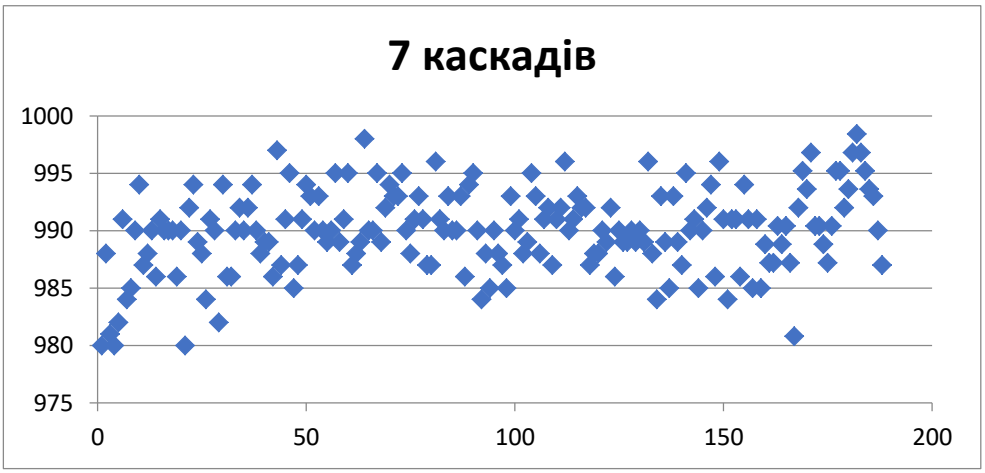

Рис. 3. Статистичний портрет ГПВБП на основі генератора Голлмана при 7-и каскадах і твірних поліномах - $x^{12}+x^6+x^4+x+1$

З Табл.1. також видно, що при збільшенні степенів поліномів в генераторі Голлмана статистичні характеристики покращуються (Рис. 4-5). А при використанні твірного полінома $x^{23}+x^5+1$, вистачає лише 2 каскади для позитивного проходження тестів NIST STS (Рис. 6).

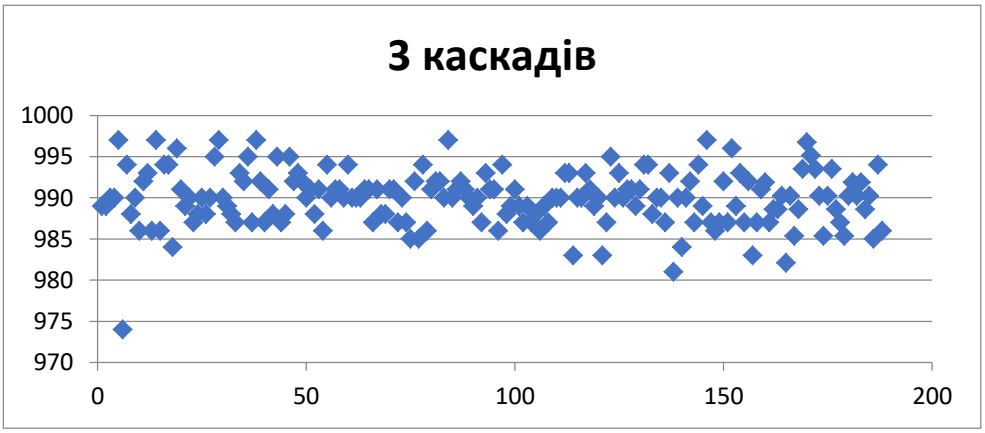

Рис. 4. Статистичний портрет ГПВБП на основі генератора Голлмана при 3-ох каскадах і твірному поліномах - $x^{16}+x^5+x^3+x^2+1$

