УДК 681.325

**М.М. СОЛОЩУК, Н.В. ОЛІЙНИК**

***Національний технічний університет "Харківський політехнічний інститут", Україна***

# ТЕХНІЧНІ РЕЗУЛЬТАТИ ПРИ ВИКОРИСТАННІ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У статті проаналізовані технічні результати роботи генераторів псевдовипадкових послідовностей, які були отриманні в результаті проведення патентних досліджень, знайдена залежність між результатами, які були одержані, і заявниками охоронних документів на генератори псевдовипадкових послідовностей. Зроблено висновки щодо актуальності отриманого результату по обраному об'єкту дослідження.

**псевдовипадкові послідовності, генератори двійкових послідовностей, технічний результат генераторів псевдовипадкових послідовностей**

## Вступ

Як зазначалося у [1], під час проведення патентних досліджень щодо генераторів псевдовипадкових послідовностей був створений звіт про патентні дослідження, який дозволяє не тільки систематизувати релевантні матеріали за різними аспектами, а й робити попередні висновки про актуальність, значущість та можливість використання генераторів псевдовипадкових послідовностей у різних галузях, наприклад, таких як космічний зв'язок, коди, що виявляють і виправляють помилки, захист інформації та інших.

**Формулювання мети роботи.** Якісні псевдовипадкові послідовності мають практично всі властивості дійсно випадкових процесів і успішно їх замінюють, так як випадкові послідовності формувати надзвичайно важко. Саме тому актуальність проблеми створення якісних генераторів псевдовипадкових послідовностей на сьогоднішній день не викликає сумнівів.

Однак, як показують проведені дослідження, існуючі генератори псевдовипадкових послідовностей відрізняються один від одного не тільки конструктивними рішеннями, новими елементами, їх з'єднаннями, галузями застосування, але також і досягнутими технічними результатами.

## Класифікація технічних результатів

Проведені патентні дослідження дозволили авторам класифікувати знайдені охоронні документи щодо генераторів псевдовипадкових послідовностей за технічними результатами.

На рис. 1 наведено загальні технічні результати, які частіше всього досягаються при застосуванні генераторів псевдовипадкових послідовностей.


Рис. 1. Загальні технічні результати генераторів псевдовипадкових послідовностей
(* інші результати не враховані)

**Забезпечення оптимальних характеристик випадкових чисел.** Добре відомо [2], що якісний генератор псевдовипадкових послідовностей, який призначений для використання в системах захисту інформації, повинен мати оптимальні статистичні властивості, а саме, псевдовипадкова послідовність не повинна відрізнятися від дійсно випадкової послідовності. Проведений аналіз відібраних патентів за технічними результатами, що досягаються при використанні знайдених винаходів, показав, що найбільше число генераторів застосовуються для забезпечення саме оптимальних характеристик випадкових чисел (39,5%).


Рис. 2. Забезпечення оптимальних характеристик випадкових чисел

Як видно з рис. 2, забезпечення оптимальних характеристик випадкових чисел досягається багатьма шляхами, однак найрозповсюдженими з них є підвищення надійності і якості статистичних параметрів формованої послідовності випадкових чисел [3], генерування псевдовипадкових послідовностей з бажаною імовірністю та поліпшення коефіцієнта перешкодостійкості [4].

**Підвищення швидкості формування випадкових чисел.** Другим за кількістю знайдених результатів є підвищення швидкості формування випадкових чисел – 23,7% від загальної кількості технічних результатів, що досягаються. Нерідко наслідком підвищення швидкості формування випадкових чисел є поширення області застосування [5].

