УДК 621.317.083

Ю.М. Костів[1], В.М. Максимович[1], О.І. Гарасимчук[2], Я.Р. Совин[2], М.М. Мандрона[1]
Національний університет "Львівська політехніка",
[1]кафедра безпеки інформаційних технологій,
[2]кафедра захисту інформації

ВИЗНАЧЕННЯ ОПТИМАЛЬНИХ ПАРАМЕТРІВ ГЕНЕРАТОРА ГОЛЛМАННА ЗА ДОПОМОГОЮ СТАТИСТИЧНИХ ТЕСТІВ NIST

Наведено результати дослідження генератора Голлманна за різної кількості базових генераторів М-послідовностей і різних степенів їх поліномів, що проводилось з використанням статистичних тестів NIST. Отримані результати дають змогу оптимізувати параметри генератора за заданих параметрів вихідної імпульсної послідовності.

Ключові слова: генератори псевдовипадкових чисел, захист інформації, псевдовипадкові числа, статистичні характеристики.

The article presents the results of Gollmann generator estimation with a different number of basic LFSR 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 pulse sequence.

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

Вступ

Псевдовипадкова послідовність – це послідовність, що виглядає як випадкова, але насправді має скінченний період повторення.

Тому, проектуючи генератори псевдовипадкових послідовностей (ГПВП), необхідно зважати на найважливішу характеристику генератора – довжину періоду, після якого числа або почнуть знову повторюватися, або їх буде можливо передбачити. Добре згенерована псевдовипадкова послідовність практично не відрізняється від істинно випадкової.

Однією з переваг ГПВП є те, що на виходах таких генераторів отримуємо результати, які можна повторити нескінченну кількість разів, задавши однакові початкові умови та параметри, що досить зручно, особливо у процесі статистичного моделювання.

Зважаючи на швидкий розвиток засобів обчислювальної і вимірювальної техніки, а також із впровадженням новітніх технологій значно розширюється сфера застосування генераторів випадкових і псевдовипадкових послідовностей, а тому ставлять нові вимоги до їх проектування та методів оцінки якості.

У наш час генератори випадкових і псевдовипадкових імпульсних послідовностей широко використовуються:

- у системах захисту інформації – для шифрування, розшифрування та генерації ключів, генерування шуму, цифрових підписів, протоколів безпеки тощо;
- в імітаційному моделюванні – для фізичних, математичних, хімічних, економічних та медичних досліджень, а також у моделюванні військових дій;
- у вимірювальній техніці – як окремі функціональні блоки вимірювальних приладів або для їхнього тестування;
- як аналогові або цифрові джерела шуму;
- як коди для радіолокаційних систем, в яких відповідний сигнал взаємно корелюється з бітовою послідовністю, що передається;
- при розробці комп'ютерних ігор.

При проектуванні та реалізації ГПВП необхідно дотримуватись таких загальноприйнятих вимог:

- простота апаратної або програмної реалізації;
- максимальна швидкодія;
- максимальна наближеність послідовності, отриманої на виході генератора, до теоретичного закону розподілу (не обов'язково рівномірного);
- можливість керування вихідними параметрами;
- можливість роботи ГПВП у широкому діапазоні частот;
- можливість швидкого переналагодження його роботи залежно від вибору вихідних параметрів.

Якщо такий генератор буде використовуватися в системах захисту інформації (а такі генератори часто є важливою ланкою в забезпеченні інформаційної безпеки, зокрема в криптографії), то до нього ставиться ще ряд додаткових вимог, що будуть жорсткішими порівняно з вимогами до генераторів, що використовуються в інших галузях. Виконання таких вимог дає змогу передусім виявити генератори, що наперед задовольняють вимоги конкретної криптографічної задачі.

Найбільшою проблемою практично будь-якого ГПВП є те, що за визначених початкових умов вони дають передбачувані результати та кореляційні залежності. А це якраз те, чого очікують від псевдовипадкових послідовностей криптоаналітики, для здійснення ефективної атаки на криптосистему, де ці генератори застосовуються. Тому, якщо такий генератор застосовуватиметься, наприклад, у криптографічних додатках, то, по-перше, він повинен проходити статистичні тести на випадковість, а по-друге, має зберігати непередбачуваність, навіть якщо частина вихідного або поточного стану стане відомою криптоаналітикові.

Ще одна проблема полягає в тому, що не існує базису, на основі якого можна зробити висновок, що гамма конкретного генератора є непередбачуваною. Поки що в світі немає універсальних та перевірених на практиці критеріїв, які б дали змогу стверджувати це. Невідома також і загальна теорія криптоаналізу, що могла б бути застосована для такого доведення, за винятком все більшої кількості конкретних способів аналізу, вироблених для різних практичних цілей. Інтуїтивно випадковість сприймається як непередбачуваність, а для того щоб вважати гамму випадковою, як мінімум необхідно, щоб її період був дуже великим, а різноманітні комбінації бітів визначеної довжини розподілялися рівномірно по всій її довжині [1].

Нині вже розроблено велику кількість різноманітних методів та принципів генерування псевдовипадкових послідовностей, кожний з яких має переваги та недоліки [2–6] та ефективно застосовується для розв'язання різноманітних задач.

Під час вибору того чи іншого типу ГПВП, окрім виконання перелічених вище вимог до послідовностей на його виході, бажано поєднувати використання найпростіших методів генерування псевдовипадкових послідовностей та одночасного забезпечення заданих статистичних характеристик на виходах таких генераторів. Також бажано передбачити можливість реалізації ГПВП як апаратно, так і програмно.

