УДК 004.005:004.9
DOI https://doi.org/10.32782/2663-5941/2025.4.2/16

Добровольський Ю.Г.
Чернівецький національний університет імені Юрія Федьковича

Дячук Р.Л.
Чернівецький національний університет імені Юрія Федьковича

ДОСЛІДЖЕННЯ ГЕНЕРАЦІЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ ЧИСЕЛ НА ОСНОВІ ТЕМНОВОГО СТРУМ ФОТОДІОДА ПРИ РІЗНИХ ТЕМПЕРАТУРАХ

У статті розглянуто актуальне питання сучасної програмної інженерії, яке полягає у розробці та дослідження зовні непередбачуваних псевдовипадкових числових послідовностей, які можуть бути покладені в основу розробки протоколів кібербезпеки. В нашому випадку в якості джерела випадкових чисел виступає темновий струм фотодіода. Відомі дослідження розглядали певні напівпровідникові вироби в якості як джерела псевдовипадкової послідовності. Але фотодіоди не були розглянуті.

Метою дослідження є дослідження генерації випадкової послідовності чисел на основі темнового струм фотодіода, які отриманих при різних температурах. Для досягнення мети дослідження було розроблено установку для вимірювання темнового струму фотодіода ФД-288 при температурі 10, 30 та 50 °С з частотою відбору 20000 значень темнового струму в секунду. Також розроблений алгоритм генерації псевдовипадкової послідовності чисел, основних на значеннях темнового струму фотодіода. Досліджено генерацію випадкової послідовності чисел на основі виміряних значень зворотного (темнового) струм фотодіода, отриманих при різних температурах. А саме при 10, 30 та 50 °С.

В результаті проведених досліджень встановлено, що найкращі результати досягнути при генерації випадкової послідовності чисел на основі темновго с руму фотодіода, отриманої при 50 °С. А саме – мінімальне значення складає 0,0 при вимозі 0.39; максимальне значення складає 0.68 при вимозі 0.39; середнє значення 0.39 при вимозі 0.39; середньоквадратичне відхилення 0.18 при вимозі 0.04; процент відсутніх елементів 0 при вимозі 0. Показано, що фотодіод, при температурі 50 °С, може бути джерелом для генерації послідовності псевдовипадкових чисел. При цьому розподіл чисел є рівномірно-хаотичним, а кожне число рівномірно представлене не частіше 0.18%, що менше за ідеальні умови, але достатньо для практичного застосування.

Подальші дослідження передбачають вивчення можливостей створеного обладнання з точки зору застосування в якості джерела ентропії інших фотодіодів та алгоритму для генерації ПВП на основі темнового струму фотодіода та підвищення швидкодії методу.

Ключові слова: *програмна інженерія, кібербезпека, фотодіод, темновий струм, випадкові числа.*

Постановка проблеми. Інформаційні технології забезпечують практично весь цифровий інформаційний потік у сучасному світі. Однак, цей потік має бути надійно захищений з огляду на інтереси як окремої людини користувача, так і держави у цілому. Це завдання загалом вирішується, як відомо, засобами кібербезпеки, методи якої ґрунтуються, у великій мірі, на технологіях програмної інженерії. Зокрема, вельми актуальним з цієї точки зору, є випадкові числові послідовності, які покликані убезпечити потоки вхідних і вихідних даних. На разі застосовуються багато методів генерації випадкових числових послідовностей. Наприклад, серед найвідоміших методів є використання обсягу стекової/купної пам'яті комп'ютера, або точне вимірювання поточного значення часу з точністю до наносекунд (час Unix), які дають набір випадкових значень, які можна використати для генерації відповідної випадкової послідовності. Зовнішня периферія комп'ютера, така як USB, клавіатура, або миша також можуть слугувати джерелами випадкових чисел. Загалом, усі ці джерела називають джерелами ентропії, або, інакше, хаосу, оскільки вважається, що їх, ці випадкові послідовності, не можна передбачити. Але, значення

випадкових послідовностей, отримані вище наведеними методами, не можна вважати абсолютно випадковими. Вони генеруються у певних діапазонах, підкоряються певним коливанням. Усі ці особливості можливо передбачити. Щоби такого не трапилося такі послідовності чисел можна перетворити на справді випадкові числа, як що їх піддати криптографічним перетворенням. Наприклад за допомогою клітинних автоматів [1]. Таки перетворення створюють рівномірно розподілені випадкові значення кожного числа в послідовності. Також вони характеризуються нерівномірним розподілом значення джерела ентропії. Отримані таким чином числові послідовності прийнято називають псевдовипадковими, оскільки вони створюються детерміновано із ентропії, і не є дійсно випадковими.

