

ПОВІДОМЛЕННЯ

про утворення разової спеціалізованої вченої ради

Заклад освіти/наукова
установа

Чернівецький національний університет імені Юрія Федьковича
(ідентифікаційний код 02071240)

1. Здобувач ступеня доктора філософії

1.1. ПІБ здобувача ступеня доктора філософії	Дячук Ростислав Любомирович
1.2. Стать здобувача	Чоловіча
1.3. Освітньо-наукова програма, яку завершує здобувач	38613 Інженерія програмного забезпечення (121 Інженерія програмного забезпечення)
1.4. Дата початку підготовки за ОНП	15.09.2022
1.5. Дата завершення підготовки за ОНП	27.02.2026
1.6. Дата завершення навчання на попередньому освітньому рівні	31.12.2020
1.7. Окремі елементи освітньо-наукової програми забезпечуються іншим закладом вищої освіти/ науковою установою (у тому числі іноземним)	ні

2. Дисертація

2.1. Тема дисертації	Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел
2.2. Анотація дисертації	<p>Дячук Р.Л. Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел. – Кваліфікаційна наукова праця на правах рукопису.</p> <p>Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 121 – «Інженерія програмного забезпечення» – Чернівецький національний університет імені Юрія Федьковича, Чернівці, 2026.</p> <p>Дисертаційна робота присвячена створенню та дослідженню інформаційної системи для генерування високоентропійної послідовності випадкових чисел (ПВЧ) на основі сучасних технологій та методів програмної інженерії, а також використання фотоелектричних явищ в якості джерела ентропії. Створена інформаційна система і її програмне забезпечення побудована на основі технології екстракції хаосу з стохастичних фізичних явищ, а саме – інтенсивності пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темного струму фотодіода з високою квантовою ефективністю. Отримані послідовності випадкових чисел також можуть оброблятися за допомогою клітинних автоматів, що суттєво збільшує рівень хаотичності випадкової послідовності. Створені генератори випадкових</p>

послідовностей, на відміну від існуючих, є простими, доступними, високопродуктивними, здатними до гнучкого налаштування. Інформаційна система загалом містить аналітичний інтелектуальний модуль спрощеної статистичної оцінки послідовності випадкових чисел, згенерованих вбудованими в неї генераторів, відрізняється високим рівнем криптостійкості, сприяє ефективному шифруванню та кодуванню для мінімізації кіберзагроз.

Проведено порівняльне дослідження статистичних і робочих характеристик аналогічних відомих генераторів ПВЧ, яке показало перевагу створеної інформаційної системи за рядом показників. А саме: за швидкістю генерації послідовності випадкових чисел, високим рівнем недетермінованої ентропії, гнучким налаштуванням, відкритим дизайном та швидкою пост обробкою. Створена інформаційна система має базові внутрішні перевірки, здатна регулювати співвідношення якості та швидкості вихідного потоку та ефективну пост обробку за допомогою клітинних автоматів. Окрім того новостворена система має відкритість апаратури та програмного забезпечення Open-hardware та open-source (GPLv3) в тому числі для застосування у нейронних мережах. Також, для роботи з крипто-примітивами на основі клітинних автоматів створено бібліотеку на мові програмування Java. Запропоновано і експериментально доведено високу якість, що генерується клітинними автоматами хаотичного типу (правила 30, 90, 105). Оптимізовано високу продуктивності і низьку ресурсоемності функціоналу на клітинних автоматах. Забезпечено неперервну генерацію послідовності випадкових чисел заданої продуктивності та якості.

Результати роботи є підґрунтям для подальших теоретичних і практичних наукових розробок із досліджень проблематики теорії генерації ПВЧ.

