technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. 9. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model. 10. Якименко І. З. Критерії оцінки рівня захисту комп'ютерних мереж з врахуванням їх архітектури // Інформатика та математичні методи в моделюванні, 2013. – Т. 3 – №1 – С. 82–90. 11. Защита сетевого периметра: наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений [Текст] / С. Норткатт [и др.]; науч. ред. Н. И. Алишов. – К.; М.; СПб.: DiaSoft, 2004. – 664 с. 12. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 445 с. 13. ISO/IEC 15408-2:1999 – Information technology – Security techniques – Code of practice for information security management.

УДК 621.319.5+004.3

Ю. М. Костів[1], В. М. Максимович[1], О. І. Гарасимчук[2], М. М. Мандрона[1,3]
Національний університет "Львівська політехніка",
[1]кафедра безпеки інформаційних технологій,
[2]кафедра захисту інформації;
Львівський державний університет безпеки життєдіяльності,
[3]кафедра управління інформаційною безпекою

ФОРМУВАННЯ ПУАССОНІВСЬКОЇ ІМПУЛЬСНОЇ ПОСЛІДОВНОСТІ НА ОСНОВІ ГЕНЕРАТОРА ГОЛЛМАННА

Показано можливість формування пуассонівської імпульсної послідовності на основі псевдовипадкової бітової послідовності. Для формування останньої використано генератор Голлманна. Якість бітової послідовності досліджували за допомогою статистичних тестів NIST. Для оцінки якості пуассонівської послідовності використано методику, що ґрунтується на критерії Пірсона.

Ключові слова: псевдовипадкові імпульсні послідовності, генератори псевдовипадкових чисел, статистичні характеристики, критерій Пірсона.

FORMING OF POISSON PULSE SEQUENCE BASED ON GOLLMAN GENERATOR

The possibility of forming Poisson pulse sequence on the base of pseudorandom bit sequence is shown. Gollman generator is used for forming the last of these sequences. Estimation of bit sequence quality was conducted with the help of NIST statistic tests. For estimation of Poisson sequence quality the methodology that based on Pearson criterion is used.

Key words: pseudorandom pulse sequences, pseudorandom number generators, statistic characteristics, Pearson criterion.

Вступ

Широке застосування розподілу Пуассона зумовлене тим, що він описує виникнення рідкісних подій з незмінною, або такою, що змінюється порівняно повільно, середньою частотою. Тому серед усього різноманіття генераторів випадкових та псевдовипадкових чисел або послідовностей важливе місце займають генератори пуассонівських імпульсних послідовностей (ГПІП).

ГППП можуть реалізовуватися як апаратними, так і програмними засобами залежно від мети їх застосування і забезпечення необхідних параметрів. Тому потрібно шукати оптимальні методи побудови ГППП, які б мали задовільні статистичні характеристики, високу швидкодію, можливість оперативної зміни середньої частоти вихідних імпульсів та простоту реалізації.

Якість ГППП, тобто відповідність статистичного розподілу в часі вихідних імпульсів пуассонівському закону, залежить від вибору базового генератора псевдовипадкової бітової послідовності (ГПБП) [1, 2]. ГППП ефективно можуть бути побудовані на основі регістрів зсуву з лінійними зворотними зв'язками (РЗЛЗЗ).

Серед ГПБП варто звернути увагу на генератор Голлманна, який реалізується на базі кількох генераторів на основі взаємопов'язаних РЗЛЗЗ. Властивості такого генератора за правильної реалізації кращі порівняно зі звичайним генератором на основі РЗЛЗЗ. Генератори Голлманна широко використовуються у різних сферах, а також можуть прямо чи опосередковано застосовуватись для виконання завдань захисту інформації.

Основний зміст

Досліджено можливості формування імпульсної послідовності з пуассонівським законом розподілу, – пуассонівської імпульсної послідовності (ППП), на основі псевдовипадкової бітової послідовності (ПБП).

Оскільки для ППП характерні низькі значення середньої частоти повторення імпульсів, а ПБП характеризуються однаковою середньою частотою наявності та відсутності імпульсів у тактові моменти часу (однаковою частотою формування 1 і 0), формування ППП на основі ПБП можна реалізувати відповідно до структури на рис. 1, до складу якої входять ГПБП і керований дільник частоти (КДЧ).