Одним з найпростіших у реалізації та найпоширеніших є спосіб генерування псевдовипадкових послідовностей на основі регістрів зсуву. Такі генератори називають генераторами М-послідовностей (генератори псевдовипадкових чисел на лінійних послідовнісних машинах (ЛПМ), або генераторами на основі регістрів зсуву з лінійними зворотними зв'язками – LFSR (Linear Feedback Shift Register). Незважаючи на свою простоту та те, що на їх виході отримуються послідовності, здебільшого прогнозовані та передбачувані, такі генератори широко використовують в різних галузях науки та техніки.

Але безпосереднє використання генераторів М-послідовностей, зважаючи на згадані недоліки, переважно не завжди ефективне, оскільки послідовність на їх виході досить легко передбачити, що особливо непридатно для їх безпосереднього застосування під час розв'язання задач захисту інформації. Тому існує багато різноманітних методів побудови складніших ГППП, які ґрунтуються на використанні генераторів М-послідовностей.

Серед таких методів варто звернути увагу на генератор Голлманна, який реалізується на основі кількох генераторів М-послідовностей, що взаємопов'язані. Властивості такого генератора за

умови правильної реалізації кращі порівняно з генератором М-послідовностей. Генератори Голлманна широко використовуються у тих самих сферах, що описані вище для ГПВЧ, а також можуть прямо чи опосередковано застосовуватись для розв'язання задач захисту інформації. Практичним дослідженням генераторів Голлманна, на відміну від інших типів генераторів (зокрема й генераторів М-послідовностей, що входять до їх складу) присвячена порівняно невелика кількість праць, що в основному зводяться до опису принципів функціонування генераторів певного типу та рекомендацій щодо їх побудови.

Тому виникає завдання, що полягає у покращенні характеристик генератора Голлманна з метою отримання на його виході псевдовипадкових послідовностей, що прямо чи опосередковано можна було б застосовувати для розв'язання задач захисту інформації. Тому доцільно спробувати модифікувати базові генератори М-послідовностей та вибрати оптимальні їх параметри, які задовольняли б певні статистичні критерії.

Для того щоб робити висновок про можливість застосування певного ГПВП для розв'язання конкретних задач, потрібно виконати оцінювання його якості та надійності. Тестування генераторів псевдовипадкових послідовностей, особливо тих, що використовуються в криптографічних додатках, є актуальним як в практичному, так і в теоретичному плані. Незважаючи на значні напрацювання в цій сфері, розробники все-таки потребують зручного інструментарію, що здатний надати допустиму метрику, яка дозволить достатньо чітко дослідити ступінь випадковості послідовності на виході генератора, а також забезпечить розробників достатнім обсягом інформації для прийняття рішення відносно якості ГПВП.

У наш час існує та широко використовується достатньо велика кількість різних типів ГПВП, а набір та методику тестування кожного з них, як правило, пропонував сам розробник генератора [7]. Тому обставини складалися так, що було важко об'єктивно порівняти різні генератори на основі спільних критеріїв. Єдиним можливим виходом з такого становища є використання деякого стандартного набору статистичних тестів, що об'єднані певною спільною методикою розрахунку необхідних показників ефективності ГПВП та прийняття рішення про випадковість послідовності, що тестується. Тому науковці почали вести інтенсивну роботу в цьому напрямі, що привела до визначення двох основних груп критеріїв. Перша така група пов'язана з пошуком закономірностей, що дають змогу відновити шифровану послідовність за порівняно невеликою кількістю матеріалу. При цьому ставляться вимоги щодо відсутності в псевдовипадковій послідовності порівняно простих міжзнакових залежностей. Друга група критеріїв ґрунтується на оцінці статистичних властивостей послідовності, а саме чи є в досліджуваній послідовності який-небудь частотний дисбаланс, що дозволяє аналітику передбачити значення наступного біта із ймовірністю більше ніж 0.5. Також повинна забезпечуватися найбільша близькість властивостей псевдовипадкової послідовності до дійсно випадкової послідовності. Ці дві групи критеріїв – основа системного підходу до розроблення тестів, що призначені для оцінки якості псевдовипадкових послідовностей.

Сьогодні для тестування псевдовипадкових послідовностей розроблено кілька програмних продуктів, що містять комплекси тестів для перевірки різних статистичних властивостей, такі як тести Д. Кнута, DIEHART, CRYPT-S, FIPS, але найвідомішим серед них є набір статистичних тестів NIST [8,9].

Мета роботи

Проведення оцінювання генераторів Голлманна за допомогою пакета статистичних тестів NIST з метою визначення впливу параметрів їх структурних елементів на якість генератора.

Генератор Голлманна та результати його досліджень

Генератор Голлманна складається з кількох послідовно з'єднаних генераторів М-послідовностей (регістрів зсуву), тактування кожного з яких керується попереднім генератором (рис. 1). Вихід останнього генератора М-послідовностей є виходом генератора.

Якщо розрядність кожного генератора дорівнює N, тоді лінійна складність системи з m генераторів М-послідовностей дорівнює [3]

$$N(2^N - 1)^{m-1}. \quad (1)$$

Криптографи радять використовувати m ≥ 15, а при рівних значеннях mN віддавати перевагу варіанту з більшою кількістю коротких LFSR, а не варіанту з меншою кількістю довгих LFSR.