Дисертація складається зі вступу, чотирьох розділів, висновків, переліку використаних джерел та чотирьох додатків. У вступі обґрунтовано актуальність теми дослідження, сформульовано мету, завдання, предмет, об'єкт та методи дослідження, вказано наукову новизну, теоретичне та практичне значення отриманих результатів, подано та проаналізовано зв'язок роботи з науковими темами. Зазначено особистий внесок здобувача, а також наведено відомості про апробацію та публікації основних результатів дисертації. Описано структуру та обсяг дисертаційної роботи. Перший розділ містить ключові відомості з теорії генерації високоентропійних ПВЧ, а також відомості про апаратні генератори ПВЧ в системах інформаційної безпеки, зокрема у криптобезпеці та крипто-кодуванні. Розглянуто різні підходи до джерела ентропії та програмно-конструкторського оточення. Проаналізовано їх значення у системах на основі криптокодових та шифрувальних конструкцій та показані сильні сторони і вузькі місця з точки зору ціни, складності, надійності, довіри, продуктивності, керованості, моніторингу і ліцензування. Розглянуто теоретичні основи оцінювання випадковості та ентропії, а також проведено порівняльний аналіз сучасних найбільш відомих генераторів ПВЧ в системах криптобезпеки.

Обґрунтовано доцільність дослідження фото-електричних явищ (ФЕЯ) та квантових як джерела ентропії для генерації ПВЧ. Така конструкція дозволить частково зменшити недоліки, які притаманні

системам, що вже існують.

На основі проведеного дослідження сформовані завдання дослідження.

У другому розділі дисертаційного дослідження описано дослідження інтенсивності пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темного струму фотодіода з високою квантовою ефективністю як природних джерел для генерації послідовності випадкових чисел. Показано, що послідовність випадкових чисел, згенерована на основі інтенсивності пікселів зображення відеокамери має непередбачуваний характер і продуктивність від 85 Мбіт/сек до 288 Мбіт/сек, в залежності роздільної здатності відеокамери. Але, така послідовність випадкових чисел не відповідає вимогам стандартів NIST. Послідовність випадкових чисел, згенерована на основі фотоструму фотодіода з високою квантовою ефективністю є непередбачуваною, а її продуктивність досягає 2 Мбіт/сек. Такі послідовності випадкових чисел, частково відповідають тестам NIST. Послідовності випадкових чисел, створені за допомогою генератора на основі темного струму фотодіода, має абсолютно непередбачуваний характер і продуктивність до 980 Мбіт/сек, яка може бути збільшена при застосування високочастотної апаратної частини. Такий генератор може використовуватись для затравки (вектора ініціалізації) гібридних генераторів випадкових послідовностей.

Проведено дослідження гібридного генератора послідовностей випадкових чисел, який поєднує у собі генератор на основі відео, або веб-камери і клітинних автоматів. Таке поєднання вирішує питання по швидкодії, надійності, контрольованості, відповідності статистичним вимогам та вимогам до безпеки і стабільності пост-обробки. Також програмна частина гібридного генератора відкриває теоретично необмежені можливості по масштабованості та паралелізації процесу генерації, а також машинного навчання за допомогою нейронної мережи.

Третій розділ присвячено створенню інформаційної системи генерування послідовності випадкових чисел на основі усіх трьох генераторів із обробкою отриманих послідовності випадкових чисел за допомогою клітинних автоматів. Таке об'єднання повністю вирішуватиме питання про непередбачуваність, хаотичність, криптостійкість та ізольованість згенерованих послідовностей. Інтерфейс інформаційної системи дозволяє керувати параметрами генерації числових послідовностей, а саме: обирати джерело послідовностей випадкових чисел (база даних, файл, на основі відео-, або веб-камери, фото- та темного струму фотодіода з високою квантовою ефективністю, гібридного з обробкою числових послідовностей за допомогою клітинних автоматів); обирати між різними діапазонами значень (біти 0-1, стандартний діапазон 1-256, або користувацький діапазон); регулювати баланс між швидкістю генерації та рівнем безпеки, який забезпечує згенерована послідовність випадкових чисел, зберігати її та аналізувати. Продуктивність інформаційної системи лежить у межах 0,980 - 288 Мбіт/с і може бути суттєво збільшена при використанні високочастотної апаратної частини. Також система передбачає можливість масштабувати всю програмну частину генератора, або ж розпаралелити процес обробки «сирої» числової послідовності всередині блоку програмної частини. Що, на прикладі послідовності

випадкових чисел, згенерованої на основі відео-зображення, або веб-камери, дозволило підвищити продуктивність у 4 рази.