Отже, джерело ентропії (хаосу), будь якого походження, можна використовувати для створення випадкових числових послідовностей. Це дозволяє отримати непередбачуваність цифрових значень, які містяться у такій послідовності. Вони використовуються в протоколах безпеки мереж, для крипто безпечних з'єднань, створення криптографічних ключів, відслідковування цілісності системи і в багатьох інших цілях [2].

Підсумовуючи вище наведене, можна напевне стверджувати, що розробка надійних, крипто стійких протоколів, які в своїй основі мають генерацію непередбачуваних, псевдовипадкових числових послідовностей є дуже актуальним завданням для сучасної програмної інженерії.

Аналіз останніх досліджень і публікацій. Сучасні генератори псевдовипадкових числових послідовностей, які базуються лише на певному програмному забезпеченні, не можуть здолати певної передбачуваності [3]. Окрім того, існуючи технології створення псевдовипадкових послідовностей, є загальнодоступні. Як що взяти генерацію ентропії, отриману за допомогою мови Java [4], то такі послідовності можуть бути, певним чином, теоретично, доступні для зламу алгоритму шифрування. Застосування квантових обчислень в кібератаках [5, 6], збільшує ефективність таких атак практично до успішного рівня.

Відомі, загалом, два підходи, за допомогою яких створюються послідовності випадкових чисел. Перший підхід використовує спеціалізовані прилади, основані на фізичних джерелах шуму [7]. Їх недолік полягає у необхідності додаткового приладового обладнання (адаптерів) та спеціалізованого програмного забезпечення для комунікації із комп'ютером.

Інший підхід базується на використанні фізичних подій, у комп'ютерних пристроях. З точки зору надійності, такий підхід є більш виправданим. Наприклад, використання в якості генератора псевдовипадкової послідовності лічильника тактової частоти процесора. Його недолік полягає у тому, що він є чутливим до зовнішніх факторів, і, таким чином, до зовнішнього впливу на процедуру генерування випадкової послідовності чисел [8]. Оптичний маніпулятор миші також може бути запропонований для генерації випадкової числової послідовності [9]. Оптичний маніпулятор миші створює досить неоднорідний розподіл випадкових чисел, про те, має малу швидкість генерації (біля 1 кбіт/с), що не дозволяє його використання у швидкісних системах шифрування.

У [10] запропонований інший метод генерації випадкової числової послідовності. Зокрема, автори використовують веб-камеру, а саме пікселі, з яких веб-камера створює зображення, в якості джерела зовнішньої непередбачуванності. Як показано авторами у [10] динаміка інтенсивності пікселів, які містяться у матриці, побудованій на основі приладу з зарядовим звя'зком (ПЗЗ)-матриця веб-камери, є абсолютно непередбачуваною. Її не видно звичайним оком, разом з тим, вона чітко фіксуються як вимірювальною апаратурою, так і програмними методами.

Спираючись на вище наведене, було розглянуто питання щодо використання в якості джерела псевдовипадкової послідовності чисел не веб-камери (пікселів, які генерують зображення), а фізичні властивості ПЗЗ матриці, на основі якої побудована веб-камера. Такі матриці створюються за звичай на основі кремнію, як що веб-камера працює у видимому діапазоні спектру. Постало питання, а чи доцільно використання в якості джерела псевдовипадкової числової послідовності не інтенсивність пікселів веб-камери, значення темнового струму кремнієвого фотодіоду. Ця величина надзвичайно динамічна і її конкретна величина у кожен момент часу змінюється. Також темновий струм фотодіоду надзвичайно чутливий до температури та інших зовнішніх впливів і є дійсно непередбачуваною величиною [11]. Раніше, у [12], розглядалися певні напівпровідникові вироби в якості як джерела псевдовипадкової послідовності. Але не фотодіоди.

Постановка завдання. Метою роботи є: дослідження генерації випадкової послідовності чисел на основі зворотного струм фотодіода, отриманих при різних температурах.

Виклад основного матеріалу. Раніше ми досліджували можливість та ефективність генерації псевдовипадкової послідовності чисел, заснованому на фіксації темнового струму кремнієвого фотодіода ФД-288. Ці дослідження показали, що ряд випадкових чисел у діапазоні [0. 9], які відповідають значенням темнового струму фотодіода, і цифровані за допомогою USB-адптера на базі Arduino (112593), мають швидкість генерації, інакше – продуктивність (Р) 980 байт/сек. Що є дуже мало. Вимоги криптографії вказують щоби випадкові числа хаотичної послідовності були у діапазоні [0. 256]. Це відповідає типу даних byte, які притаманні мови програмування Java. Підсилення сигналу темнового струму на 5 Вольт, переводить характеристику розподілу по значенню псевдовипадкових чисел у бік «рівномірно-хаотичної». А саме, кожне отримане число у послідовності представлено рівномірно. Його повторення зустрічається у діапазоні 0.3–0.7 %, при ідеальному варіанті: 1/256 = 0.004, або 0.4%.