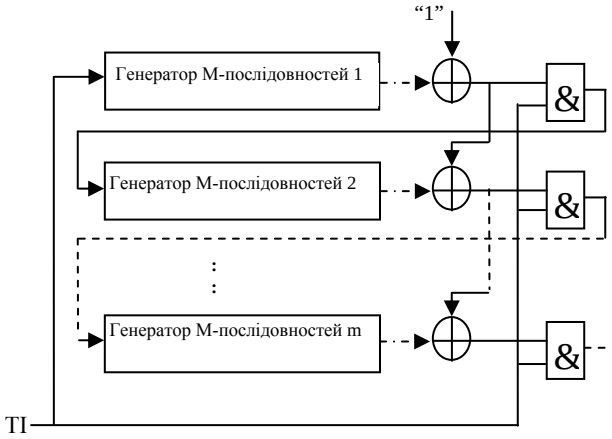

Рис. 1. Генератор Голлманна

Концептуально цей вид генераторів достатньо простий і може бути використаний для генерації псевдовипадкових послідовностей з величезними періодами, великими лінійними складностями та задовільними статистичними властивостями.

Такі генератори чутливі до розкриття, або так званого закривання (look-in), що являє собою метод, за допомогою якого спочатку криптоаналітик відновлює вхід останнього регістра зсуву в каскаді, а потім зламує весь каскад регістр за регістром. В деяких випадках це становить суттєву проблему та зменшує ефективну довжину ключа алгоритму, але для мінімізації можливості такого розкриття можна застосувати ряд визначених заходів.

Рівняння генератора М-послідовностей має вигляд [3]:

$$Q(t+1) = T^r Q(t), \tag{2}$$

де $Q(t)$ і $Q(t+1)$ – стани регістра ГППП відповідно в моменти часу t і $t+1$ (до і після приходу синхроімпульсу); T – квадратна матриця порядку N такого вигляду:

$$T_1 = \begin{vmatrix} a_1 & a_2 & \dots & a_{N-1} & a_N \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{vmatrix} \quad \text{або} \quad T_1 = \begin{vmatrix} 0 & \dots & 0 & 0 & a_N \\ 1 & \dots & 0 & 0 & a_{N-1} \\ & \dots & & & \\ 0 & \dots & 1 & 0 & a_2 \\ 0 & \dots & 0 & 1 & a_1 \end{vmatrix}, \tag{3}$$

N – степінь примітивного полінома

$$\Phi(x) = \sum_{i=0}^{N} a_i x^i, \quad a_N = a_0 = 1, \quad a_j \in \{0,1\}, \quad j = \overline{1,(N-1)}, \tag{4}$$

r – натуральне число.

Детальні принципи реалізації генераторів М-послідовностей в цій роботі не наведено, оскільки вони відомі й детально описані у великій кількості літератури. Доведено [5], що кращі статистичні характеристики мають ті генератори М-послідовностей, які модифіковані (зі складнішою реалізацією). Для дослідження та оцінки якості генераторів Голлманна ми вирішили змінювати розрядність базових генераторів М-послідовностей, а також змінювати кількість таких генераторів. Оцінювання якості генератора виконаємо за допомогою пакета статистичних тестів NIST. Результати такого оцінювання генератора Голлманна поки що в літературі відсутні. Для цього ми розробили імітаційну модель такого генератора мовою Delphi, яка дає змогу одержувати вихідні послідовності залежно від зміни згаданих вище параметрів.

Статистичні тести NIST – пакет статистичних тестів, який розробила в 1999 р. лабораторія інформаційних технологій (Information Technology Laboratory), що є головною організацією Національного інституту стандартів і технологій США (NIST) [10]. Фахівці NIST запропонували методику проведення статистичного тестування генераторів псевдовипадкових чисел, що орієнтовані на застосування в системах захисту інформації – зокрема в криптографії. Тому цей пакет використовуються для визначення якісних та кількісних ознак випадковості послідовності чисел, що необхідно для криптографів та криптоаналітиків.

Пакет NIST STS містить 15 статистичних тестів, які розроблені для перевірки гіпотези про випадковість двійкових послідовностей довільної довжини, що генеруються ГПВП. Кожен з цих тестів спрямований на виявлення різноманітних дефектів випадковості.

Результати кожного статистичного тесту повинні тлумачитись з певною обережністю і застереженням, щоб уникнути неправильних висновків про досліджуваний генератор.

Базовим принципом тестування за допомогою статистичних тестів NIST є перевірка певної нульової гіпотези H_0 про те, що послідовність, яка перевіряється, випадкова. З цією нульовою гіпотезою пов'язана альтернативна гіпотеза H_a про те, що послідовність – не випадкова. За результатами кожного тесту отримують висновок про прийняття або відхилення нульової гіпотези, ґрунтуючись на сформованій досліджуваним генератором послідовності. Кінцеве рішення про те, чи досліджувана послідовність є випадковою, чи ні, приймають за результатами сукупності усіх тестів [8].

Порядок тестування окремої двійкової послідовності S згідно з тестами NIST має такий вигляд [9]:

1. Висувається нульова гіпотеза H_0, тобто припущення про те, що ця двійкова послідовність S є випадковою.
2. За послідовністю S обчислюється статистика тесту c(S).
3. З використанням спеціальних функцій та статистики тесту обчислюється значення ймовірності $P = f(c(S))$, $P \in [0, 1]$.
4. Значення ймовірності P порівнюється з рівнем значущості $\alpha, \alpha \in [0.001, 0.01]$. Якщо $P \geq \alpha$, то гіпотеза H_0 приймається, в іншому випадку приймається альтернативна гіпотеза.