У четвертому розділі висвітлено результати застосування розробленої інформаційної системи при формуванні вхідного вектора для хеш-функції, для стеганографічних систем із підвищеними вимогами до прихованості та стійкості, а також для формування криптографічних ключів із високим рівнем ентропії та криптостійкості. Результати роботи, а саме удосконалений алгоритм створення хеш-функції, стеганографічні алгоритми та алгоритми генерації криптографічних ключів за допомогою розробленої інформаційної системи генерації послідовностей випадкових чисел, впроваджені та використовуються у ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» для підвищення криптостійкості програмного забезпечення. У висновках підсумовано основні результати дисертаційного дослідження.

У додатках подано наукові публікації, в яких відображено основні наукові результати роботи, відомості про апробацію результатів дисертації, акти та довідки про впровадження результатів роботи, лістинг частини коду програми.

Теоретичне значення. Результати теоретичних досліджень, а саме методологію екстракції хаосу з таких стохастичних фізичних явищ як інтенсивність пікселів з зображення веб-камери, фото- та темновий струм фотодіода, а також методологія використання клітинних автоматів для забезпечення високої якості хаотичності та оптимізація високої продуктивності і низької ресурсоемності функціоналу можуть застосовуватись для досліджень у галузі програмної інженерії, а також у навчальних курсах кафедри програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича (та інших ЗВО), пов'язаних з криптозахистом, методичних розробках, навчальних посібниках, які застосовуються в освітньому процесі і науково-дослідній роботі студентів та аспірантів.

Практичне значення. Розроблені у дисертаційній роботі інформаційна

система для генерації послідовностей випадкових чисел може в подальшому використовуватися для практичної реалізації.

Запропоновані підходи до генерації вхідного вектора хеш-функцій із використанням клітинних автоматів та послідовностей випадкових чисел, стеганографічні алгоритми та алгоритми генерації криптографічних ключів, використовуються у компанії ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» – для розробки власного програмного забезпечення підвищеної криптостійкості.

2.3. Ключові слова дисертації програмне забезпечення, випадкові числа, джерела ентропії, хаотична система, кібербезпека, крипто-кодування, інформаційна система, шифрування, генератор, відеокамера, зображення, фотодіод, квантова ефективність, хеш-функція, нейромережа

2.4. Посилання, за яким розміщено текст дисертації на сайті ЗВО <https://archer.chnu.edu.ua/xmlui/handle/123456789/14285>

2.7. Публікації здобувача, зараховані за темою дисертації

Diachuk R., Dmytrashchuk K., Mazurets A., Prokhorov H., Yanushevskiy S. Photosensitive matrix as a source of entropy. Proceedings of SPIE - The International Society for Optical Engineering. 2025. Vol. 13813, Seventeenth International Conference on Correlation Optics. 138132C. (Scopus).

Рік	2025
Ключові слова	cybersecurity, information system, photodiode, random numbers sequences, Software engineering
DOI	10.1117/12.3092587
ISSN	0277-786X
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/105025421860?origin=resultslist

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. 01004.

Рік	2024
Ключові слова	software engineering, chaos, crypto-resistance, software reliability, random number generator
DOI	10.31861/sisiot2024.1.01004
ISSN	-
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://journals.chnu.edu.ua/sisiot/article/view/571

Добровольський Ю., Дячук, Р. Дослідження зворотного струму фотодіода для генерації надійної випадкової послідовності чисел. Вісник Хмельницького національного університету. Серія: Технічні науки. 2025. Т. 357, № 5.1. С. 126-132

Рік	2025
Ключові слова	Програмна інженерія, кібербезпека, фотодіод, темновий струм, випадкові числа
DOI	10.31891/2307-5732-2025-357-15
ISSN	-
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/2062

Prokhorov H., Hanzhelo M., Diyachuk R., Yanushevskiy S. Investigation of statistical characteristics of random number sequences generated by a webcam using cellular automata functionality and NIST patterns. Security of infocommunication systems and Internet of things. 2025. Vol 3, № 1. P. 01007.

