Механізм генерації "звукового вітру" – при прийнятті блоком AEaS рішення про доцільність урухомлення режиму стабілізаційної обробки – подається збуджувальний сигнал на силовий п'єзоелемент – пластину припасовану до денця комірки TRP. Тривалість ЕО задається після тестування конкретної RT (тобто RT з конкретним складом, підібраним так, щоб температура його плавлення відповідала робочому інтервалу контрольованого процесу).

Після проведення ЕО рекомендованих параметрів – проводиться повторний контроль процесу ФП – при реєстрації АЕ-сигналів (рис. 5) належних параметрів (відповідаючим кристалізації максимально дрібнозернистої та гомогенної структури RT) – видається дозвіл/рекомендація щодо можливості проведення тестування термометрів.

Запропонована система дає змогу контролювати відтворюваність температури топлення евтектичного репера в межах ±0.05K.

1. Прохоренко С., Стадник Б., Войтурський Я. Попередні результати апробації температурного репера на базі In-Ga-Sn евтектики // Вимірювальна техніка та метрологія . – 2003. – 63. – 32 с. 2. Prokhorenko S.V., Mudry S.I. Metal Melts at the Clusters and Fractals Representation // Acta Metalurgika Slovaca. – 2001. – 7. – P. 422–426. 3. Прохоренко С., Стадник Б., Бояр З. Контроль гравітаційної седиментації робочого елементу температурного репера з використанням методики акустичної емісії // Вимірювальна техніка та метрологія. – 2002. – № 59. – С. 76–80. 4. Prokhorenko S., Stadnyk B., Bylica A. Determination of structural and thermal-physics requirements of stabilization of an equilibrium crystallization of a eutectic alloys // Archives of Foundry. – 2002. – Vol. 2. – N 6. – P. 189–194. 5. Прохоренко С., Стадник Б.. Гомогенізація евтектичного розтопу температурного репера шляхом віброобробки // Вимірювальна техніка та метрологія. – 2002. – № 61. – С. 44–46. 6. Prokhorenko V., Bylica A., Mudry S., Prokhorenko S. Effect of magnetic field and cooling speed on crystallization processes of Sn-Bi alloys // Acta Metalurgika Slovaca. – 2001. – 7.– P. 412–415.

УДК 681.3

В.М. Сокіл
Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин

ГЕНЕРАТОР ВИПАДКОВИХ ЧИСЕЛ

Запропоновано новий варіант реалізації апаратного генератора випадкових чисел. Розглянуто структуру пристрою та описано основні принципи його функціонування.

New solution proposes for the hardware random number generator's implementation. The structure of system is considered and the principles of its functionality are described.

Вступ. Сьогодні в світі спостерігається помітна зміна пріоритетів при виборі шляхів здійснення комерційної діяльності. Зараз електронною поштою передають не тільки якісь нотатки чи тексти, але й комерційні контракти та іншу важливу фінансову інформацію. WEB використовується для розповсюдження програмного забезпечення та здійснення електронного бізнесу. Віртуальні захищені мережі (Virtual Private Network – VPN) розширюють корпоративні мережі за рахунок відкритих каналів мережі Internet. Захищена електронна пошта, доступ по WEB, VPN вимагають так званої "сильної" криптографії (strong security) [1]. Така криптографія забезпечує конфіденційність, аутентифікацію, контроль доступу, цілісність інформації та повну звітність. Основними складовими "сильної" криптографії є цифрові сертифікати та криптографія з відкритими ключами. Багато великих компаній вже розгорнули та успішно експлуатують корпоративні системи безпеки, основою яких є інфраструктура відкритих ключів та цифрові сертифікати. Такі системи використовують такі механізми:

- криптографічне закриття інформації для забезпечення секретності
- цифрові підписи для забезпечення звітності та цілісності інформації
- цифрові сертифікати для аутентифікації користувачів, програм та сервісів, а також для забезпечення контролю доступу (авторизація)

Алгоритми та протоколи цих підсистем широко використовують випадкові числа [2]. Прикладами таких алгоритмів та протоколів можуть бути:

- протоколи генерування та розподілу сеансових ключів симетричних криптосистем,
- протоколи генерування ключів для асиметричних криптосистем,
- різноманітні схеми аутентифікації як взаємної, так і односторонньої

У цих випадках послідовність чисел, що використовується, обов'язково повинна бути непередбачуваною та випадковою. Випадкова бітова послідовність може розглядатися як результат підкидання симетричної монети, сторони якої позначені відповідно як "0" та "1". Результатом кожного підкидання з однаковою ймовірністю може бути як "0", так і "1" Окрім того, кожне підкидання повністю незалежно від попередніх, його результат ніяк не впливає на наступні результати. Отже, підкидання симетричної монети – це ідеальний генератор випадкової бітової послідовності, значення "0" і "1" з'являються випадково та рівномірно. Всі елементи послідовності генеруються незалежно один від одного, значення наступного елемента послідовності неможливо визначити, знаючи кількість згенерованих до цього елементів.