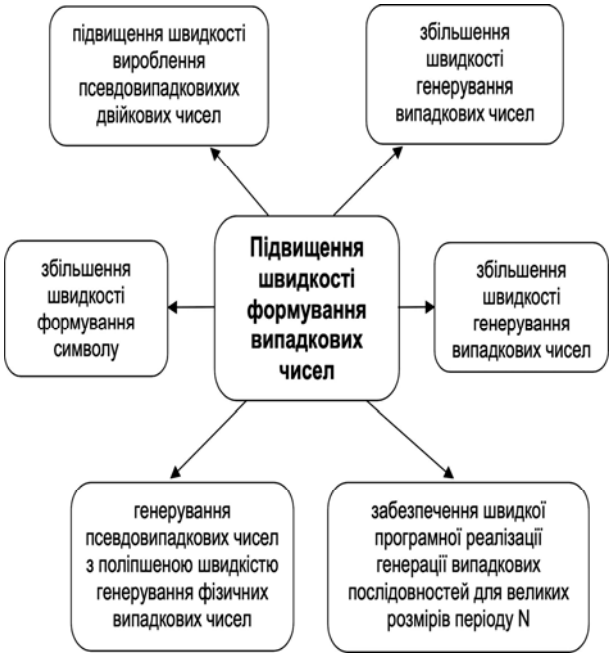


Рис. 3. Підвищення швидкості формування випадкових чисел

**Одночасне формування кількох послідовностей**. Одним з важливіших результатів роботи генераторів псевдовипадкових послідовностей є одночасне формування кількох послідовностей випадкових чисел. Кількість охоронних документів з такими технічними результатами становить близько 10,5% відібраних охоронних документів. Генератори псевдовипадкових послідовностей з одночасним формуванням кількох послідовностей, як правило, відносяться до галузі генерації випадкових чисел в обчислювальній техніці, техніці зв'язку і можуть бути використані для захисту інформації обчислювальних систем, для статистичного аналізу випадкових процесів і полів. Однак результати досліджень показали, що існуючі генератори псевдовипадкових послідовностей, які призначені для одночасного

формування кількох послідовностей випадкових чисел, мають недоліки, наприклад, одночасно формують тільки дві послідовності [6] або кількість різних числових послідовностей одного періоду, що генеруються генератором, зумовлена обмеженою кількістю початкових станів [7]. Таким чином, є необхідність в розробці нового генератора псевдовипадкових послідовностей, який би забезпечив одночасне формування кількох послідовностей одного періоду, що генеруються.

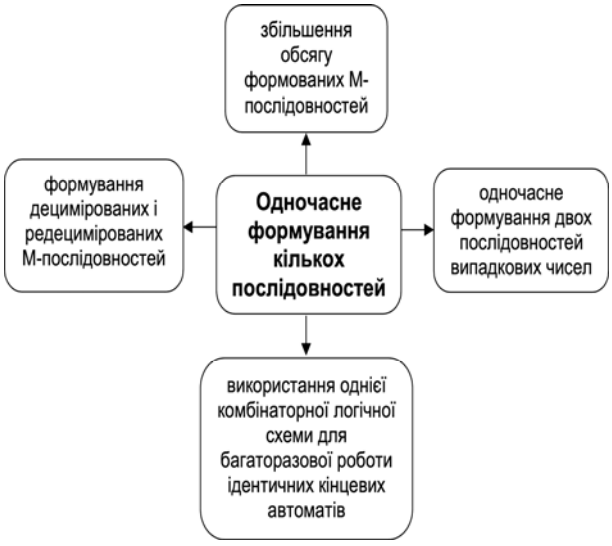


Рис. 4. Одночасне формування кількох послідовностей

**Спрощення конструкції генератора.** Проведений аналіз показав, що спрощенням конструкції генератора займаються в понад 10,5% всіх розробок (рис. 5).

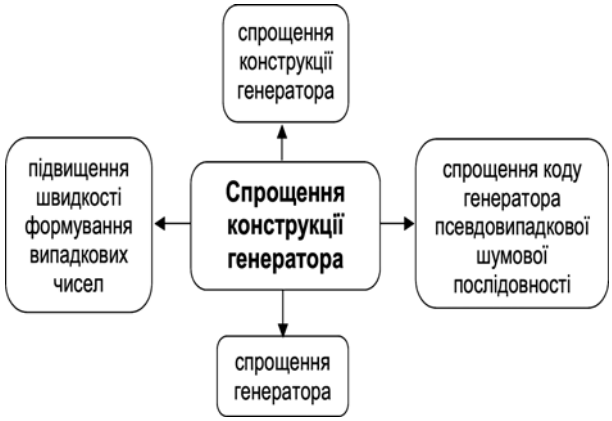


Рис. 5. Спрощення конструкції генератора

Як показують дослідження, по 2,6% від загальної кількості технічних результатів, що досягаються при використанні генераторів псевдовипадкових послідовностей, займають забезпечення високої надійності генерації випадкових рівно імовірних чисел та розробка способу і пристрою для генерації чисел випадкових чисел, менш дорогого, ніж попередні методи.