Рік	2025
Ключові слова	software engineering, cybersecurity, random number sequences, webcam, cellular automata
DOI	10.31861/sisiot2025.1.01007
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://journals.chnu.edu.ua/sisiot/article/view/949

Добровольський Ю., Дячук Р. Дослідження генерації випадкової послідовності чисел на основі темногого струм фотодіода при різних температурах. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки. 2025. Т. 36 (75), № 4. Ч. 2. С. 119-126.

Рік	2025
Ключові слова	програмна інженерія, кібербезпека, фотодіод, темновий струм, випадкові числа
DOI	10.32782/2663-5941/2025.4.2/16
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.tech.vernadskyjournals.in.ua/journals/2025/4_2025/part_2/18.pdf

3. Захист

3.1. Посилання, за яким здійснюватиметься онлайн-трансляція захисту <https://www.youtube.com/channel/UC7PNEvK5g8CET3dTxA-x0yQ>

4. Разова рада

4.1. Дата рішення Вченої ради про утворення разової ради 27.04.2026

4.2. Дата наказу про введення у дію рішення Вченої ради про утворення разової ради 28.04.2026

Голова разової ради

ПІБ	Баловсяк Сергій Васильович
Місце роботи	Чернівецький національний університет імені Юрія Федьковича
Посада	доцент (Основне місце роботи)
Факультет або інший	Навчально-науковий інститут фізико-технічних та комп'ютерних

структурний підрозділ	наук
Науковий ступінь	Доктор наук, 05.13.05 Комп'ютерні системи та компоненти
Дата отримання диплома доктора філософії (кандидата наук)	-
ORCID	0000-0002-3253-9006

Публікації за тематикою дисертації

Balovskyak S., Odaiska Kh., Yakovenko O., Iakovlieva I. Adjusting the brightness and contrast parameters of digital video cameras using artificial neural networks. Proceedings of SPIE - The International Society for Optical Engineering: Sixteenth International Conference on Correlation Optics. 2024. Vol. 12938. P. 1293801 - 1293801-4. (Scopus).

Рік	2024
Ключові слова	artificial neural network, digital video camera, video camera adjusting
DOI	10.1117/12.3009429
ISSN	0277-786X
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85184145221?origin=resultslist

Hrynyk N., Balovskyak S., Branashkoa V., Dubovyka O., Odaiska Kh. Improving accuracy of photogrammetry method by masking images and using coordinates of video cameras. Proceedings of SPIE - The International Society for Optical Engineering: Seventeenth International Conference on Correlation Optics. 2025. Vol. 13813, P. 138130L- 138130L-7 (Scopus).

Рік	2025
Ключові слова	3D model, 3DF Zephyr, artificial neural networks, cloud platform, image segmentation, photogrammetry, software, YOLO
DOI	10.1117/12.3091445
ISSN	0277-786X
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/105025459592?origin=resultslist

Баловсяк С., Гнатюк Ю. Масштабування цифрових зображень у телекомунікаційній системі методами інтерполяції та за допомогою згорткових нейронних мереж. Вісник Хмельницького національного університету. Серія: технічні науки. 2025. Т. 357, №5.1. С. 31-38.

Рік	2025
Ключові слова	телекомунікаційні системи, масштабування цифрових зображень, згорткові нейронні мережі, методи інтерполяції, хмарні технології, програмне забезпечення

DOI	10.31891/2307-5732-2025-357-3
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/2055/1980

Рецензент

ПІБ	Шпатар Петро Михайлович
Місце роботи	Чернівецький національний університет імені Юрія Федьковича
Посада	Директор (Основне місце роботи)
Факультет або інший структурний підрозділ	Навчально-науковий інститут фізико-технічних та комп'ютерних наук
Науковий ступінь	Кандидат наук, 05.27.01 Твердотільна електроніка
Дата отримання диплома доктора філософії (кандидата наук)	11.10.2007
ORCID	0000-0003-4088-1458

Публікації за тематикою дисертації

Aleksieiev A., Prokofiev M., Shpatar P. A method of quantum communication using sideband-modulated infrared emission. Proceedings of SPIE - The International Society for Optical Engineering. 2024. Vol. 12938. P. 129380T-129380T-5 (Scopus).