З урахуванням вище наведеного, було запропоновано підвищити температуру фотодіода для збільшення розкиду значень темнового струму. Було проведено вимірювання темнового струму фотодіода ФД-288 при температурі 10, 30 та 50 °С, що відповідає умовам його експлуатації за допомогою установки, блок-схема якої наведена на рисунку 1.

Температуру на фотодіоді знижували до 10 °С і підвищували до 30 та 50 °С за допомогою термоелектричного охолоджувача. Зменшення чи збільшення температури на фотодіоді здійснювали змінюючи полярність живлення на охолоджувачі. Температура фотодіода контролювалася в цокольній області його корпуса, за допомогою термометра цифрового Тензор-42, який забезпечує вимірювання температури у діапазоні 0–200 °С із дискретністю показів 0,01 °С із межею основної відносної похибки ± 0,05 °С. Темновий струм вимірювався при зміщенні на p-n переході фотодіоду 1 В.

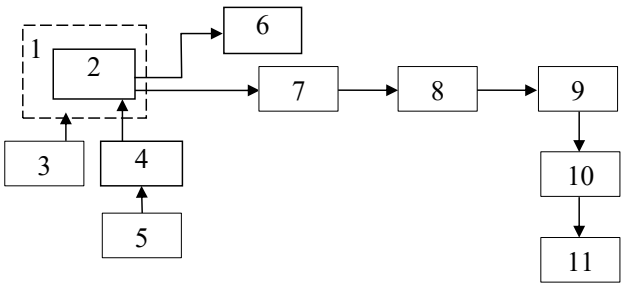

Рис. 1. Блок-схема установки для вимірювання темнового струму фотодіода ФД-288 при температурі 10, 30 та 50 °С

1 – світлонепроникний екран, 2 – фотодіод, 3 – блок живлення фотодіода, 4 – термоелектричний охолоджувач, 5 – блок живлення термоелектричного охолоджувача, 6 – термометр цифровий Тензор-42, 7 – ППСН, 8 – контролер Arduino (112593), 9 – USB-адаптер, 10 – USB порт комп'ютера, 11 – процесор комп'ютера

Далі, виміняні значення темнового струму у режимі on-line за допомогою прецизійного перетворювача струм-напруга (ППСН) перетворюються у напругу (U_T) і, використовуючи USB-адаптер на основі Arduino (112593), передавалися до комп'ютера, як це показано на рис. 1. В комп'ютері значення U_T відображалися у вигляді гістограм.

Далі, за допомогою засобів програмного забезпечення (ПЗ) мови програмування Java (версія 17), із використанням бібліотеки javax-usb, розроблений алгоритм генерації псевдовипадкової послідовності чисел (ПВЧ), основних на значеннях темнового струму фотодіода (рис. 2).

У подальшому цей список випадкових чисел досліджується на відповідність статистичним характеристикам за допомогою бібліотеки DescriptiveStatistics. Для графічного відображення статистичних характеристик використовувалась бібліотека jfree.chart та jfree.data.

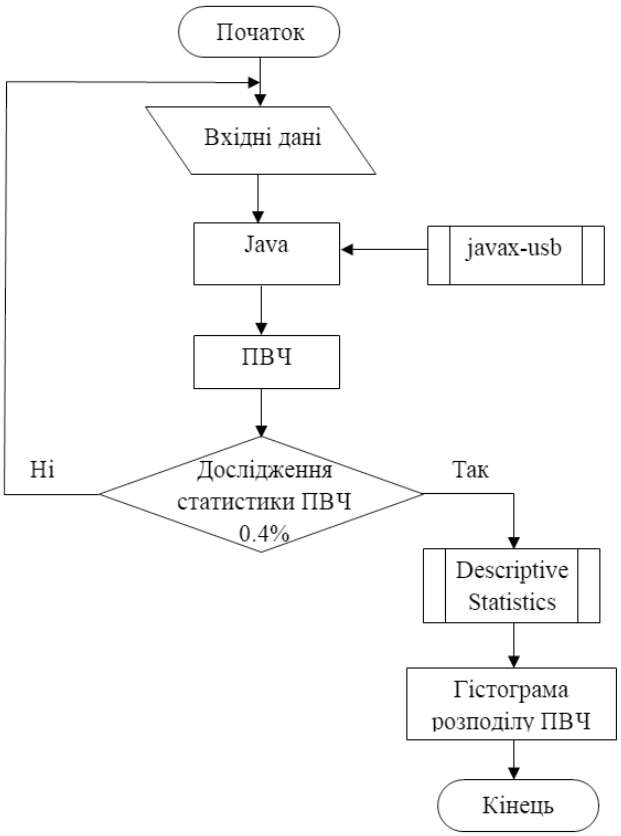

Рис. 2. Блок-схема алгоритму генерації псевдовипадкової послідовності чисел

При кожній температурі було виміряно по 20000 значень темнового струму в секунду. Динаміка темнового струму при трьох температурах – 10,

30 та 50 °С наведена на рисунках. 3, 4 та 5 відповідно.

