https://doi.org/10.31891/2307-5732-2025-357-15
УДК 004.005:004.9

ДОБРОВОЛЬСЬКИЙ ЮРІЙ
Чернівецький національний університет ім. Ю. Федьковича
https://orcid.org/0000-0002-1248-3615
e-mail: y.dobrovolsky@chnu.edu.ua
ДЯЧУК РОСТІСЛАВ
Чернівецький національний університет ім. Ю. Федьковича
e-mail: r.diachuk@chnu.edu.ua

ДОСЛІДЖЕННЯ ЗВОРОТНОГО СТРУМУ ФОТОДІОДА ДЛЯ ГЕНЕРАЦІЇ НАДІЙНОЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ ЧИСЕЛ

В роботі наведено результати досліджень в напрямку створення надійних, безпечних протоколів кібербезпеки, які базуються на генерації зовні непередбачувані псевдовипадкові, хаотичні числових послідовностях. Зокрема вивчено доцільності застосування в якості джерела випадкової послідовності чисел величини зворотного (темнового) струму фотодіода на основі кремнію, який працює у фотодіодному режимі. В результаті проведених досліджень показано, що фотодіод може бути джерелом ентропії для генерації випадкових чисел. Такий розподіл є рівномірно-хаотичним і кожне число представлено приблизно рівномірно у діапазоні 0.3 — 0.7 %.

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

DOBROVOLSKY YURIY
DYACHUK ROSTISLAV
Chernivtsi National University named after Yu. Fedkovych

STUDY OF THE REVERSE CURRENT OF A PHOTODIODE FOR THE GENERATION OF A RELIABLE RANDOM SEQUENCE OF NUMBERS

The paper presents the results of research in the direction of creating reliable, secure cybersecurity protocols based on the generation of externally unpredictable pseudo-random, chaotic numerical sequences. Methods for generating random sequences are, in turn, one of the defining components of cybersecurity from the point of view of software engineering, namely, ensuring the security of incoming and outgoing data flows. The source of entropy (chaos) can be used to generate random numerical sequences. This provides a certain uniqueness and, most importantly, unpredictability of values. Such pseudo-random numerical sequences are used in various networks to ensure efficient and secure connections, generate cryptographic keys, monitor integrity, and in many other areas. The purpose of our research was to examine the question of whether it is possible to use the value of the reverse current, for example, of a darkened photodiode, as a source of a random numerical sequence. The interest in this issue is due to the fact that the reverse current of a photodiode operating in the photodiode mode, i.e. when electrically biased at the p-n junction, is a truly physically unpredictable quantity. As a result of the study, it turned out that if the reverse (otherwise - dark) current of the photodiode is used as a source of a random sequence, the random number generation performance for Arduino will be 980 bytes/sec., which is quite small, since the histogram of the distribution of the value of random numbers, obtained by methods using the DescriptiveStatistics library, is close to the Gaussian distribution. But, if you amplify the dark current signal to 5 Volts, the histogram of the distribution of the value of random numbers obtained from the FD using an amplifier is uniformly chaotic. Namely, each number is represented approximately evenly in the range of 0.3 - 0.7%. Given that the ideal fraction for each number in this case (1/256) is 0.4%. Thus, it is shown that the photodiode, namely its reverse (dark) current, can be a source of entropy for generating random numbers.

Keywords. *Software engineering, cybersecurity, photodiode, dark current, random numbers*

Стаття надійшла до редакції / Received 16.07.2025
Прийнята до друку / Accepted 15.08.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Одним з напрямків розвитку інформаційних технологій, з точки зору захисту інтересів людини, держави і суспільства в цілому є кібербезпека [1]. Методи генерації випадкових послідовностей є, в свою чергу, одним із визначальних компонентів кібербезпеки з точки зору програмної інженерії, а саме - забезпечення безпеки вхідни х та вихідних потоків даних. Оскільки процесори не здатні до самостійної генерації випадкових числових послідовностей, їм, для виконання такої задачі, потрібна програмна допомога. Відомі різні методи генерації. Зокрема, комп'ютер використовує обсяг стекової/купної пам'яті, або використовує поточне значення часу, що вимірюється в наносекундах (час Unix) в якості випадкового значення, з якого формується відповідна послідовність. Можна застосовувати дані з зовнішніх пристроїв. Наприклад, миша, USB, клавіатура, інші джерела. Вони усі називаються джерелами ентропії (хаосу). Слід зауважити, що ці значення, самі по собі, не є випадковими повністю. Вони знаходяться у певних мажах, або мають коливання, які можна передбачити. Для перетворення таких чисел на дійсні випадкові числа у потрібному діапазоні, до цих чисел можна застосувати криптографічні перетворення. Наприклад такі, що притаманні клітинними автоматами [4-5], для отримання рівномірно розподілених випадкових значень, які мають нерівномірно розподілені значення джерела ентропії. Такі значення називають псевдовипадковими. Тому, що вони генеруються детерміновано з ентропії, а не є насправді випадковими.