Очевидно, використовувати монету в криптографії як генератор випадкових чисел не дуже зручно. Однак гіпотетична бітова послідовність такого ідеалізованого генератора випадкових чисел використовується як еталонна при оцінці інших генераторів випадкових і псевдовипадкових чисел.

При побудові підсистем аутентифікації та генерування сеансових ключів неможливість передбачити елементи послідовності набагато важливіша, ніж статистична випадковість послідовності чисел.

Криптографічні системи в основному використовують алгоритмічні методи генерування випадкових чисел. Вхідні дані алгоритмів, що використовуються для генерування, називають ініціалізуючими значеннями. Відповідні алгоритми є детермінованими, а тому генерують послідовність чисел, які не є статистично незалежними. Такі генератори називають генераторами псевдовипадкових чисел. Для забезпечення неможливості передбачити елементи послідовності потрібно дуже обережно вибирати ініціалізуючі значення. Якщо відомі алгоритм генерації та ініціалізуючі значення, то елементи псевдовипадкової послідовності стають цілком передбачувані. Оскільки в багатьох випадках алгоритм генерації широко відомий, то ініціалізуюче значення повинно зберігатися в секреті. Крім того, саме ініціалізуюче значення повинно бути непередбачуваним.

В "істинно" випадковій послідовності кожне число статистично незалежне одне від одного, таким чином його неможливо передбачити. Генератори "істинно" випадкових послідовностей під час генерації використовують недетерміновані джерела в поєднанні з деякою функцією обробки. Функція обробки використовується для запобігання генерації невипадкових чисел (наприклад, появи довгих рядків одиниць або нулів). Недетерміноване джерело – це, як правило, якась фізична величина, наприклад шум в електронній схемі, часова схема роботи користувача (час між натисканнями клавіш на клавіатурі або рухами мишки), квантовий ефект у напівпровідниках, імпульсні детектори іонізуючого випромінювання. Причому можуть використовуватися різні комбінації таких джерел. Вихідні значення генератора можуть безпосередньо використовуватися як випадкові числа або подаватися на генератор псевдовипадкових чисел. Для безпосереднього використання (без наступної обробки) згенерована послідовність повинна перевірятися на випадковість за допомогою статистичних тестів. Наприклад, таке фізичне джерело, як шум в електронній схемі може містити періодичну складову, що хоч і з'являється випадково, але по статистичних тестах не є такою.

“Білий шум” як недетерміноване джерело випадкових чисел. При розробці апаратного генератора випадкових чисел як недетерміноване джерело був обраний найдоступніший варіант – шум в електронній схемі. У будь-якій електронній схемі є кілька некорельованих джерел шуму. Загальний шум таких джерел – це їх геометрична сума [3]:

$$U_R = \sqrt{\overline{U_1^2} + \overline{U_2^2} + \overline{U_3^2} + \dots}\,. \tag{1}$$

Перше джерело шуму – це тепловий шум опору, відомий також як шум Джонсона (на честь фізика Джона Бертрана Джонсона John Bertrand Johnson, що відкрив це явище у 1928 році). На відміну від дробового шуму, що виникає від проходження носіїв заряду через потенційний бар’єр, шум Джонсона виникає при хаотичному тепловому русі носіїв заряду в провіднику. Щільність шумової напруги опору не залежить від частоти (умова білого шуму) і дорівнює

$$e_r^2(f) = 4 \cdot k \cdot T \cdot R, \tag{2}$$

де T – температура довкілля в Кельвінах; k = 1.28 x 10-23 J/K – константа Больцмана; R – значення опору (Ω).