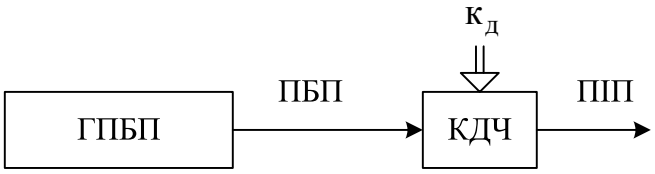


Рис. 1. Структурна схема формування ППП

Статистичні характеристики ППП повинні відповідати певним критеріям, для визначення яких можна скористатись розробленою нами методикою [3], що дає змогу проводити дослідження у всьому діапазоні середніх значень частот ППП. Якість ПБП можна визначити за допомогою статистичних тестів NIST [4].

До складу набору NIST входять 15 статистичних тестів, але під час тестування обчислюють 188 значень імовірності P, які можна розглядати як результат роботи окремих тестів.

На підставі результатів тестування приймають або відхиляють гіпотезу про те, що ця 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. Значення α вибирають в інтервалі [0.001, 0.01].

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

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

За результатами обчислень визначено межі довірчого інтервалу; якщо результат виконання тесту потрапляє у межі 0,999439–0,0980561, то робимо висновок, що тест успішно пройдено, якщо не потрапляє – не пройдено. На статистичних портретах досліджуваних генераторів (рис. 2, 3) довірчий інтервал позначено широкими пунктирними лініями.

Тестування проведено за рівня значущості α = 0,01, який рекомендували розробники NIST. У цьому випадку статистичний портрет генератора має вигляд матриці розміром 1000×188, елементами якої є 188000 значень відповідних імовірностей.

У цій роботі для побудови ГПБП вибрано генератор Голлманна, статистичні характеристики різних варіантів побудови якого досліджено в роботі [5]. Знайдено варіанти, що забезпечують високу якість ПБП, тобто такі, що проходять усі тести NIST.

На рис. 2 зображено статистичний портрет генератора Голлманна, побудований на трьох однакових РЗЛЗЗ, кожен з яких відповідає поліному $\Phi(x) = 1 + 6x + 7x$, матриці T1 і степеню матриці r=1. По осі абсцис відкладено номер тесту NIST, по осі ординат – імовірність проходження тесту.

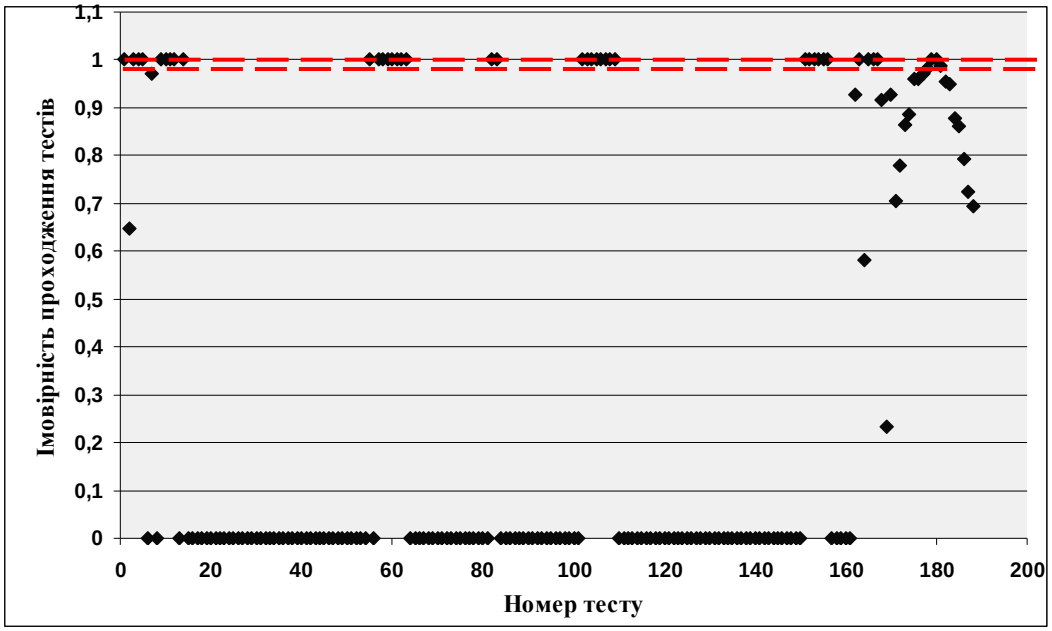


Рис. 2. Статистичний портрет генератора Голлманна на основі твірних поліномів 7-го степеня