Зрозуміло, що джерело ентропії (хаосу) можна використати для генерації випадкових числових послідовностей. Це забезпечує певну унікальність і, що головне, непередбачуваність значень. Такі псевдовипадкові числові послідовності застосовуються в різноманітних мережах для забезпечення ефективних та безпечних з'єднань, генерації криптографічних ключів, моніторингу цілісності, а також багатьох інших напрямках [6].

Тому створення надійних, безпечних протоколів, які базуються на генерації зовні непередбачувані псевдовипадкові числових послідовностях є актуальним завданням сучасної програмної інженерії та кібербезпеки.

Аналіз досліджень та публікацій

Існуючи генератори, які створюють програмне забезпечення, є досить передбачуваними [7]. Друга вада існуючих методів генерації псевдовипадкових послідовностей, полягає у їх загальнодоступності. Наприклад, генерації, створені мовою Java [8, 9], теоретично, можуть бути умовно доступні для успішної атаки на алгоритм шифрування. Розвиток обчислювальних потужностей, зокрема квантові обчислення [10, 11], успішність атаки зростає до практичного рівня.

Загалом, для генерації випадкових чисел використовуються два основних методи. Один базується на розробці і використанні спеціалізованих пристроїв, які використовують певні фізичні джерела шуму [12, 13]. Такі пристрої вимагають додаткових адаптерів для використання з звичайними комп'ютерами.

Другий методичний підхід передбачає застосування також фізичних подій, але таких, що відбуваються у комп'ютерних пристроях. Він, очевидно, є більш доцільним.

Наочний приклад цього методу генерації випадкових чисел є застосування лічильника тактової частоти процесора. Але, цей метод чутливий до зовнішніх чинників, і, відповідно, до зовнішнього впливу на процес генерації випадкових чисел [14, 15]. У [16] пропонується генерація випадкової послідовності на основі оптичного маніпулятора миші. Такий метод надає можливість генерувати випадкові числа, які мають неоднорідний розподіл. Але, такий метод забезпечує швидкість генерації випадкової послідовності чисел лише 1 кбіт/с. Це обмежує його застосування у високошвидкісних системах шифрування.

Принципово новий підхід до генерації випадкової числової послідовності запропоновано у [17, 18]. Він полягає у використанні вебкамери, як джерело зовнішньої непередбачуванності, зокрема її статистичні, криптографічні та швидкістні характеристики. Виявлено, що значення інтенсивності пікселів вебкамери мають непередбачуванний характер, їх не видно неозброєним оком, але вони чітко фіксуються апаратно-програмними засобами. Оскільки вебкамери зазвичай побудовані на основі ПЗС матриць, створених на основі кремнію, нам здалося доцільним розглянути наступне питання. Чи можливе застосування в якості джерела випадкової числової послідовності не зображення, яке створює вебкамера, а, власне значення зворотного струму, наприклад, затемненого фотодіоду, створеного на основі кремнію. Подібні роботи проводилися раніше [19, 20], але в них, в якості джерела випадкової послідовності, розглядалися інші напівпровідникові вироби.

Цікавість до цього питання зумовлена тією обставиною, що зворотний струм фотодіоду, який працює у фотодіодному режимі, т.т. при електричному зміщення на p-n переході, є дійсно не передбачувана величина [21]. Зазвичай, при створення фотодіодів, або інших фоточутливих напівпровідникових приладів, нормується максимальна межа темнового струму при певному зміщення на p-n переході [22]. А точне значення постійно змінюється в певних межах. Це зумовлено і великою кількістю чинників, що впливають на генерацію зворотного (темнового) струму фотодіда. В першу чергу – величиною електричного змішення на p-n переході.

Формулювання цілей статті

Метою роботи є: вивчення доцільності застосування в якості джерела випадкової послідовності чисел величини зворотного струму фотодіода на основі кремнію, який працює у фотодіодному режимі.