Друге джерело – це шум операційного підсилювача. Він складається із трьох частин [4]: шумова напруга, що диференційно прикладена до двох входів, і два шумові струми, по одному на кожному із входів. Шумову модель операційного підсилювача з резистивним зворотним зв’язком показано на рис. 1

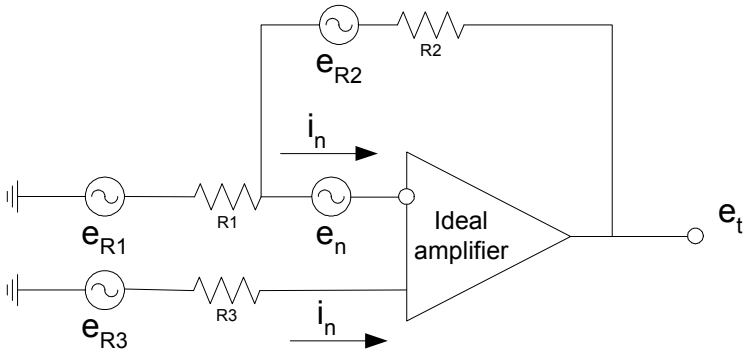

Рис. 1. Шумова модель операційного підсилювача

Отже, вираз для визначення загального шуму на вході операційного підсилювача з резистивним зворотним зв’язком має такий вигляд:

$$\begin{aligned} U_{Tin} &= \sqrt{e_t^2 \cdot BW} = \\ &= \sqrt{\begin{aligned} &e_n^2 + 4kTR_3 + 4kTR_1\left[R_2/(R_1+R_2)\right]^2 + \\ &+i_n^2 R_3^2 + i_n^2\left[R_1R_2/(R_1+R_2)\right]^2 + \\ &+4kTR_2\left[R_1/(R_1+R_2)\right]^2 \end{aligned}} \cdot\sqrt{BW} \end{aligned} \tag{3}$$

де R_1 – опір послідовного резистора інвертуючого входу; R_2 – опір резистора зворотного зв’язку; R_3 – опір послідовного резистора неінвертуючого входу; e_n – густина вхідної шумової напруги; i_n – густина вхідного шумового струму; BW – смуга пропускання шуму;

$$BW = 1.57 f_{CL}, \tag{4}$$

де f_{CL} – смуга пропускання частот замкнутого операційного підсилювача.

Загальний шум на виході операційного підсилювача дорівнює:

$$U_{Tout} = U_{Tin} \cdot NG, \tag{5}$$

де NG – коефіцієнт підсилення шуму.

Для резистивного зворотного зв'язка підсилювача коефіцієнт підсилення шуму не залежить від частоти й може бути обчислений відповідно до табл. 1.

Таблиця 1

Коефіцієнт підсилення шуму

Джерело шуму у вигляді шумової напруги	Значення NG
Шум Джонсона на резисторі R_3: $\sqrt{4KTR_3}$	$1+R_2/R_1$
Шумовий струм, що протікає через R_3: In_3	$1+R_2/R_1$
Вхідна шумова напруга: V_n	$1+R_2/R_1$
Шум Джонсона на резисторі R_1: $\sqrt{4KTR_1}$	$-R_2/R_1$
Шум Джонсона на резисторі R_2: $\sqrt{4KTR_2}$	1

Структурна схема генератора випадкових чисел. Структурну схему апаратного генератора випадкових чисел показано на рис. 2. Як джерело теплового шуму використовуються два однакові резистори з великим номіналом опору (близько 10^6 Ом). Для одержання необхідного рівня сигналу й смуги пропускання частот використовується трикаскадний підсилювач зі збалансованим коефіцієнтом підсилення й автокореляцією рівня нуля сигналу. Операційний підсилювач підсилює сигнал і приводить його до рівня аналогової землі AGND. Після підсилення шумовий сигнал подається на вхід компаратора. Рівень спрацьовування компаратора дорівнює рівню AGND. Якщо значення сигналу від'ємне відносно AGND, то на виході компаратора – нуль, в іншому випадку на виході компаратора – одиниця. Отже, з недетермінованого сигналу білого шуму ми отримуємо випадковий бітовий потік.

Наступна обробка отриманого бітового потоку здійснюється програмно. Програмний модуль формує вихідний бітовий потік, перетворює його в байтовий потік і передає через порт RS232. Логіку роботи програми можно легко зрозуміти з наведеної на рис. 3 блок-схеми.