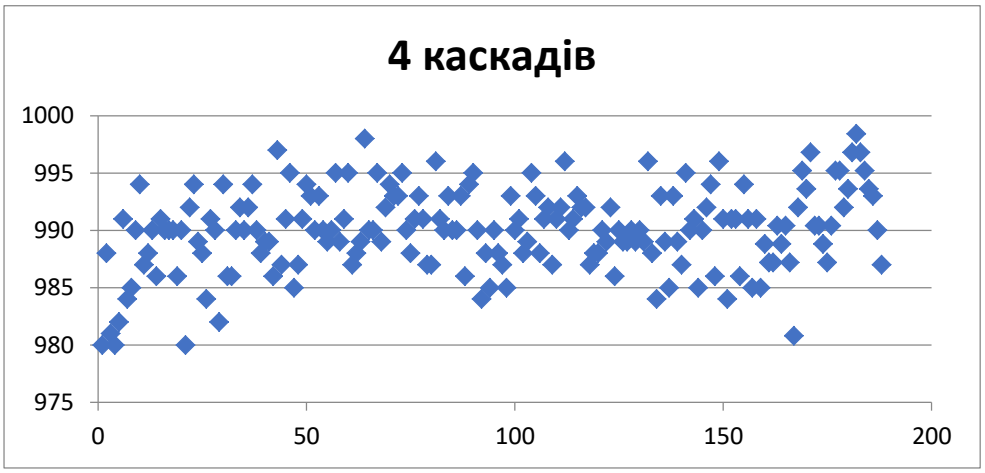

Рис. 5. Статистичний портрет ГПВБП на основі генератора Голлмана при 4-ох каскадах і твірному поліном - $x^{16}+x^5+x^3+x^2+1$

З Табл.1. також можна побачити, що при збільшенні степенів поліномів в генераторі Голлмана статистичні характеристики покращуються (Рис. 4-5).

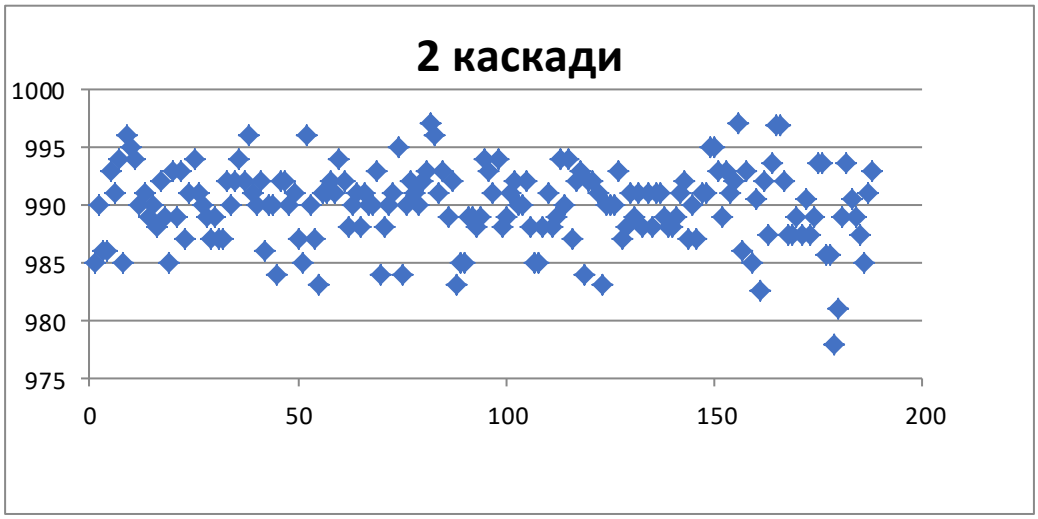

Рис. 6. Статистичний портрет ГПВБП на основі генератора Голлмана при 3-х каскадах і твірних поліномах - $x^{23}+x^5+1$