Виклад основного матеріалу

Особливості генерації темнового струму фотодіода.

Темновий струм фотодіоду визначають при вимірювання вольт-амперної характеристики фотодіоду, в залежності від режиму роботи (фотодіодний, або фотогальванічний) та падаючої на нього оптичній потужності (Р). Ця характеристика, для наочності процесу, наведена на рис. 1 [23].

Величину темнового струму ФЧЕ ФД I_{Ti} у мікроамперах розраховують за формулою

$$I_{Ti} = \frac{U_{\text{ні}}}{R_{\text{ні}}}, \quad (1)$$

де $U_{ні}$ – спад напруги на опорі навантаження $R_{ні}$ і-того ФЧЕ, мВ, $R_{ні}$ – опір навантаження і-того ФЧЕ, кОм.

В загальному випадку темновий струм, що протікає через p-n перехід (I_t), визначається сумою дифузійного струму в нейтральній області (I_D) та генераційного в збідненій області (I_G) [24]:

$$I_t = I_D + I_G. \quad (2)$$

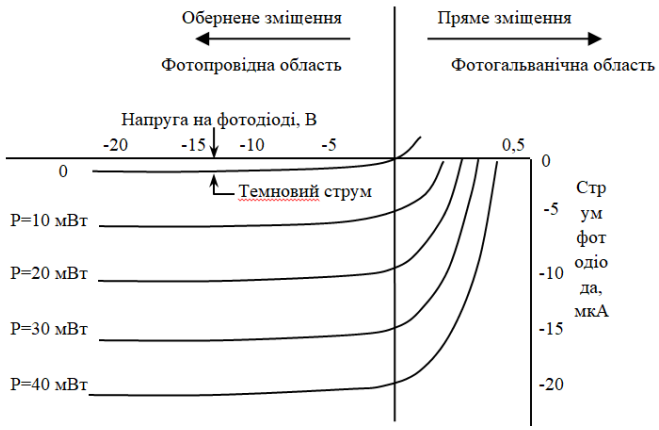

Рис. 1. Вольт-амперна характеристика фотодіоду, в залежності від режиму роботи та падаючої на нього оптичній потужності

Але, крім згаданих, загально відомих чинників що впливають на величину темнового струму, існує ще декілька, пов'язаних з особливістю технологічних процесів, за допомогою яких виготовляються сучасні кристали p-n кремнієвих фотодіодів.

1. Генерація носіїв струму на поверхні розподілу кремній – окисел кремнію, та в області виходу p-n переходу на поверхню кристалу (т.з. поверхнева складова I_t);

2. Генерація носіїв струму торцевою поверхнею кристалу;

3. Генерація носіїв струму на зворотному боці кристалу.

Іншими словами, вся зовнішня поверхня кристалу p-n фотодіоду може бути джерелом носіїв зворотного (темнового) струму. Всі ці згадані чинники генерують струм за межами розповсюдження збідненої області, але здатні досягати її за рахунок дрейфу .

Причиною поверхневих струмів є наявність інверсійних шарів поблизу поверхні розділу напівпровідник-діелектрик, які виникають внаслідок присутності фіксованого заряду в діелектрику. Ця границя виникає в наслідок термічних процесів, в ході яких формується p-n- перехід. Інверсійний шар збільшує площу p-n переходу, що в свою чергу приводить до збільшення темнового струму.

Джерелом носіїв струму, які здатні збільшувати темновий струм, може бути також і торцева поверхня кристалу фотодіода, яка утворюється під час вирізання топології фотодіоду з кремнієвої пластини [25].

Таким чином, з огляду на фізичні процеси, які зумовлюють величину темнового струму фотодіоду, він, темновий струм, може бути розглянутий як джерело генерації випадкової послідовності для створення відповідного генератора методами мікроелектроніки та програмної інженерії.

Блок-схема вимірювання темнового струму фотодіода наведена на рис. 2.

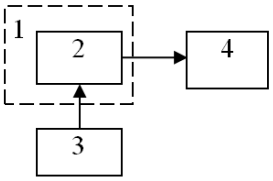

Рис. 2. Блок-схема установки для вимірювання темнового струму фотодіода.
1 – світлонепроникний екран; 2 – фотодіод; 3 – блок живлення; 4 – вольтметр постійного струму

Як видно з рисунку 2, блок-схема для вимірювання темнового струму досить проста. Основна вимога до неї - забезпечення відсутності будь-якої засвітки ФД.