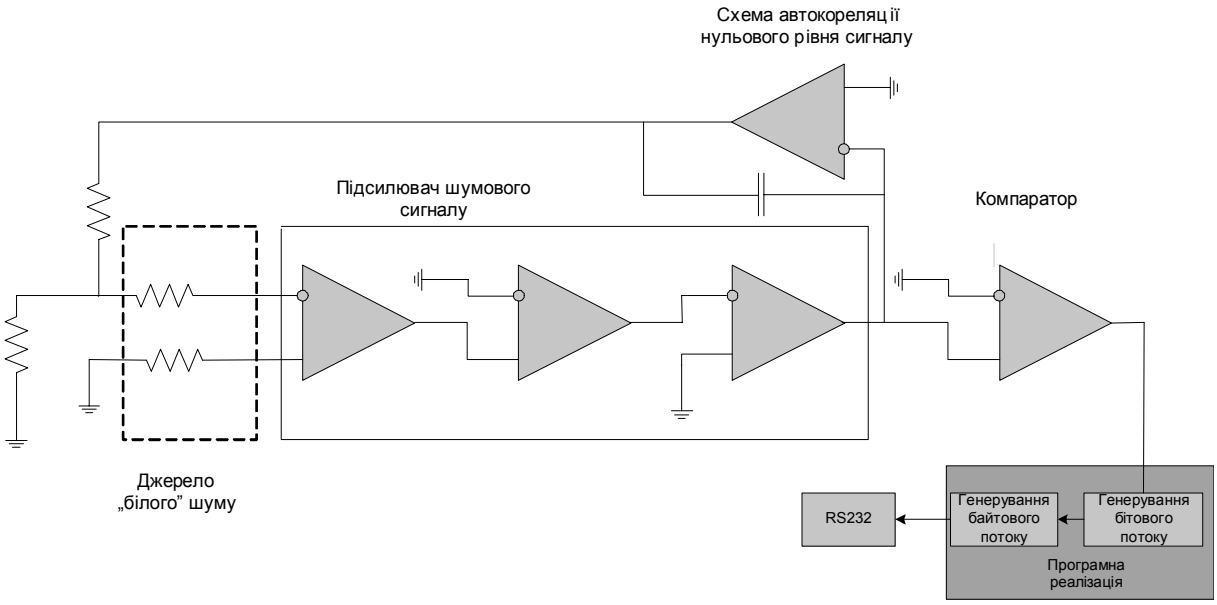

Рис. 2. Структурна схема генератора випадкових чисел

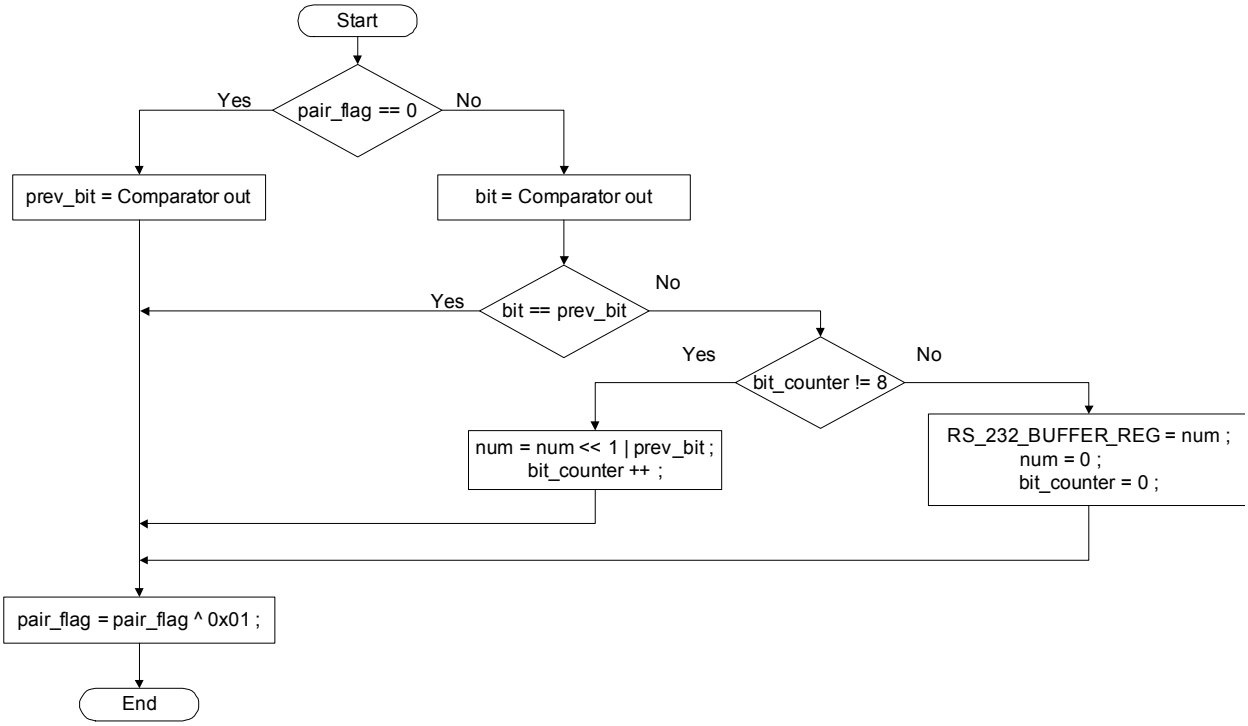

Рис. 3. Блок-схема роботи програмного модуля генератора випадкових чисел

Деякі аспекти практичної реалізації генератора випадкових чисел. Запропонована структура для тестування та подальшого дослідження була реалізована у вигляді дослідного зразка (рис. 4).

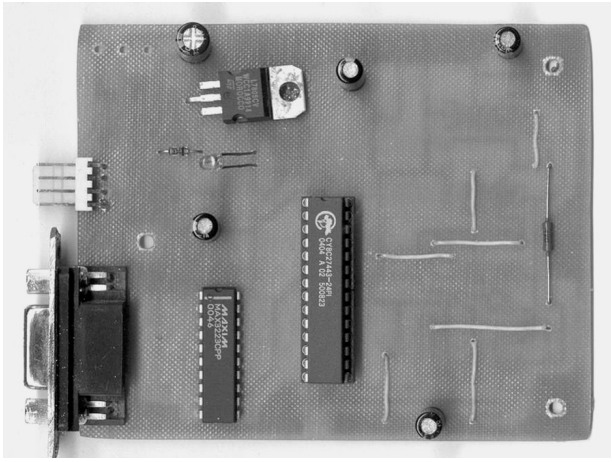

Рис. 4. Фотографія дослідного зразка генератора випадкових чисел

При побудові генератора необхідно підсилювати дуже слабкий широкосмуговий шумовий сигнал. Тому для трикаскадного сигнального підсилювача використовувалися точні операційні підсилювачі з низьким рівнем шуму (2.4 n/√Hz) та смугою пропускання сигналу 28 Мгц. Коефіцієнт підсилення кожного підсилювача дорівнює 20, тобто сумарний коефіцієнт трикаскадного підсилювача дорівнює 8000.

Вихідний сигнал компаратора для подальшої програмної обробки подається на порт мікроконтролера CY8C27443 фірми Cypress MicroSystems. Замість нього може використовуватись будь-який мікроконтролер з вбудованим таймером та інтерфейсом RS232. Вся програмна обробка бітового потоку здійснюється в обробнику переривань від таймера.

Друкована плата генератора повністю екранована. Це дозволяє позбутися впливу сторонніх періодичних електромагнітних завад.

Тестування розробленого генератора випадкових чисел. Для тестування генератора використовувались дві групи тестів [5]: графічні та оціночні тести. У графічних тестах статистичні властивості послідовностей відображаються у вигляді графічних залежностей, по виду яких