Рік	2024
Ключові слова	laser, lateral frequencies, Photodiode, polarization
DOI	10.1117/12.3010050
ISSN	0277-786X
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85184140876?origin=resultslist

Гресь О., Галюк С., Круліковський О., Заяц Р., Ластівка Г., Шпатар П. Розроблення генераторів псевдовипадкових послідовностей на основі хеш-функцій з використанням багатовимірних хаотичних систем. Вимірювальна та обчислювальна техніка в технологічних процесах. 2024. №4. С. 362–371.

Рік	2024
Ключові слова	генератор, хеш-функція, хаотична система, статистичні тести
DOI	10.31891/2219-9365-2024-80-44
ISSN	–
Одноосібне авторство	ні

Містить державну таємницю / службову інформацію	ні
Посилання	https://vottp.khmnu.edu.ua/index.php/vottp/article/view/428/406
<p>Halyts R., Shpatar P., Yaremchuk Y. Amplification pulse signals a single-photon detector based on an avalanche photodiode. Proceedings of SPIE - The International Society for Optical Engineering. 2024. Vol. 12938. P. 129380K-129380S-5 (Scopus).</p>	
Рік	2024
Ключові слова	Avalanche photodiodes, laser, quantum efficiency, single-photon detector
DOI	10.1117/12.3010049
ISSN	0277-786X
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85184149521?origin=resultslst

Офіційний опонент

ПІБ	Бараннік Володимир Вікторович
Місце роботи	Харківський національний університет імені В.Н. Каразіна
Посада	професор з во (Основне місце роботи)
Факультет або інший структурний підрозділ	Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Науковий ступінь	Доктор наук, 05.12.02 Телекомунікаційні системи та мережі
Дата отримання диплома доктора філософії (кандидата наук)	–
ORCID	0000-0002-2848-4524

Публікації за тематикою дисертації

Barannik V., Sidchenko S., Barannik D., Yermachenkov A., Savchuk M., Pris G. Video images' compression method based on floating positional coding with an unequal codograms length. Radioelectronic and Computer Systems. 2023. No 1(101). P. 134-146. (Scopus).

Рік	2023
Ключові слова	authenticity, compression, confidentiality, encoding, encryption, image, lossless, video
DOI	10.32620/reks.2023.1.11
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні

Посилання	https://www.scopus.com/pages/publications/85176954041?origin=resultslist
<p>Бараннік В.В., Єлісеєв Е.С., Бабенко М.В., Цімура Ю.В., Худаєв О.В., Сіненко Д.В., Дубовик Г.В., Неминуший С.В., Онпченко П. М. Метод блочного кодування кластеризованих трансформант в спектрально-параметричному просторі = Method Local-Monotonic Determination Lengths of Binary Block Codes of Clustered Transformants. Вісник Національного технічного університету України «Київський політехнічний інститут»: Серія Радіотехніка, Радіоапаратобудування. 2024. №. 98. С. 13–22. (Web of Science)</p>	
Рік	2024
Ключові слова	відеозображення, спектрально-параметричний опис трансформант, якість відеозображень, локально-монотонне кодування, маркери блочних кодів, пікове відношення сигнал/шум
DOI	10.20535/RADAP.2024.98.13-22
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.webofscience.com/wos/woscc/full-record/WOS:001390813500002

Бараннік В.В., Сідченко С.О., Бараннік Д.В., Черномаз І.К., Гуржій П.М., Григор'ян М.Б. Метод зберігання елементів службових складових криптокомпресійних кодограм відеозображень = Saving Elements Methods for Service Components of Images Cryptocompression Codograms. Вісник Національного технічного університету України «Київський політехнічний інститут»: Серія Радіотехніка, Радіоапаратобудування. 2023. №. 92. С. 28–40. (Web of Science)

Рік	2023
Ключові слова	захист інформації, зображення, конфіденційність, криптокомпресія, стиснення, шифрування
DOI	10.20535/RADAP.2023.92.28-40
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.webofscience.com/wos/woscc/full-record/WOS:001058481800004