Набір NIST складається з 15 статистичних тестів. Залежно від вхідних параметрів обчислюється 188 значень ймовірності P, які можна розглядати як результат роботи окремих тестів [10].

Отже, у результаті тестування двійкової послідовності формується вектор значень ймовірностей $P=\{P_1,P_2 \ldots P_{188}\}$. Аналіз складових P_i цього вектора дає змогу вказати на конкретні дефекти випадковості послідовності, що тестується.

За допомогою імітаційної моделі генератора ми змогли дослідити параметри різної кількості базових генераторів від двох до тридцяти.

Тест вважається пройденим, якщо імовірність проходження тесту P потрапить у межі від 0,98 до 1,00. Якщо ж імовірність P буде нижчою за 0,98, вважається, що тест не пройдено. За отриманими результатами статистичного тестування 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. Отже, статистичний портрет генератора – матриця розміром 1000×188, елементами якої є 188000 значень відповідних імовірностей.

Результати статистичних досліджень генераторів Голлмана подано на рис. 2–8. На осі абсцис відкладено номер тесту NIST STS, на осі ординат – імовірність проходження тесту.

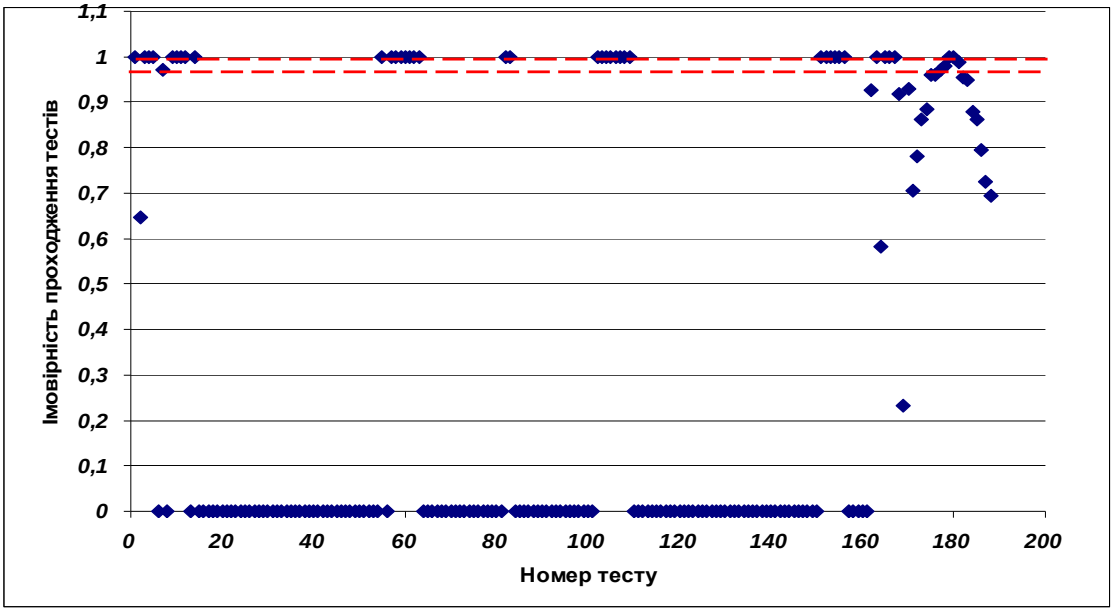

Рис. 2. Статистичний портрет генератора Голлманна з двома генераторами М-послідовності на основі твірного полінома $1 \oplus x^6 \oplus x^7$

Із статистичного портрета генератора видно, що більшість тестів містяться на смузі 0. А у виділений діапазон потрапляє лише декілька ітерацій тесту. З метою визначення оптимальних способів побудови генератора Голлманна змінювалась кількість базових генераторів М-послідовностей (рис. 3–5).

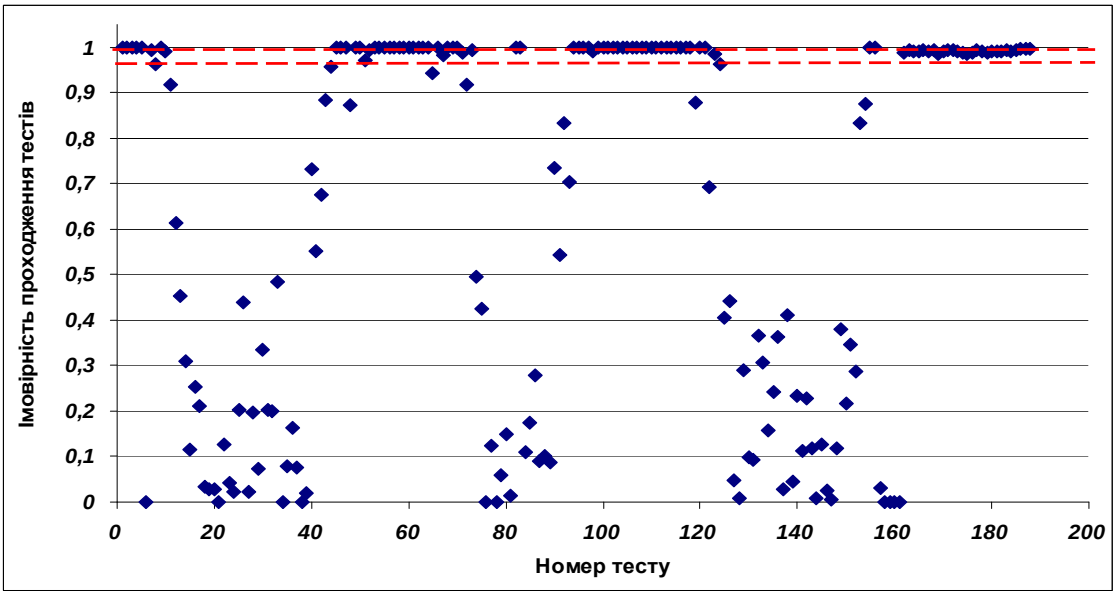

Рис. 3. Статистичний портрет генератора Голлманна з трьома генераторами М-послідовності на основі твірного полінома $1 \oplus x^6 \oplus x^7$