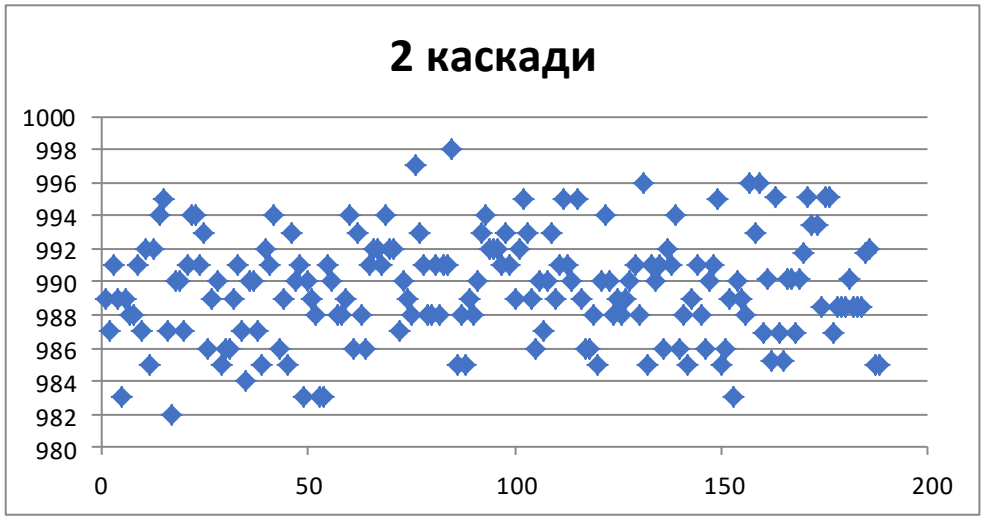

Рис. 7. Статистичний портрет ГПВБП на основі генератора Голлмана при 3-х каскадах і твірних поліномах - $x^{29}+x^2+1$

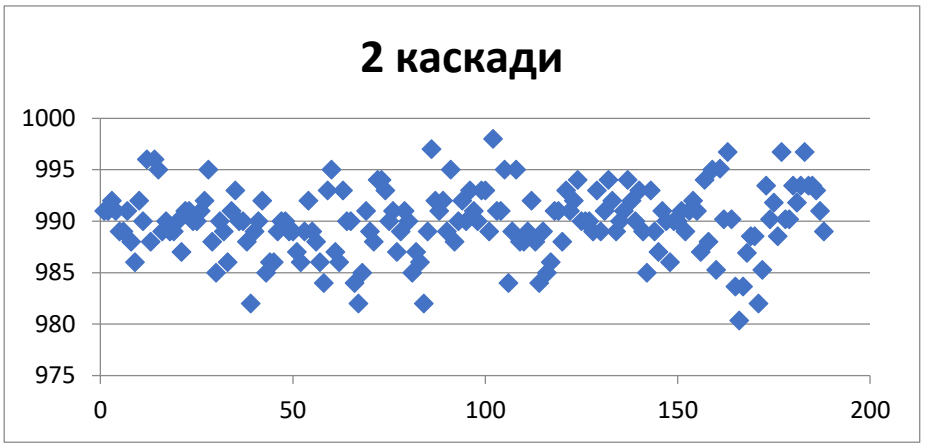

Рис. 8. Статистичний портрет ГПВБП на основі генератора Голлмана при 3-х каскадах і твірних поліномах - $x^{35}+x^2+1$

А при використанні твірного полінома $x^{23}+x^5+1$, вистачає лише 2 каскади для позитивного проходження тестів NIST STS (Рис. 6). Такі ж результати статистичних тестів показує і генератор псевдовипадкових бітових послідовностей Голлмана при більших степенях твірного полінома і кількості каскадів рівній двох (Рис.6, Рис.7, Рис.8).

Висновки. Збільшення кількості базових генераторів LFSR – послідовності і збільшення степенів їх поліномів приводить до підвищення якості генератора Голлманна. При цьому для зафіксованих значень цих кількостей генератор Голлманна проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики. Вибір конкретних параметрів генератора Голлманна повинен визначатись з заданими рівнями статистичними характеристика.

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. Мандрона М.Н. Исследование статистических характеристик модифицированных генераторов Фибоначчи / М.Н. Мандрона, В.Н. Максымовыч // Проблемы управления и информатики : межд. наук. - техн. журн. – 2014. - №6. – С. 28-36.
4. Mandrona M.M. Examination of multi link generators of pseudorandom sequences built using R-blocks / M.M. Mandrona, Yu.M. Kostiv, V.M. Maksymovych, O.I. Harasymchuk // Sustainable development : International journal. – Varna : Euro-Expert Ltd. – 2014. – № 18. – Pp. 110-118.
5. NIST SP 800-22. A Statistic Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application: [Електронний ресурс]. - April 2000. - Режим доступу: http://csrc.nist.gov./publications/niatpubs//SP800-22rev1a.pdf