Опис методу дослідження темнового струму для створення хаотичної числової послідовності**.**

Задача одержання цифрового сигналу у комп'ютер з аналогового джерела вирішена давно. Це може бути USB-адптер на базі Arduino (112593), або навіть лінійний аудіо-вхід мікрофона [26]. В нашому випадку використовувався кремнієвий фотодіод ФД-288.

Темновий струм генерується у деякому діапазоні 0 .. 10, мА, що відповідає напрузі 0..100 мВольт. Роздільна здатність Arduino складає 5 mV. Таким чином весь діапазон 0 .. 100 мВ можна розділити на 10 піддіапазонів, і кожен з них буде відповідати числу в діапазоні 0 … 10.

Методами програмної інженерії, зокрема мовою програмування Java версії 17, використовуючи бібліотеку javax-usb, величини виміряної напруги вводяться в комп'ютер через USB-порт і вікладаються у список у вигляді випадкових чисел [0..10]. 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.

На рис. 3. Приведена гістограма розподілення випадкових чисел по значенню.

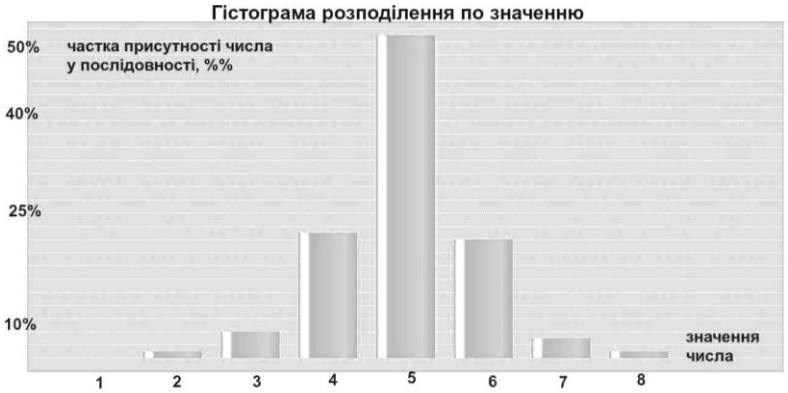

Рис. 3. Гістограма розподілення по значенню випадкових чисел, що одержані з ФД

На рис. 3 видно, що 50 % всіх чисел це п'ятірки, четвірки і шестірки взяли по 20 %, трійки - 4% і т.д. Розподіл носить нормальний (гаусівський) характер.

Таким чином одержаний ряд випадкових чисел у діапазоні [0 .. 9]. Швидкість генерації, або продуктивність (P) у такому випадку становитиме для Arduino: P = 980 байт/сек.

Проте криптографія вимагає випадкові числа у діапазоні [0 .. 255], що відповідає типу даних byte мови програмування Java.

Для забезпечення такого діапазону варто підсилити сигнал темнового струму до 5 Вольт (верхня межа Arduino). Таке підсилення добавить у вимірювану величину ще і теплового шуму. У цьому випадку вищенаведена характеристика більше зсунеться у сторону «рівномірно-хаотичної».

У цьому випадку роздільна здатність отриманого сигналу буде складати: 5.0 Вольт / 1024 = 5 мілівольт.

Таким чином вимір у діапазоні [0..5] мілівольт буде відповідати нульовому байту, а вимір у діапазоні [4.995..5.0] Вольт — 255-ому байту.

У нашому експерименті на протязі 100 сек було згенеровано послідовність випадкових чисел розміром у 98 кілобайт. На рис. 4 наведено гістограму розподілу по значенню випадкових чисел, що згенеровані за допомогою генерації темнового струму ФД.