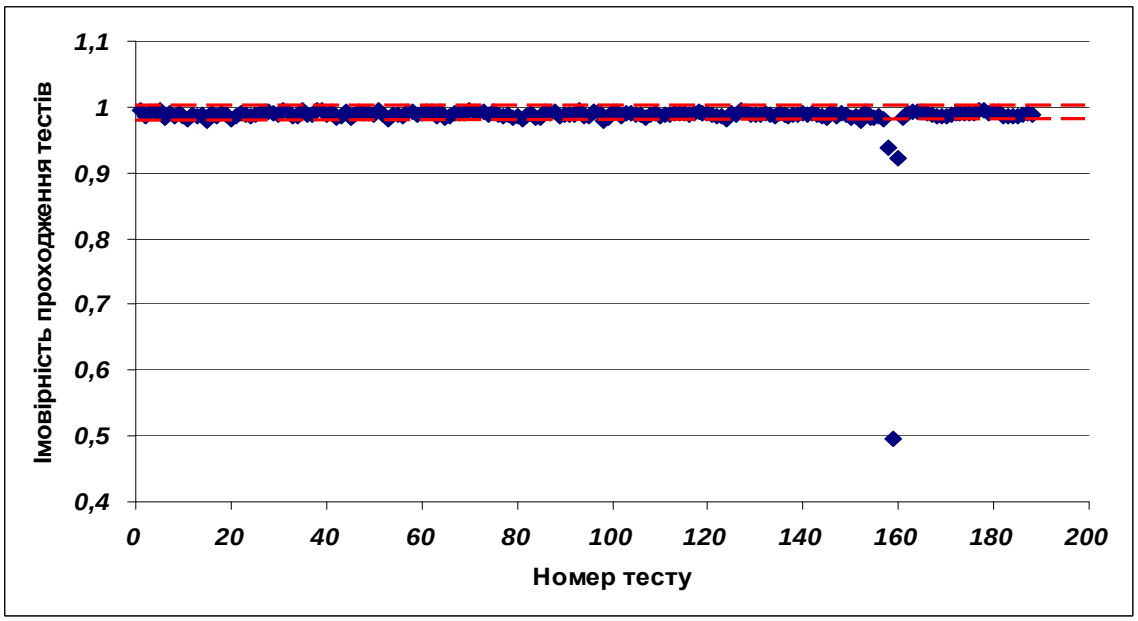

Рис. 4. Статистичний портрет генератора Голлманна з п'ятьма генераторами М-послідовності на основі твірного полінома $1 \oplus x^6 \oplus x^7$

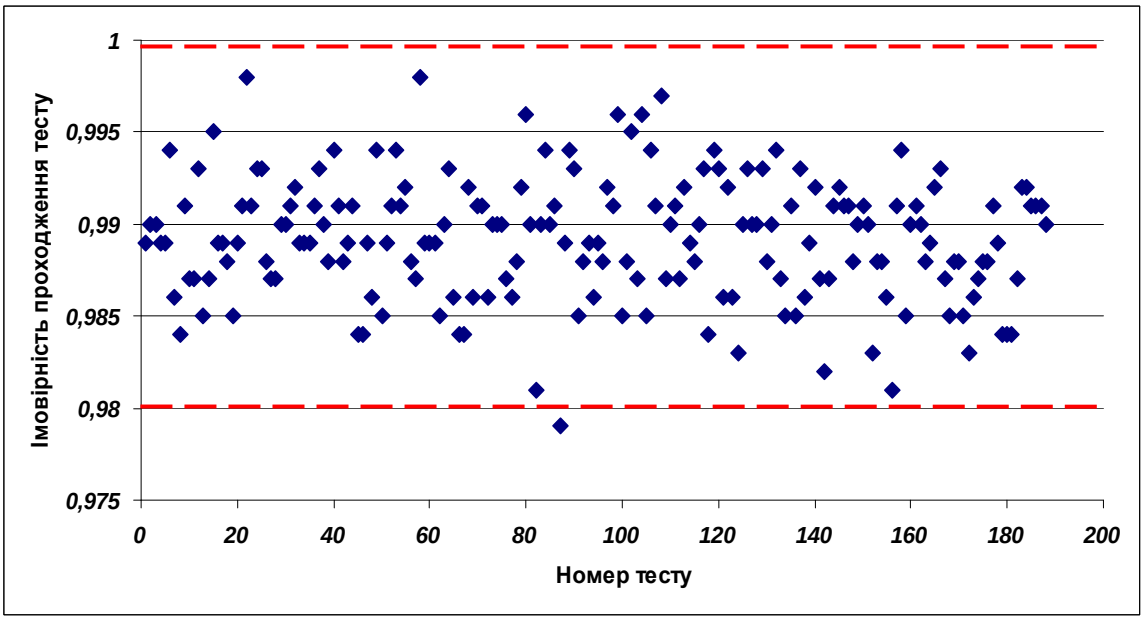

Рис. 5. Статистичний портрет генератора Голлманна з сімома генераторами М-послідовності на основі твірного полінома $1 \oplus x^6 \oplus x^7$

Як видно з наведених рисунків, зі збільшенням кількості базових генераторів М-послідовностей якість генератора Голлманна покращується, оскільки кількість непройдених тестів зменшується.