З рисунків 3–5 видно, що при температурі 10 °С діапазон виміряних значень темнового струму складає від 10^{-11} до $8 \cdot 10^{-9}$ А, при температурі 30 °С діапазон виміряних значень темнового струму складає від 10^{-11} до $8 \cdot 10^{-7}$А, а при температурі 50 °С діапазон виміряних значень темнового струму складає від 10^{-11} до $7 \cdot 10^{-7}$А. При цьому найбільший розкид значень спостерігається при 10 °С, а найбільша густина розподілу значень темнового струму спостерігається при 50 °С.

З отриманого набору даних (значень темнового струмку, в подальшому перетворених у напругу і переданого до комп'ютера) були згенеровані ПВП згідно алгоритму, наведеному на рис. 2.

На рис. 6. наведена гістограма розподілення випадкових чисел по значенню для температури 10 °С.

З рисунку видно, що не всі елементи випадкової послідовності (байти) представлені одноковою часткою присутності. Байти у діапазоні [5 … 25]

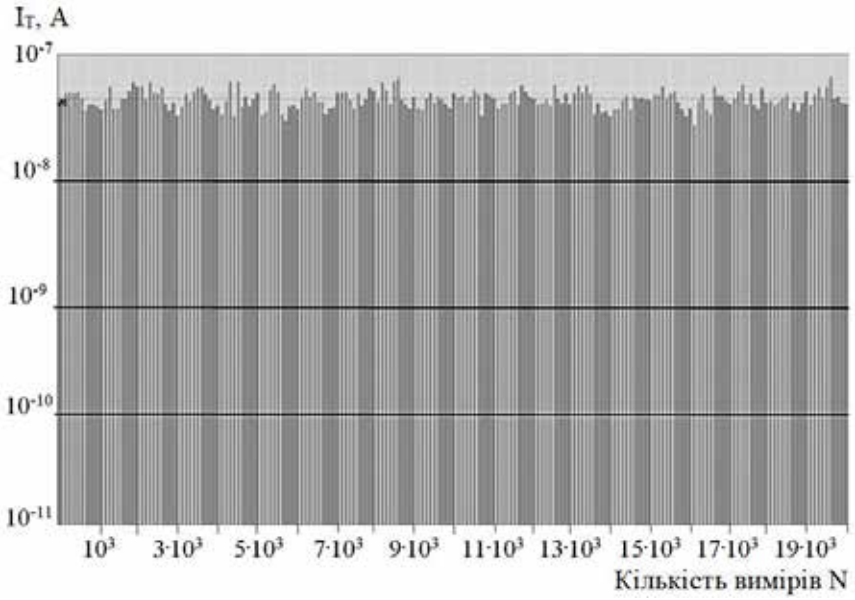

Рис. 3. Динаміка темнового струму при температурі 50 °С

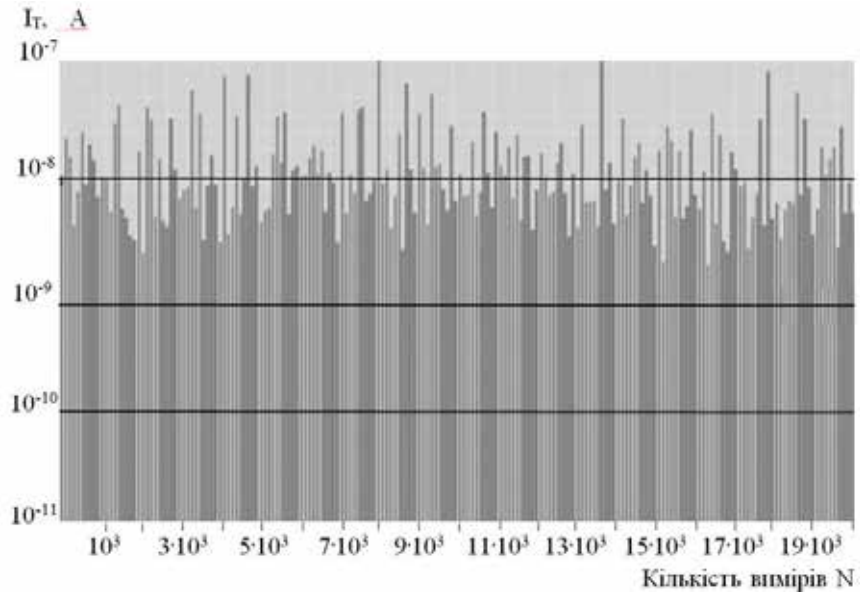

Рис. 4. Динаміка темнового струму при температурі 30 °С

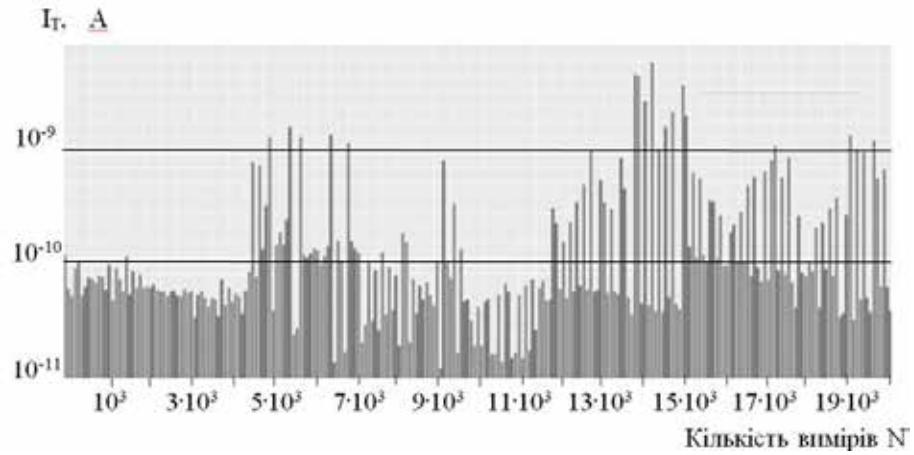

Рис. 5. Динаміка темнового струму при температурі 10 °С

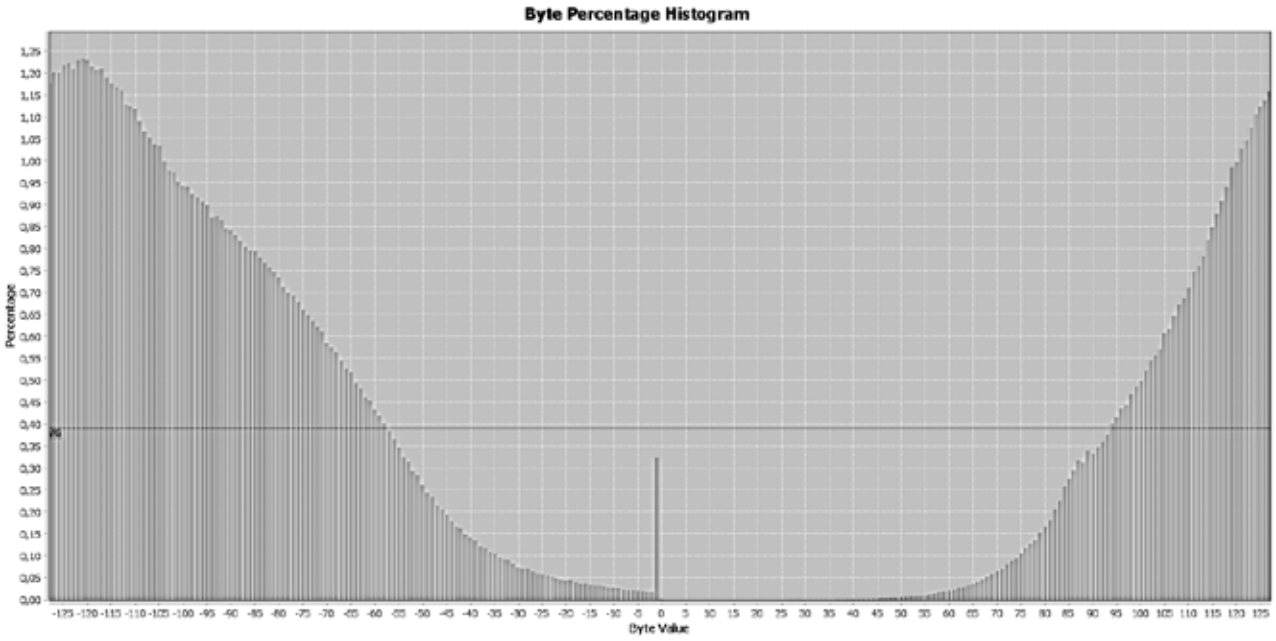

Рис. 6. Гістограма розподілення випадкових чисел, що були згенеровані, по значенню величини для температури 10 °С

взагалі відсутні у послідовності, а байти у діапазоні [120 … 125] займають приблизно 1,2 % частки від усіх елементів послідовності. Хоча всі числа носять абсолютно випадковий характер, такий розподіл не є задовільним з точку зору вимог програмної інженерії до криптозахисту.

На рис. 7 наведена гістограма розподілення випадкових чисел по значенню для температури 30 °С.