З рис. 2 видно, що генератор з твірними поліномами 7-го степеня має погані статистичні характеристики. Практично всі результати тестування – за межами довірчого інтервалу. Це означає, що в послідовності є близько розташовані одна до одної повторювані ділянки, що, своєю чергою, демонструє відхилення від випадкового характеру досліджуваної послідовності.

Спробуємо покращити якість генератора Голлманна, змінюючи значення степеня полінома, та проводити подальше оцінювання за допомогою пакета тестів NIST.

На рис. 3 зображено статистичний портрет генератора Голлманна, побудований на трьох однакових РЗЛЗЗ, кожен з яких відповідає поліному $\Phi(x) = 1 + 18x + 25x$, матриці T1 і степеню матриці r=1. По осі абсцис відкладено номер тесту NIST, по осі ординат – імовірність проходження тесту.

Генератор Голлманна на основі твірних поліномів 25-го степеня проходить усі тести NIST (рис. 3), що свідчить про його задовільні статистичні характеристики.

Як видно з наведених рисунків, зі збільшенням степеня твірного полінома якість генератора Голлманна покращується, оскільки кількість непройдених тестів зменшується.

На рис. 4 наведено результати оцінки якості ПІП, у разі побудови КДЧ на базі лічильника імпульсів з модулем лічби $к_д$, тобто схеми, на вихід якої надходить кожен $к_д$ імпульс її вхідної послідовності.

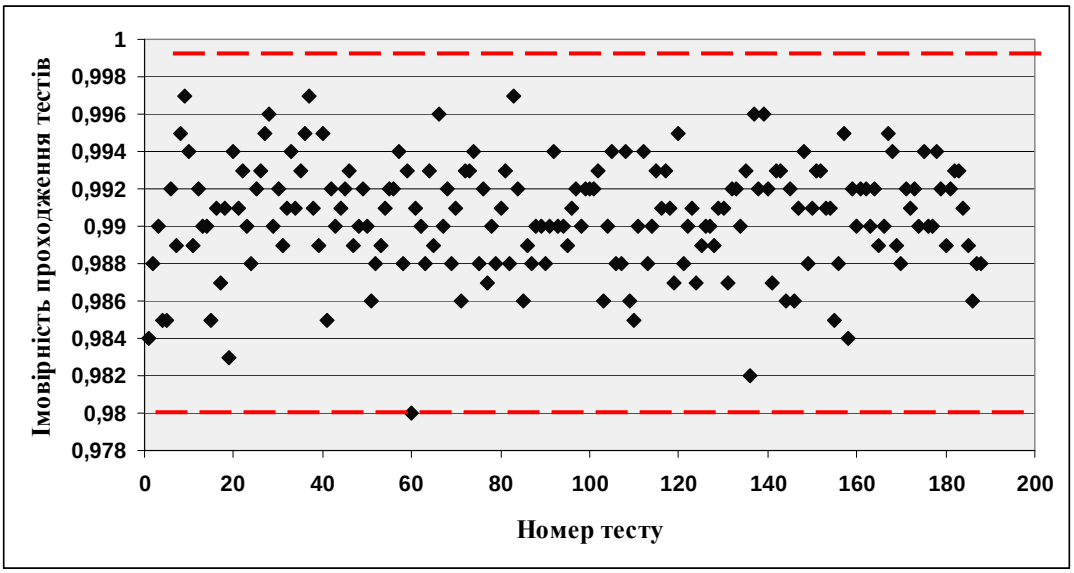
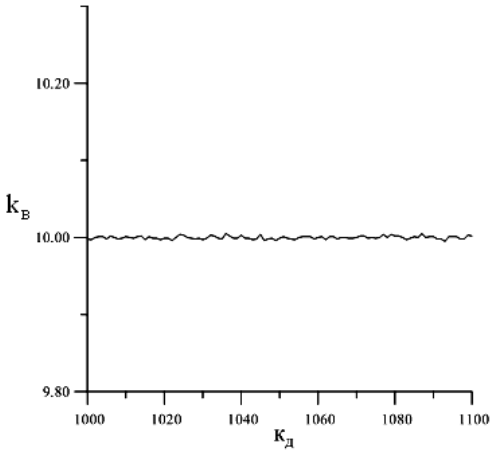
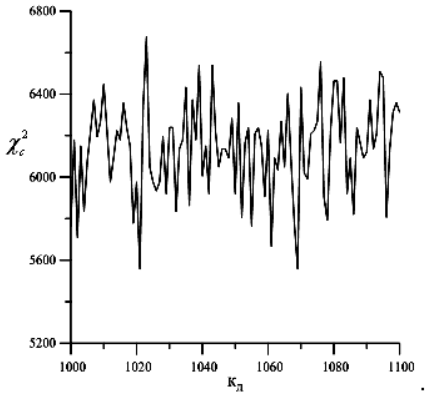