Детальний звіт з оцінювання за допомогою пакета статистичних тестів NIST вищезгаданих генераторів Голлманна, реалізованих на основі полінома 7-го степеня, наведено в табл. 1.

Таблиця 1

Результати тестування генератора Голлманна на основі твірного полінома $1 \oplus x^6 \oplus x^7$

№	Статистичний тест	Кількість базових генераторів М - послідовності								
		2	*3*	*5*	*6*	*7*	*8*	*10*	*15*	*20*
1	Монобітний (частотний) тест	-	-	+	+	+	+	+	+	+
2	Частотний блоковий тест	-	-	+	+	+	+	+	+	+
3	Тест накопичених сум	-	-	+	+	+	+	+	+	+
4	Тест перевірки серій	-	-	+	+	+	+	+	+	+
5	Найдовшої серії одиниць	-	-	-	+	+	+	+	+	+
6	Перевірки рангу двійкових матриць	-	-	+	+	+	+	+	+	+
7	Тест на основі дискретного пертворення Фур'є	-	-	+	+	+	+	+	+	+
8	Тест на відповідність шаблону без перекриття	-	-	+	+	+	+	+	+	+
9	Тест на відповідність шаблону з перекриттям	-	-	+	+	+	+	+	+	+
10	Універсальний тест Мауера	-	-	-	+	+	+	+	+	+
11	Тест на основі апроксимації ентропії	-	-	-	-	+	+	+	+	+
12	Тест серій	-	-	-	+	+	+	+	+	+
13	Тест лінійної складності	-	+	+	+	+	+	+	+	+
14	Тест випадкових блокувань	-	+	+	+	+	+	+	+	+
15	Тест випадкових блокувань 2	-	+	+	+	+	+	+	+	+

Аналогічні дослідження проводились над генераторами Голлманна, реалізованими на основі поліномів інших степенів. Зокрема, для поліномів 17-го степеня отримані оцінки наведено на рис. 6–8.

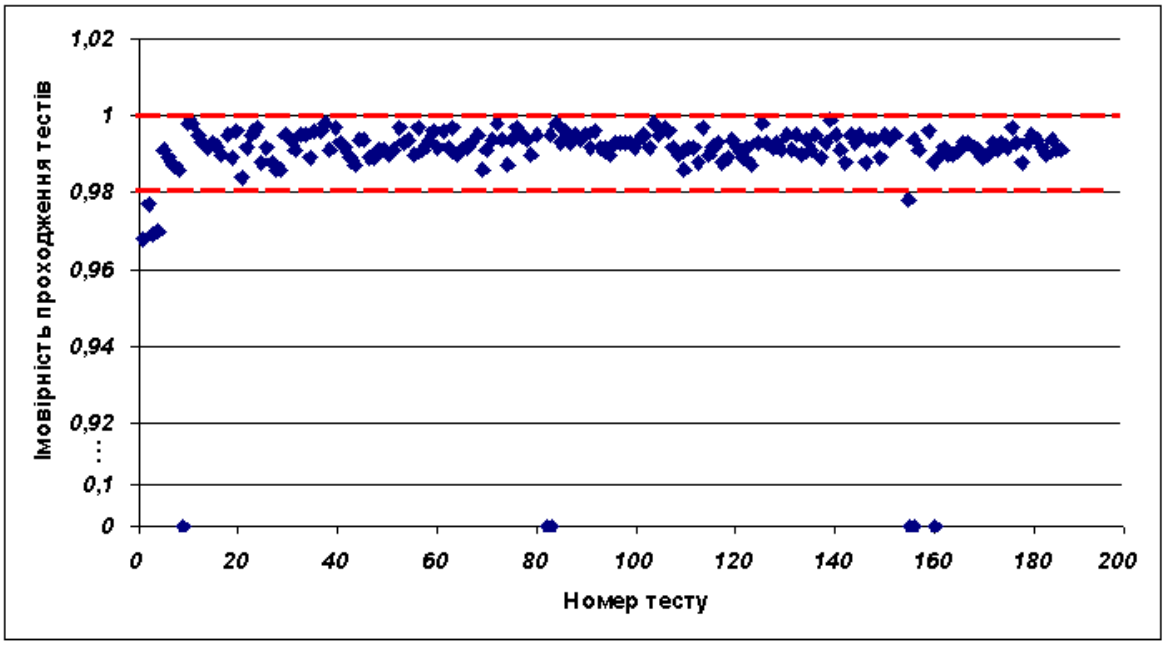

Рис. 6. Статистичний портрет генератора Голлманна з двома генераторами М-послідовності на основі твірного полінома $1 \oplus x^{12} \oplus x^{17}$

З наведеного графіка видно, що цей генератор не пройшов лише 7 тестів, що порівняно з аналогічним генератором Голлманна, реалізованим на твірному поліномі $1 \oplus x^6 \oplus x^7$, є значно кращим результатом.