## Залежність між технічними результатами винаходів та їх заявниками

За результатами проведеного аналізу виявлена залежність між технічними результатами винаходів та їх заявниками, а саме:

1. Забезпеченням оптимальних характеристик випадкових чисел в основному займаються:

– значні закордонні фірми, такі як NIPPON ELECTRIC (JP), JAPAN TECH RES & DEV INST; MITSUBISHI ELECTRIC CORP (JP);

– російські вищі навчальні заклади, такі як "Военный университет связи" (RU), "Военная академия Ракетных войск стратегического назначения им. Петра Великого" (RU) та російське "Федеральное государственное унитарное предприятие "Концерн "Системпром" (RU).

2. Підвищенням швидкості формування випадкових чисел займаються:

– Харківський державний університет радіоелектроніки (UA);

– Севастопольський військово-морський інститут ім. Нахімова (UA);

– TOKYO SHIBAURA ELECTRIC CO (JP).

3. Одночасним формуванням кількох послідовностей випадкових чисел займаються:

– "Государственное унитарное предприятие Воронежский научно-исследовательский институт связи" (RU), Предприятие КБ "Луч" (RU) та ADVANCED MICRO DEVICES INC (US).

4. Над спрощенням конструкції генератора працювали:

– "Иркутский политехнический інститут" (SU);

– "Московский інженерно-физический інститут" (SU);

– "Казанский Авиационный Институт им. Туполева" (SU);

– MATSUSHITA ELECTRIC IND CO (JP).

## Висновки

Таким чином, проведений аналіз охоронних документів щодо генераторів псевдовипадкових послідовностей за технічними результатами знайдених під час проведення патентних досліджень дозволив авторам статті класифікувати отримані результати роботи існуючих генераторів псевдовипадкових послідовностей та зробити висновки про актуальність та значущість розробки генераторів псевдовипадкових послідовностей з одночасним формуванням кількох послідовностей випадкових чисел, якими займаються автори даної статті.

## Література

1. Солощук М.М., Олійник Н.В. Патентні дослідження щодо генераторів псевдовипадкових послідовностей // Вестник Национального технического университета "Харьковский политехнический институт": Сборник научных трудов. Тематический выпуск: Автоматика и приборостроение. – Х.: НТУ "ХПИ". – 2003.

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

3. Пат. № 2191421 RU, МПК8 G06F7/58. Генератор последовательности случайных чисел. – № 2001122038; Подано 08.08.2001; Опубл. 20.10.2002.

4. Пат. № 2295215 JP, МПК G01S7/282. Генератор последовательности сигналов с максимальным периодом. – № 19890116442; Подано 10.05.1989; Опубл. 06.12.1999.

5. Пат. № 36108 UA, МПК8 G06F7/58. Спосіб генерації випадкових чисел та пристрій для його здійснення. – № 99116006; Подано 02.11.1999; Опубл. 16.04.2001.

6. Пат. № 2081451 RU, МПК6 G06F7/58. Генератор последовательностей случайных чисел. – № 94017087/09; Подано 10.05.1994; Опубл. 10.06.1997.

7. Пат. № 1283950 SU, МПК4 H03K3/84. Генератор псевдослучайных двоичных последовательностей. – № 3932828; Подано 23.07.1985; Опубл. 15.01.1987.

*Надійшла до редакції 28.08.2006*

**Рецензент:** д-р техн. наук, проф. Г.В. Пєвцов, Національний технічний університет "Харківський політехнічний інститут", Харків.