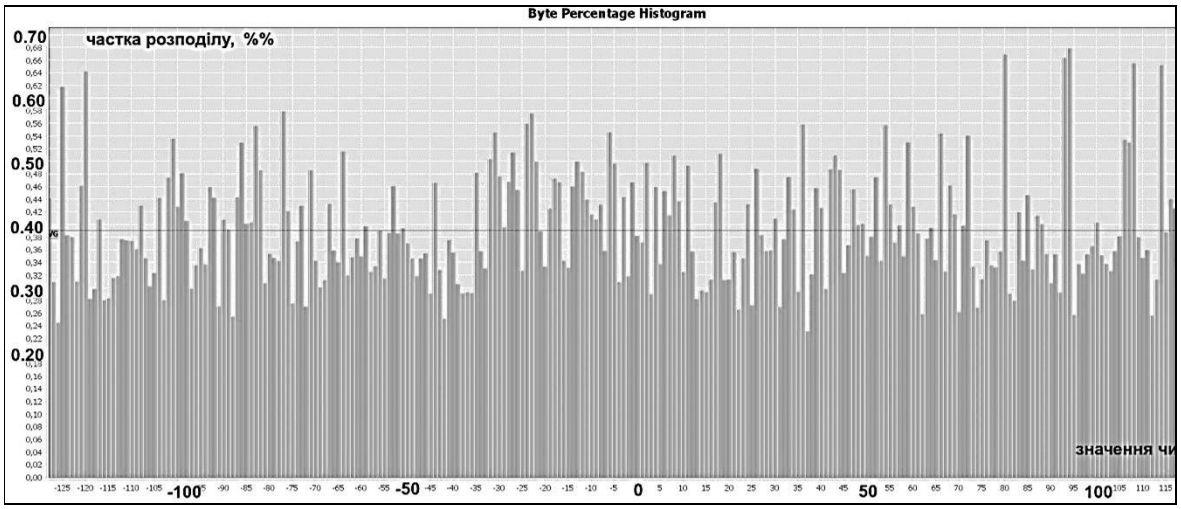

Рис. 4. Гістограма розподілу по значенню випадкових чисел , що згенеровані ФД

На гістограмі (рис. 4) видно, що підсилювач сигналу вніс свій додатковий хаос у процес генерації випадкових чисел. Тепер отриманий характер розподілу є рівномірно-хаотичний. Кожне число представлено приблизно рівномірно у діапазоні 0.3 — 0.7 %. Нагадаємо, що ідеальна частка для кожного числа 1/256 = 0.004, або 0.4%.

Проведено дослідження надійності генерації випадкової послідовності.

Конструкція запропонованого пристрою (блок-схема на рис. 2) містить серійний фотодіод, а вихідний сигнал з нього – динамічні зміни його темнового струму, в якості джерела ентропії, обробляється засобами DescriptiveStatistics. Фотодіод є серійним виробом. Його надійність підтверджується що найменше 1000 годинами безвідмовної роботи. Щодо DescriptiveStatistics, то надійність цього програмного продукту складає не менше 1000 годин безвідмовної роботи за оцінкою експертів.

Таким чином, запропонований метод генерації випадкової послідовності чисел за допомогою фотодіода в якості генератора такої послідовності, є досить надійним.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Вивчена доцільність застосування в якості джерела випадкової послідовності чисел зворотній (темновий) струму фотодіода на основі кремнію, який працює у фотодіодному режимі. Показано, що ФД може бути джерелом ентропії для генерації випадкових чисел. Такий розподіл є рівномірно-хаотичним і кожне число представлено приблизно рівномірно у діапазоні 0.3 — 0.7 %. Перспективою подальших досліджень є створення макетного пристрою для генерації випадкової послідовності з регульованим значенням хаотичності, яке би обиралось в залежності від потрібного рівня криптозахисту.

Література

1. Указ президента України №37/2022 “Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України". URL: https://www.president.gov.ua/documents/372022-41289.

2. H. Fukś, “Four state deterministic cellular automaton rule emulating random diffusion,” In: Chopard, B., Bandini, S., Dennunzio, A., Arabi Haddad, M. (eds) Cellular Automata. ACRI 2022. Lecture Notes in Computer Science, vol. 13402, 2022. Springer, Cham. https://doi.org/10.1007/978-3-031-14926-9_13.

3. Dobrovolsky Y. Development of a hash algorithm based on cellular automata and chaos theory / Y. Dobrovolsky, D. Hanzhelo, M. Hanzhelo, D. Trembach, G. Prokhorov // Eastern-European Journal of Enterprise Technologies. 5/9 (113) 2021. P. 48-55. DOI: 10.15587/1729-4061.2021.242849.

4. A. Cicuttin, L. De Micco, M. L. Crespo, et al., “Looking for suitable rules for true random number generation with asynchronous cellular automata,” Nonlinear Dynamics, vol. 111, pp. 2711-2722, 2022. https://doi.org/10.1007/s11071-022-07957-8.

5. L. Li, Y. Luo, S. Qiu, et al., “Image encryption using chaotic map and cellular automata,” Multimed Tools Appl, vol. 81, pp. 40755–40773, 2022. https://doi.org/10.1007/s11042-022-12621-9.