Для температури 30 °С видно з гістограми, що розподілення дещо вирівнялась – немає відсутніх елементів. Проте круті нерівності гістограми не дають нам змогу характеризувати цей розподіл, як рівномірний. Скоріше всього це хаотичний розподіл.

На рис. 8 наведена гістограма розподілення випадкових чисел по значенню для температури 50 °С.

Для температури 50 °С видно з гістограми, що розподілення дещо стала плавною. Це дає нам змогу характеризувати цей розподіл, як рівномірно-хаотичний. І для деяких випадків (особливо у стеганографії) такий розподіл є цілком задовільний.

Проте візуальний огляд гістограми не дає нам кількісних показників якості згенерованих ПВЧ. За допомогою мови Джава, зокрема статистичної бібліотеки DescriptiveStatistics, вдалось обчислити параметри, що характеризують якість згенерованої ПВЧ для кожної температури.

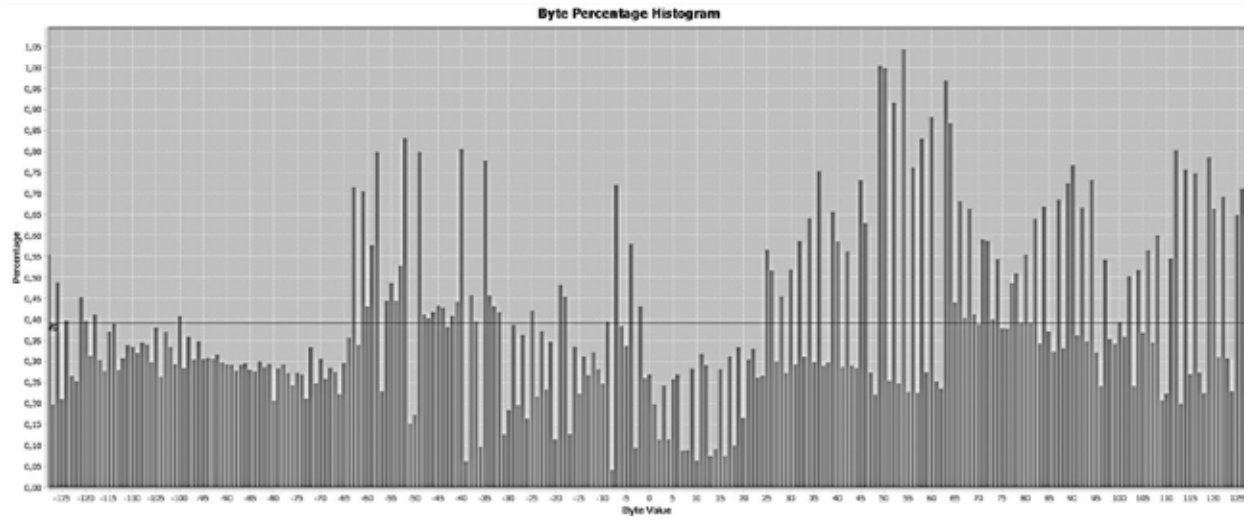

Рис. 7. Гістограма розподілення випадкових чисел, що були згенеровані, по значенню величини для температури 30 °С

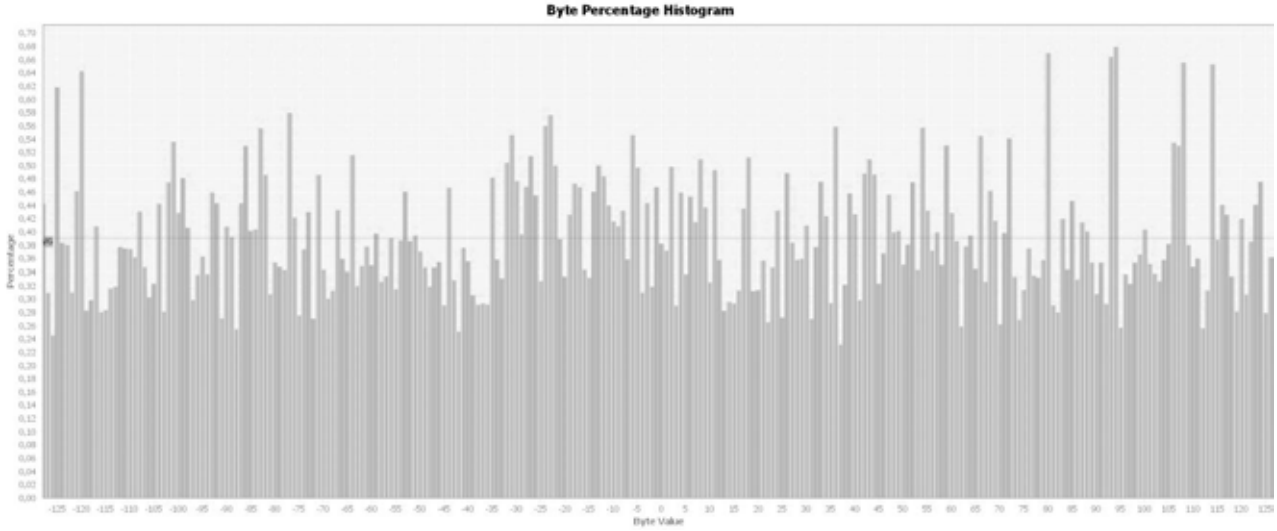

Рис. 8. Гістограма розподілення випадкових чисел, що були згенеровані, по значенню величини для температури 50 °С