роблять висновки щодо властивостей досліджуваної послідовності. Ця група складається із множини таких різних тестів, як гістограма розподілу елементів, розподіл елементів на площині, перевірка серій, перевірка на монотонність, автокореляційна функція, графічний спектральний тест. При тестуванні генератора використовувалися два тести – гістограма розподілу елементів та розподіл елементів на площині [5]. В оціночних тестах статистичні властивості послідовностей визначаються числовими характеристиками. На основі оціночних критеріїв робляться висновки про ступінь близькості властивостей аналізованої й істинно випадкової послідовностей. Є кілька різних добірок оціночних тестів, наприклад набір тестів Дж. Марсалья [6], Х. Густафсона [7], А. Менезиса [8], рекомендація NIST [9]. З цієї групи використовувались два тести з рекомендації NIST – частотний монобітний тест та тест дірок.

Гістограма розподілу елементів дозволяє оцінити рівномірність розподілу елементів у досліджуваній послідовності, а також визначити частоту появи конкретного символу. Для випадкової послідовності частоти появи символів повинні бути приблизно однакові. Побудова розподілу елементів на площині дає можливість виявити наявність залежностей між елементами досліджуваної послідовності. Якщо між елементами послідовності відсутні залежності, то точки на полі розташовані хаотично. Якщо ж між елементами є певна залежність, на полі спостерігаються візерунки – послідовність не є випадковою. На рис. 5 показано результати графічних тестів. Візуальна оцінка дає позитивний результат – послідовність може бути випадковою.