6. Asia Othman Aljahdal, “Random Number Generators Survey” International Journal of Computer Science and Information Security (IJCSIS),Vol. 18, No. 10, October 2020 https://doi.org/10.5281/zenodo.4249406.

7. Florette Martinez. Attacks on Pseudo Random Number Generators Hiding a Linear Structure. Cryptographers’ Track at the RSA Conference 2022, Mar 2022, Virtual Event, United States. pp.145-168, ⟨10.1007/978-3-030-95312-6_7⟩. ⟨hal-03737675⟩.

8. Class SecureRandom. All Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html.

9. M. Cornejo, S. Ruhault, “(In)Security of Java SecureRandom Implementations”, Journées Codage et Cryptographie, 2014.

10. Остапов С.Е., Добровольський Ю.Г. Квантова інформатика та квантові обчислення / С.Е.Остапов. Ю.Г. Добровольський - Чернівці: ЧНУ, 2021. - 99 с.

11. Jacak, J.E., Jacak, W.A., Donderowicz, W.A. *et al.* Quantum random number generators with entanglement for public randomness testing. *Sci Rep* **10**, 164 (2020). https://doi.org/10.1038/s41598-019-56706-2.

12. Seongmo Park, Byoung Gun Choi, Taewook Kang, Kyunghwan Park, Youngsu Kwon, Jongbum Kim, “Efficient hardware implementation and analysis of true random-number generator based on beta source.” ETRI Volume 42, Issue4 ,Special Issue on SoC and AI processors, August 2020, Pages 518-526, https://doi.org/10.4218/etrij.2020-0083.

13. Barannik, V., Sidchenko, S., Barannik, N., & Khimenko, A. (2021). The method of masking overhead compaction in video compression systems. *Radioelectronic and Computer Systems*, (2), 51-63. doi:https://doi.org/10.32620/reks.2021.2.05.

14. Agata KAŹMIERCZYK, Andrzej Ł. CHOJNACKI, Kornelia BANASIK (2022). Pseudorandom number generators as applied in reliability analysis. Kielce University of Technology, Faculty of Electrical Engineering, Automatic Control and Computer Science, Department of Power Engineering, Power Electronics and Electrical Machines, doi:10.15199/48.2022.12.44.

15. Barannik, V., Barannik, N., Ignatiev, O., & Khimenko, V. (2021). Method of indirect hiding of information in the process of compressing video images. *Radioelectronic and Computer Systems*,(4), 119-131. doi:https://doi.org/10.32620/reks.2021.4.10].

16. Ostapov, S., Diakonenko, B., Fylypiuk, M., Hazdiuk, K., Shumyliak, L., & Tarnovetska, O. (2023). Symmetrical Cryptosystems based on Cellular Automata. International Journal of Computing, 22(1), 15-20. https://doi.org/10.47839/ijc.22.1.2874.

17. R. Diachuk, Y. Dobrovolsky, D. Hanzhelo, H. Prokhorov, and D. Trembach, “Research the Level of Chaotic and Reliability in Webcam-generated Random Number Sequences”, *SISIOT*, vol. 2, no. 1, p. 01004, Aug. 2024, doi: 10.31861/sisiot2024.1.01004.

18. Yurii Dobrovolsky and Gregory Prokhorov "Primary processing of an optical image on autonomous mobile optical systems using cellular automata", Proceedings Proc. SPIE 12938, Sixteenth International Conference on Correlation Optics, 129380K (5 January 2024); https://doi.org/10.1117/12.3009624.

19. Soorat R., Ashok M. K. VudayagiriHardware Random number Generator for cryptography // arXiv, 2015. https://doi.org/10.48550/arXiv.1510.01234.

20. R. Soorat M. Kandukuri A. Vudayagiri Hardware Random number Generator for cryptography // Nanosystems Physics Chemistry Mathematics. October 2015. DOI: 10.17586/2220-8054-2017-8-5-600-605.

21. Antoni Rogalski. Infrared and Terahertz Detectors, Third Edition Published June 13, 2022 by CRC Press, 1066 Pages. https://www.routledge.com/Infrared-and-Terahertz-Detectors-Third-Edition/Rogalski/p/book/9781032338668#top.

22. Dobrovolsky Yu.G. Photodiode on the basis of epitaxial phosphate gallium with increased sensitivity at a wavelength of 254 nm / Yu.G. Dobrovolsky, V.M. Lipka, V.V. Strebezhev, Yu.O. Sorokatyi, M.O. Sorokatyi, O.P.Andreeva // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. - №1. – 2020. – p.36-39 scopus **DOI:** https://doi.org/10.35784/iapgos.910 https://e-iapgos.pl/resources/html/articlesList?issueId=12149.