Порівняльні статистичні характеристики згенерованих послідовностей, отриманих з значень темнового струму прирізних температурах, наведені у таблиці 1.

Нагадаємо, що для ідеального рівномірного розподілу [13]:

– мінімальне значення min = 0.39;

– максимальне значення max = 0.39;

– середнє значення mean = 0.39;

– середньоквадратичне відхилення st dev = 0.04;

– процент відсутніх елементів absent = 0%.

Самою показовою характеристикою э середньо квадратичне відхилення. Чим менше відхилення, тим менше розкид значень, тим більш рівномірним є розподіл.

Як видно з таблиці 1, середньо квадратичне відхилення зменшується із зростанням температури. Зокрема встановлено, що найкращі результати досягнути при генерації випадкової послідовності чисел на основі темновго с руму фотодіода, отриманої при 50 °С. А саме – мінімальне значення складає 0,0 при вимозі 0.39; максимальне значення складає 0.68 при вимозі 0.39; середнє значення 0.39 при вимозі 0.39; середньоквадратичне відхилення 0.18 при вимозі 0.04; процент відсутніх елементів 0 при вимозі 0.

Показано, що фотодіод, при температурі 50 °С, може бути джерелом для генерації послідовності псевдовипадкових чисел. При цьому розподіл чисел є рівномірно-хаотичним, а кожне число

Таблиця 1

Статистичні характеристики згенерованих послідовностей

Температура	10°C	30°C	50°C	Вимоги ідеального розподілу ПВП
Статистичні параметри розподілу, %	min: 0.0 max: 1.27 mean: 0.39 std dev: 0.85 absent: 8%	min: 0.0 max: 1.05 mean: 0.39 std dev: 0.33 absent: 0	min: 0.0 max: 0.68 mean: 0.39 std dev: 0.18 absent: 0	min: 0.39 max: 0.39 mean: 0.39 st dev: 0.04 absent: 0

рівномірно представлене не частіше 0.18%, що менше за ідеальні умови, але достатньо для практичного застосування.

Подальші дослідження передбачають вивчення можливостей створеного обладнання з точки зьору застосування в якості джерела ентропії інших фотодіодів та алгоритму для генерації ПВП на основі темнового струму фотодіода та підвищення швидкодії методу.

Висновки. У даному дослідженні розроблено установку для вимірювання темнового струму фотодіода ФД-288 при температурі 10, 30 та 50 °С з частотою відбору 20000 значень темнового струму в секунду. Також розроблений алгоритм генерації псевдовипадкової послідовності чисел, основних на значеннях темнового струму фотодіода. Досліджено генерацію випадкової послідовності чисел на основі виміряних значень зворотного (темнового) струм фотодіода, отриманих при різних температурах. А саме при 10, 30 та 50 °С. Встановлено, що найкращі результати досягнути при генерації випадкової послідовності чисел на основі темновго с руму фотодіода, отриманої при 50 °С. А саме – мінімальне значення складає 0,0 при вимозі 0.39; максимальне значення складає 0.68 при вимозі 0.39; середнє значення 0.39 при вимозі 0.39; середньоквадратичне відхилення 0.18 при вимозі 0.04; процент відсутніх елементів 0 при вимозі 0. Показано, що фотодіод, при температурі 50 °С, може бути джерелом для генерації послідовності псевдовипадкових чисел. При цьому розподіл чисел є рівномірно-хаотичним, а кожне число рівномірно представлене не частіше 0.18%.

Список літератури:

1. Cicuttin A. De Micco L. Crespo M. L. et al. Looking for suitable rules for true random number generation with asynchronous cellular automata. Nonlinear Dynamics. 2022. Vol. 111, P. 2711-2722. DOI: 10.1007/s11071-022-07957-8.

2. Aljahdal A. O. Random Number Generators Survey. International Journal of Computer Science and Information Security. 2020. Vol. 18, No. 10. P. 14-22. DOI: 10.5281/zenodo.4249406.

3. Martinez F. Attacks on Pseudo Random Number Generators Hiding a Linear Structure. Cryptographers' Track at the RSA. Conference 2022. (Virtual Event, United States., Mar 2022). P. 145-168.