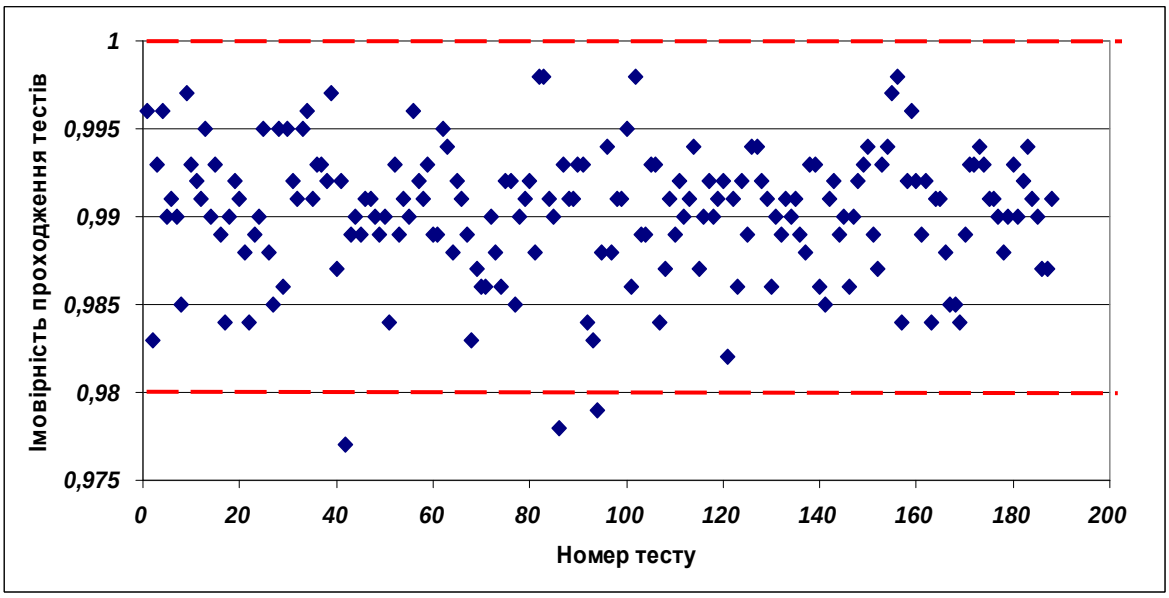

Рис. 7. Статистичний портрет генератора Голлманна з трьома генераторами М-послідовності на основі твірного полінома $1 \oplus x^{12} \oplus x^{17}$

Як видно з рис. 7, отримані результати значно кращі від попередніх, тільки три значення менші за 0,98, отже, збільшення кількості генераторів М-послідовності істотно впливає на криптостійкість генератора. Це підтверджує наступний крок – вибір 5 генераторів.

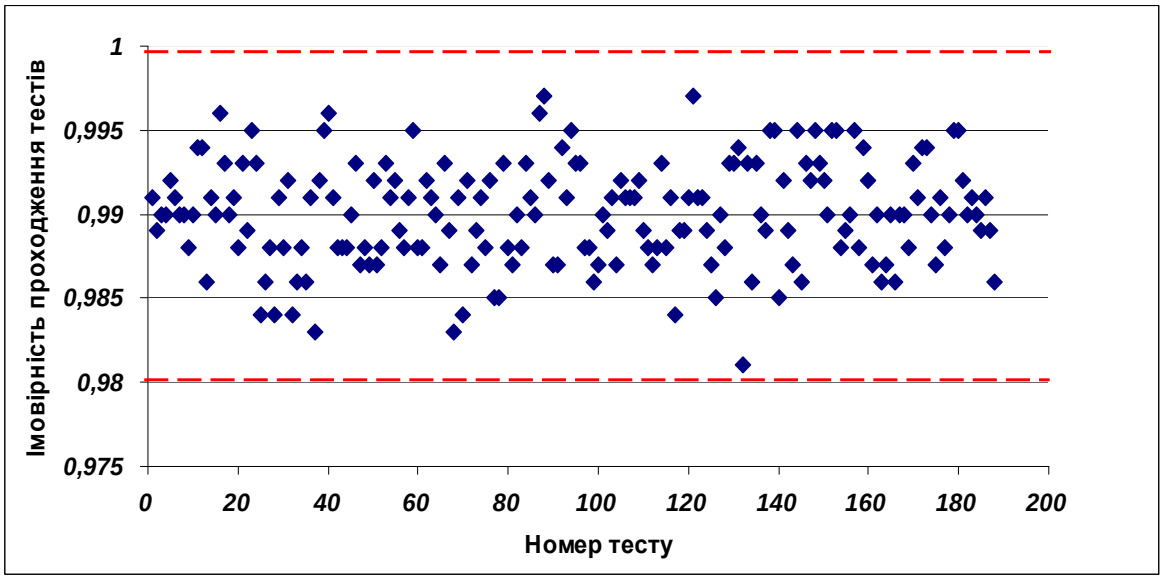

Рис. 8. Статистичний портрет генератора Голлманна з п'ятьма генераторами М-послідовності на основі твірного полінома $1 \oplus x^{12} \oplus x^{17}$

Як бачимо з рис. 8, досліджений генератор проходить усі тести NIST STS. Результати тестів вищі від межі 0,98, що згідно з вимогами статистичного оцінювання за допомогою пакета NIST свідчить про достатню криптографічну стійкість.

Детальний звіт з оцінювання за допомогою пакета статистичних тестів NIST вищезгаданих генераторів Голлманна, реалізованих на основі полінома 17-го степеня, наведено в табл. 2.