23. Новітня техніка і технології: Навчальний посібник. Укл.: Ю.Г. Добровольський, І.С. Романюк. Чернівці: Чернівецький національний університет, 2021. 232с. ISBN 978-966-423-612-3.

24. Sze S. M., NgK. K.: Physics of Semiconductor Devices. 3rd Edition. John Wiley & Sons Inc., New Jersey 2006.

25. p-i-n Photodiode Based on Silicon with Short Rise Time. Yu.G. Dobrovolsky, O.P. Andreeva, M.S. Gavrilyak, L.J. Pidkamin, G.V. Prokhorov, JOURNAL OF NANO- AND ELECTRONIC PHYSICS. Vol. 10 No 4, 04019(5pp) (2018). http://dx.doi.org/10.21272/jnep.10(4).04019.

26. Г.В. Прохоров, В.Г. Прохоров, Ю.Г. Добровольський. Аналогово-частотний перетворювач для введення даних в комп'ютер // Науковий вісник Чернівецького університету. Комп'ютерні системи та компоненти. 2011. Т. 2. Вип. 1.- С.101-105.

References

1. Ukaz prezydenta Ukrainy №37/2022 "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 30 hrudnia 2021 roku "Pro Plan realizatsii Stratehii kiberbezpeky Ukrainy". URL: https://www.president.gov.ua/documents/372022-41289.

2. H. Fukś, "Four state deterministic cellular automaton rule emulating random diffusion," In: Chopard, B., Bandini, S., Dennunzio, A., Arabi Haddad, M. (eds) Cellular Automata. ACRI 2022. Lecture Notes in Computer Science, vol. 13402, 2022. Springer, Cham. https://doi.org/10.1007/978-3-031-14926-9_13.

3. Dobrovolsky Y. Development of a hash algorithm based on cellular automata and chaos theory / Y. Dobrovolsky, D. Hanzhelo, M. Hanzhelo, D. Trembach, G. Prokhorov // Eastern-European Journal of Enterprise Technologies. 5/9 (113) 2021. P. 48-55. DOI: 10.15587/1729-4061.2021.242849.

4. A. Cicuttin, L. De Micco, M. L. Crespo, et al., "Looking for suitable rules for true random number generation with asynchronous cellular automata," Nonlinear Dynamics, vol. 111, pp. 2711-2722, 2022. https://doi.org/10.1007/s11071-022-07957-8.

5. L. Li, Y. Luo, S. Qiu, et al., "Image encryption using chaotic map and cellular automata," Multimed Tools Appl, vol. 81, pp. 40755–40773, 2022. https://doi.org/10.1007/s11042-022-12621-9.

6. Asia Othman Aljahdal, "Random Number Generators Survey" International Journal of Computer Science and Information Security (IJCSIS),Vol. 18, No. 10, October 2020 https://doi.org/10.5281/zenodo.4249406.

7. Florette Martinez. Attacks on Pseudo Random Number Generators Hiding a Linear Structure. Cryptographers' Track at the RSA Conference 2022, Mar 2022, Virtual Event, United States. pp.145-168, (10.1007/978-3-030-95312-6_7). (hal-03737675).

8. Class SecureRandom. All Implemented Interfaces. URL: https://docs.oracle.com/javase/8/docs/api/java/security/SecureRandom.html.

9. M. Cornejo, S. Ruhault, "(In)Security of Java SecureRandom Implementations", Journées Codage et Cryptographie, 2014.

10. Ostapov S.E., Dobrovolskyi Yu.H. Kvantova informatyka ta kvantovi obchyslennia / S.E.Ostapov. Yu.H. Dobrovolskyi - Chernivtsi: ChNU, 2021. - 99 s.

11. 11. Jacak, J.E., Jacak, W.A., Donderowicz, W.A. *et al*. Quantum random number generators with entanglement for public randomness testing. *Sci Rep* 10, 164 (2020). https://doi.org/10.1038/s41598-019-56706-2.

12. Seongmo Park, Byoung Gun Choi, Taewook Kang, Kyunghwan Park, Youngsu Kwon, Jongbum Kim, "Efficient hardware implementation and analysis of true random-number generator based on beta source." ETRI Volume 42, Issue4 ,Special Issue on SoC and AI processors, August 2020, Pages 518-526, https://doi.org/10.4218/etrij.2020-0083.