4. Class SecureRandom. All Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html (дата звернення: 21.06.2025).

5. Остапов С.Е., Добровольський Ю.Г. Квантова інформатика та квантові обчислення: навч. посібник. Чернівці: ЧНУ ім. Ю. Федьковича, 2021. – 99 с.

6. Jacak J.E., Jacak W.A., Donderowicz W.A. Wojciech A. Jacak L. Quantum random number generators with entanglement for public randomness testing. Scientific Reports. 2020. Vol. 10, № 164. P. 121-130. DOI: 10.1038/s41598-019-56706-2.

7. Бараннік В. В., Сідченко С. О., Бараннік Н. В., Хіменко А. М. Метод маскувального ущільнення службових даних в системах компресії відеозображень. Радіоелектронні і комп'ютерні системи. 2021. № 2 (98). С. 51-63 DOI: 10.32620/reks.2021.2.05.

8. Бараннік В. В., Бараннік Н. В., Ігнатьєв О. О., Хіменко А. М. Метод непрямого приховування інформації в процесі стиснення відеозображень. Радіоелектронні і комп'ютерні системи. 2021. № 4. С. 119-131 DOI: 10.32620/reks.2021.4.10.

9. Ostapov, S., Diakonenko, B., Fylypiuk, M., Hazdiuk, K., Shumyliak, L., Tarnovetska, O. Symmetrical Cryptosystems based on Cellular Automata. International Journal of Computing. 2023. № 22. P. 15-20. DOI: 10.47839/ijc.22.1.2874.

10. Diachuk R., Dobrovolsky Y., Hanzhelo D., Prokhorov H., Trembach D. Research the Level of Chaotic and Reliability in Webcam-generated Random Number Sequences. Security of Infocommunication Systems and Internet of Things. 2024. Vol. 2, № 1. P. 1-6. DOI: 10.31861/sisiot2024.1.01004.

11. Rogalski A. Infrared and Terahertz Detectors. Third Edition. London, CRC Press, 2022, 1066 P.
12. Soorat R., Ashok M. K. Vudayagiri Hardware Random number Generator for cryptography. arXiv. 2015. DOI: 10.48550/arXiv.1510.01234.
13. Веригіна І. В., Островська О. В. Теорія ймовірностей та математична статистика: Частина 2. Випадкові величини: Лекції і практикум. Київ, КПІ ім. Ігоря Сікорського, 2021. 77 с. URL:https://surl.li/kuhkuk (дата звернення: 21.06.2025).

Dobrovolsky Yu.G., Diachuk R.L. STUDY OF RANDOM NUMBER SEQUENCE GENERATION BASED ON DARK CURRENT OF A PHOTODIODE AT DIFFERENT TEMPERATURES

The article considers a topical issue of modern software engineering, which consists in the development and study of externally unpredictable pseudo-random number sequences that can be used as a basis for the development of cybersecurity protocols. In our case, the dark current of a photodiode acts as a source of random numbers. Known studies have considered certain semiconductor products as sources of a pseudo-random sequence. But photodiodes were not considered.

The purpose of the study is to study the generation of a random sequence of numbers based on the dark current of a photodiode, which are obtained at different temperatures. To achieve the goal of the study, a device was developed for measuring the dark current of a photodiode HD-288 at temperatures of 10, 30 and 50 °C with a sampling frequency of 20000 dark current values per second. An algorithm for generating a pseudo-random sequence of numbers based on the dark current values of the photodiode has also been developed. The generation of a random sequence of numbers based on the measured values of the reverse (dark) current of a photodiode obtained at different temperatures was investigated. Namely at 10, 30 and 50 °C.

As a result of the conducted research, it was found that the best results were achieved when generating a random sequence of numbers based on the dark current of a photodiode obtained at 50 °C. Namely – the minimum value is 0.0 at the requirement of 0.39; the maximum value is 0.68 at the requirement of 0.39; the average value is 0.39 at the requirement of 0.39; the standard deviation is 0.18 at the requirement of 0.04; the percentage of missing elements is 0 at the requirement of 0. It is shown that a photodiode, at a temperature of 50 °C, can be a source for generating a sequence of pseudo-random numbers.

In this case, the distribution of numbers is uniformly chaotic, and each number is uniformly represented no more than 0.18%, which is less than ideal conditions, but sufficient for practical application. Further research involves studying the capabilities of the created equipment in terms of using other photodiodes as a source of entropy and an algorithm for generating PVP based on the dark current of the photodiode and increasing the speed of the method.

Key words: *software engineering, cybersecurity, photodiode, dark current, random numbers.*

Дата надходження статті: 20.06.2025
Дата прийняття статті: 30.06.2025
Опубліковано: 27.10.2025