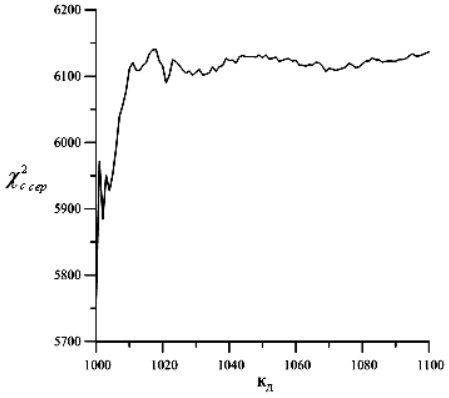
Рис. 3. Статистичний портрет генератора Голлманна на основі твірних поліномів 25-го степеня



а



б



в

Рис. 4. Результати дослідження ПІП, сформованої за допомогою генератора Голлманна і КДЧ на базі лічильника імпульсів

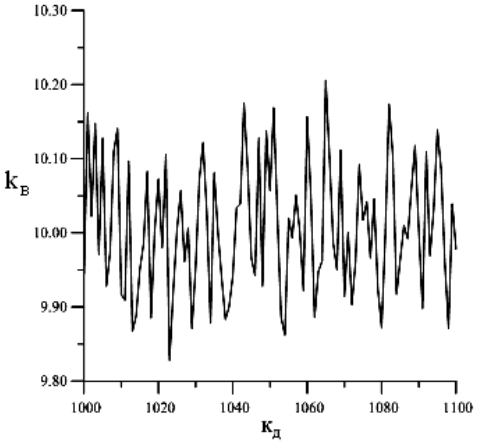
Дослідження проведено за методикою, описаною в роботі [3], з тією відмінністю, що значення $i_{\max}$ визначено за формулою

$$i_{max} = 2 \cdot \kappa_д \cdot k_c . \quad (1)$$

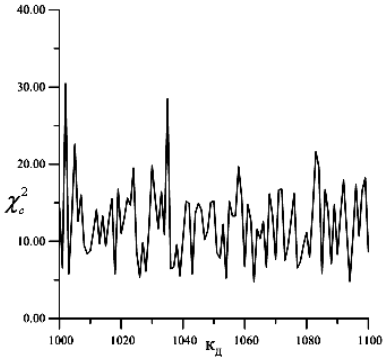
При цьому прийнято такі значення: $n_{max} = 1000$, $k_c = 10$.

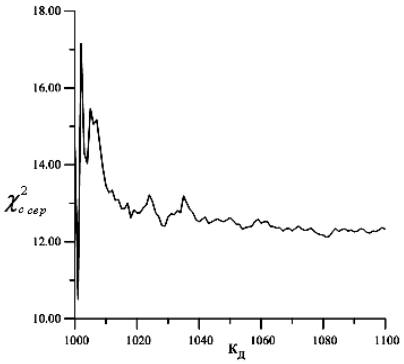
Генератор Голлманна побудовано на трьох однакових регістрах зсуву з лінійними зворотними зв'язками (РЗЛЗЗ), кожен з яких відповідає поліному $Ф(x) = 1 + 18x + 25x$, матриці Т1 і степеню матриці r=1. На рис. 1 подано: *а* – залежність середнього значення кількості ПІП – $k_в$, що відповідають i_{max}, від коефіцієнта ділення $k_д$; *б* – залежність критерію Пірсона χ_c^2 від $k_д$; *в* – залежність поточного значення $\chi_c^2 - \chi^2_{ссер}$ від $k_д$.