13. Barannik, V., Sidchenko, S., Barannik, N., & Khimenko, A. (2021). The method of masking overhead compaction in video compression systems. *Radioelectronic and Computer Systems*, (2), 51-63. doi:https://doi.org/10.32620/reks.2021.2.05.

14. Agata KAŹMIERCZYK, Andrzej Ł. CHOJNACKI, Kornelia BANASIK (2022). Pseudorandom number generators as applied in reliability analysis. Kielce University of Technology, Faculty of Electrical Engineering, Automatic Control and Computer Science, Department of Power Engineering, Power Electronics and Electrical Machines, doi:10.15199/48.2022.12.44.

15. Barannik, V., Barannik, N., Ignatiev, O., & Khimenko, V. (2021). Method of indirect hiding of information in the process of compressing video images. *Radioelectronic and Computer Systems*,(4), 119-131. doi:https://doi.org/10.32620/reks.2021.4.10.

16. Ostapov, S., Diakonenko, B., Fylypiuk, M., Hazdiuk, K., Shumyliak, L., & Tarnovetska, O. (2023). Symmetrical Cryptosystems based on Cellular Automata. International Journal of Computing, 22(1), 15-20. https://doi.org/10.47839/ijc.22.1.2874.

17. R. Diachuk, Y. Dobrovolsky, D. Hanzhelo, H. Prokhorov, and D. Trembach, "Research the Level of Chaotic and Reliability in Webcam-generated Random Number Sequences", *SISIOT*, vol. 2, no. 1, p. 01004, Aug. 2024, doi: 10.31861/sisiot2024.1.01004.

18. Yurii Dobrovolsky and Gregory Prokhorov "Primary processing of an optical image on autonomous mobile optical systems using cellular automata", Proceedings Proc. SPIE 12938, Sixteenth International Conference on Correlation Optics, 129380K (5 January 2024); https://doi.org/10.1117/12.3009624.

19. Soorat R., Ashok M. K. VudayagiriHardware Random number Generator for cryptography // arXiv, 2015. https://doi.org/10.48550/arXiv.1510.01234.

20. R. Soorat M. Kandukuri A. Vudayagiri Hardware Random number Generator for cryptography // Nanosystems Physics Chemistry Mathematics. October 2015. DOI: 10.17586/2220-8054-2017-8-5-600-605.

21. Antoni Rogalski. Infrared and Terahertz Detectors, Third Edition Published June 13, 2022 by CRC Press, 1066 Pages. https://www.routledge.com/Infrared-and-Terahertz-Detectors-Third-Edition/Rogalski/p/book/9781032338668#top.

22. Dobrovolsky Yu.G. Photodiode on the basis of epitaxial phosphate gallium with increased sensitivity at a wavelength of 254 nm / Yu.G. Dobrovolsky, V.M. Lipka, V.V. Strebezhev, Yu.O. Sorokatyi, M.O. Sorokatyi, O.P.Andreeva // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska. - №1. – 2020. – p.36-39 scopus **DOI:** https://doi.org/10.35784/iapgos.910 https://e-iapgos.pl/resources/html/articlesList?issueId=12149.

23. Novitnia tekhnika i tekhnolohii: Navchalnyi posibnyk. Ukl.: Yu.H. Dobrovolskyi, I.S. Romaniuk. Chernivtsi: Chernivetskyi natsionalnyi universytet, 2021. 232s. ISBN 978-966-423-612-3.

24. Sze S. M., NgK. K.: Physics of Semiconductor Devices. 3rd Edition. John Wiley & Sons Inc., New Jersey 2006.

25. p-i-n Photodiode Based on Silicon with Short Rise Time. Yu.G. Dobrovolsky, O.P. Andreeva, M.S. Gavrilyak, L.J. Pidkamin, G.V. Prokhorov, JOURNAL OF NANO- AND ELECTRONIC PHYSICS. Vol. 10 No 4, 04019(5pp) (2018). http://dx.doi.org/10.21272/jnep.10(4).04019.

26. H.V. Prokhorov, V.H. Prokhorov, Yu.H. Dobrovolskyi. Analohovo-chastotnyi peretvoriuvach dlia vvedennia danykh v kompiuter // Naukovyi visnyk Chernivetskoho universytetu. Kompiuterni systemy ta komponenty. 2011. T. 2. Vyp. 1.- S.101-105.