Таблиця 2

Результати тестування генератора Голлманна на основі твірного полінома $1 \oplus x^{12} \oplus x^{17}$

№	Статистичний тест	Кількість базових генераторів М - послідовності				
		2	*3*	*4*	*5*	*10*
1	Монобітний (частотний) тест	-	+	+	+	+
2	Частотний блоковий тест	-	+	+	+	+
3	Тест накопичених сум	-	+	+	+	+
4	Тест перевірки серій	-	+	+	+	+
5	Найдовшої серії одиниць	+	+	+	+	+
6	Перевірки рангу двійкових матриць	+	+	+	+	+
7	Тест на основі дискретного перетворення Фур'є	+	+	+	+	+
8	Тест на відповідність шаблону без перекриття	-	-	+	+	+
9	Тест на відповідність шаблону з перекриттям	-	+	+	+	+
10	Універсальний тест Мауера	+	+	+	+	+
11	Тест на основі апроксимації ентропії	+	+	+	+	+
12	Тест серій	-	+	+	+	+
13	Тест лінійної складності	+	+	+	+	+
14	Тест випадкових блокувань	+	+	+	+	+
15	Тест випадкових блокувань 2	+	+	+	+	+

На рис. 9 графічно показано середнє значення імовірності проходження тестів NIST STS досліджуваних генераторів Голлманна з різною кількістю базових генераторів М-послідовності й твірними поліномами $1 \oplus x^6 \oplus x^7$ та $1 \oplus x^{12} \oplus x^{17}$.

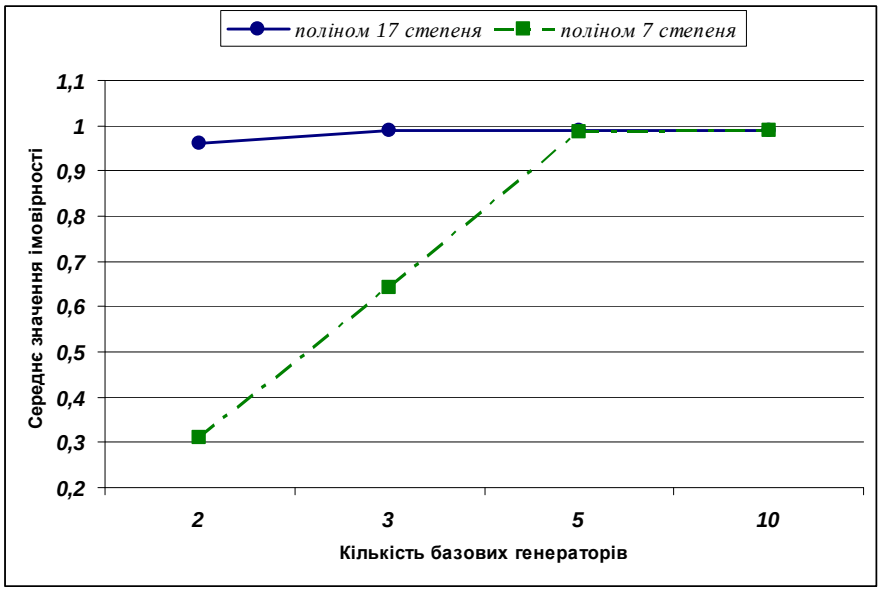

Рис. 9. Порівняння середнього значення імовірності проходження тестів NIST різними генераторами Голлманна

Висновки

Збільшення кількості базових генераторів М–послідовності і збільшення степенів їх поліномів поліпшує якість генератора Голлманна. При цьому для зафіксованих значень цих кількостей генератор Голлманна проходить усі тести NIST, що свідчить про його задовільні статистичні характеристики і криптостійкість.

Конкретні параметри генератора Голлманна необхідно вибирати із заданими рівнями криптостійкості й статистичними характеристиками, заданою швидкодією і оптимальним об'ємом обладнання, що може бути предметом подальших досліджень.

1. Жельников В. Криптография от папируса до комп'ютера / В. Жельников – М.: ABF, 1996. – 254 с. 2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ – ОБРАЗ, 2001. – 368 с. 3. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / Иванов М.А., Чугунков И.В. – М.: КУДИЦ – ОБРАЗ, 2003. – 240 с. 4. Гарасимчук О.І. Генератори псевдовипадкових чисел, їх застосування, класифікація, основні методи побудови і оцінка якості / О.І. Гарасимчук, В.М. Максимович // Захист інформації. – Київ – 2002 – 7 с. 5. Гарасимчук О. І. Генератори пуассонівського імпульсного потоку на основі генераторів М-послідовностей / О.І. Гарасимчук, В.М. Максимович // Вісник Нац. ун-ту "Львівська політехніка". "Комп'ютерні науки та інформаційні технології", – 2004. – № 521 – С. 17–23. 6. Rock A. Pseudorandom Number Generators for Criptographic Applications / A. Rock. – Salzbuburg, 2005. – P. 57–65. 7. Вильданов Р.Р. Тесты псевдослучайных последовательностей и реализующее их программное средство / Вильданов Р.Р., Мещеряков Р.В., Бондарчук С.С. // Доклады Томского государственного университета систем управления и радиоэлектроники – № 1 (25). – Часть 2. – 2012. – 108 с. 8. 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. 9. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Форт, 2012. – 880 с. 10. Статистические тесты NIST [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/Статистические_тесты_NIST