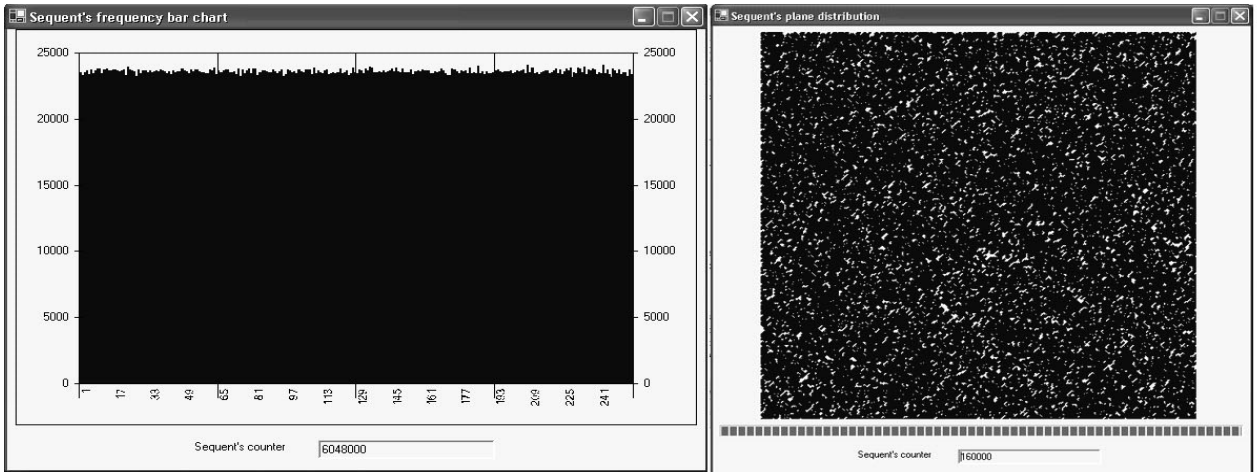

Рис. 5. Результати графічних тестів

Мета частотного монобітного тесту – перевірити рівномірність появи 0 і 1 у досліджуваній послідовності. Для випадкової послідовності кількість 0 та 1 у послідовності повинна бути приблизно однаковою. Тест "дірок" дозволяє перевірити рівномірність розподілу 0 і 1 у досліджуваній послідовності на основі аналізу кількості появи блоків – підпослідовностей, що складаються з одних одиниць, і дірок – підпослідовностей, що складаються з одних нулів. Алгоритми тестів та критерії оцінки повністю описані в [9], в табл. 2 та 3 наведено результати для 5 послідовностей по 32000 байт в кожній. Кожна послідовність задовольняє критерії випадкової. Отже, можна зробити висновок, що в результаті досліджень був побудований генератор істинно випадкових чисел.

Таблиця 2

Результати частотного монобітного тесту

Номер	Sn	P-value	Результат
1	46	0.9276	пройдено
2	300	0.5532	пройдено
3	418	0,4082	пройдено
4	27	0,9574	пройдено
5	108	0,8310	пройдено

Таблиця 3

Результати тесту “дірок”

Номер	P-value	Результат
1	0.573	пройдено
2	0.2316	пройдено
3	0.936	пройдено
4	0.7203	пройдено
5	0.8318	пройдено

Висновки. У роботі запропоновано новий варіант побудови генераторів випадкових чисел. Використання теплового шуму опору в поєднанні з шумом операційного підсилювача забезпечує необхідну стабільність шумового сигналу. Для тестування та подальшого дослідження запропонованого варіанта був реалізований дослідний зразок. Результати тестування згенерованих послідовностей доводять працездатність запропонованого варіанта побудови генератора випадкових чисел.

1. Understanding Public Key Infrastructure (PKI), An RSA Data Security White Paper. 2. Столлингс В. Криптография и защита сетей – Принципы и практика. – К., 2003. 3. Israelsohn Josbua. Noise 101, EDN-Europe, February 2004. – P. 37. 4. Романов В. Шумы в операционных усилителях, ЕКиС.– К.: VD MAIS, 2003. – № 8. 5. Іванов М., Чугункою И. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. – М., 2003. 6. Marsaglia G. DIEHARD Statistical tests. 7. Gustafson H. et. al. A computer package for measuring strength encryption algorithms. Journal of computers and security. – 1994. – Vol. 13, No 8. – P. 687–697. 8. Menezes A., van Oorshot P., Vanstone S. Handbook of applied cryptography. CRC Press, 1997. 9 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, May 2001, available at: http://csrc.nist.gov/rng/SP800-22b.pdf.