Відповідно до запропонованої методики оцінки якості ПІП [3], що ґрунтується на критерії Пірсона, статистичні характеристики послідовності є задовільними, якщо виконується умова $\chi_c^2 < \chi^2_{кр}$. Для вибраних рівня значущості $\alpha = 0{,}05$ і степеня свободи $r = 13$ маємо $\chi^2_{кр} = 22{,}4$. Отже, статистичні характеристики досліджуваної імпульсної послідовності не відповідають пуассонівському закону розподілу. Це можна пояснити тим, що використання КДЧ на основі лічильника імпульсів не дає змоги виконати одну з умов, що визначають пуассонівську послідовність: імовірність формування імпульсів у будь-який момент часу не повинна залежати від передісторії – наявності чи відсутності імпульсів у попередні моменти часу.



а





б *в*

Рис. 5. Результати дослідження ПІП, сформованої за допомогою генератора Голлманна і КДЧ за алгоритмом (2): а – залежність середнього значення $k_в$ від коефіцієнта ділення $К_Д$; б – залежність $\chi^2_с$ від $К_Д$; в – залежність поточного значення $\chi^2_{сер}$ від $К_Д$

На рис. 5 наведено результати оцінки якості ПІП у разі реалізації алгоритму роботи КДЧ за алгоритмом (2):

```
if x_ПБП :=1 then
begin
    x:= random (К_Д);                                    (2)
    if x=1 then x_ПІП := 1 else x_ПІП := 0;
end;
```

де $x_{ПБП}$ і $x_{ПІП}$ – наявність імпульсів на виходах ГПБП і КДЧ, а x – псевдовипадкове число.

У цьому випадку, оскільки умова $\chi_c^2 < \chi_{кр}^2$ виконується практично для усіх значень $К_Д$, імпульсна послідовність на виході КДЧ відповідає пуассонівському закону розподілу.

Висновок

Доведено можливість формування пуассонівської імпульсної послідовності із задовільними статичними характеристиками на основі псевдовипадкової бітової послідовності, зокрема, у разі формування останньої за допомогою генератора Голлманна.

Показано, що генератор Голлманна, за відповідного вибору початкових умов, може використовуватись як структурний елемент у схемі генерування псевдовипадкової послідовності з пуассонівським законом розподілу. Щоб оцінити можливість такого застосування, достатньо використати систему статистичного тестування NIST для оцінки якості ГПБП та запропоновану нами методику оцінювання якості ПІП.

1. Гарасимчук О. І., Максимович В. М., Алгоритм формування пуассонівського імпульсного потоку // Вісник Національного університету "Львівська політехніка" "Автоматика, вимірювання та керування". – 2003. – № 475. – С. 21–25. 2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях: учебное пособие / М. А. Иванов, И. В. Чугунков. – М.: Изд-во НИЯУ МИФИ, 2012. – 400 с. 3. Kostiv Yu. M. Methodology for research of Poisson pulse sequence generators using Pearson's Chi-squared test / Yu. M. Kostiv, V. M. Maksymovych, O. I. Harasymchuk, M. M. Mandrona // Sustainable development: International journal. – Varna: Euro-Expert Ltd. – 2013. – № 9. – P. 67–72. 4. Костів Ю. Використання статистичних тестів NIST STS для дослідження генераторів М-послідовностей / Костів Ю., Максимович В., Мандрона М., Рибак Ю. // матер. 1-ї Міжнар. наук.-техн. конф. "Захист інформації і безпека інформаційних систем", 31 травня – 01 червня 2012 р. – Львів, 2012. – С. 118–119. 5. Костів Ю. М. Оцінка якості генератора Голлманна, реалізованого на основі модифікованих генераторів М – послідовностей / Гарасимчук О. І., Костів Ю. М., Паршенко Т. Г. // Системи обробки інформації. Вісник Харківського університету повітряних сил ім. Івана Кожедуба. – Харків. – 2010. – № 6 (87). – С.35–38.