Офіційний опонент

ПІБ	Євсеєв Сергій Петрович
Місце роботи	Національний технічний університет "Харківський політехнічний інститут"
Посада	Завідувач кафедри (Основне місце роботи)
Факультет або інший структурний підрозділ	Навчально-науковий інститут комп'ютерних наук та інформаційних технологій
Науковий ступінь	Доктор наук, 21.05.01 Інформаційна безпека держави

Дата отримання диплома доктора філософії (кандидата наук)	-
ORCID	0000-0003-1647-6444

Публікації за тематикою дисертації

Yevseiev S., Rzayev K., Laptiev O., Hasanov R., Milov O., Asgarova B., Camalova J., Pohasii S. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European Journal of Enterprise Technologies. 2022. Vol. 5. No 9 (119). P. 6–16. (Scopus Q3 – <https://www.scimagojr.com/journalsearch.php?q=21100450083&tip=sid&clean=0>).

Рік	2022
Ключові слова	Cipher stability, Crypto-algorithm, Crypto-resistance, Entropy sources, Pseudo-random numbers, Random numbers, Uncertainty zone
DOI	10.15587/1729-4061.2022.265774
ISSN	-
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85141781206?origin=resultslist

Yevseiev S., Havrylova A., Milevskiy S., Sinitsyn I., Chalapko V., Dukin H., Hrebeniuk V., Diedov M., Bekirova L., Shpak O. Development of an improved SSL/TLS protocol using post-quantum algorithms. Eastern-European Journal of Enterprise Technologies. 2023. Vol. 3. No 9 (123). P.33–48. (Scopus Q3 – <https://www.scimagojr.com/journalsearch.php?q=21100450083&tip=sid&clean=0>).

Рік	2023
Ключові слова	algebraic geometric codes, flawed codes, improved SSL/TLS protocol, improved UMAC algorithm, post-quantum encryption algorithms
DOI	10.15587/1729-4061.2023.281795
ISSN	-
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85165404054?origin=resultslist

Pohasii S., Yevseiev S., Zhuchenko O., Milov O., Lysechko V., Kovalenko O., Kostyak M., Volkov A., Lezik A., Susukailo V. Development of crypto-code constructs based on LDPC codes. Eastern-European Journal of Enterprise Technologies. 2022. Vol. 2. No 9 (116). P. 44–59. (Scopus Q3 – <https://www.scimagojr.com/journalsearch.php?q=21100450083&tip=sid&clean=0>).

Рік	2022
Ключові слова	Crypto-code constructs, low-density parity-check codes, security concept
DOI	10.15587/1729-4061.2022.254545
ISSN	-

Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://www.scopus.com/pages/publications/85130069202?origin=resultslist

Офіційний опонент

ПІБ	Гарасимчук Олег Ігорович
Місце роботи	Національний університет "Львівська політехніка"
Посада	Доцент (Основне місце роботи)
Факультет або інший структурний підрозділ	Інститут комп'ютерних технологій, автоматики та метрології
Науковий ступінь	Кандидат наук, 05.13.05 Комп'ютерні системи та компоненти
Дата отримання диплома доктора філософії (кандидата наук)	17.01.2008
ORCID	0000-0002-8742-8872

Публікації за тематикою дисертації

Гарасимчук О.І., Войтусік С.С., Цебак О.А. Застосування генераторів псевдовипадкових чисел у машинному навчанні. Комп'ютерні системи та мережі. 2025. Вип. 7, № 1. С. 79–90.

Рік	2025
Ключові слова	генератори псевдовипадкових чисел, машинне навчання, ініціалізація нейронних мереж, стохастична оптимізація, відтворюваність
DOI	10.23939/csn2025.01.079
ISSN	–
Одноосібне авторство	ні
Містить державну таємницю / службову інформацію	ні
Посилання	https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38959/k250473-81-92_0.pdf

Хомік М.А., Гарасимчук О.І. Аналіз загроз для генераторів псевдовипадкових чисел і псевдовипадкових послідовностей та заходи захисту. Захист інформації. 2023. Т. 25. № 4. С. 172–184.

Рік	2023
Ключові слова	генератори псевдовипадкових чисел, генератори псевдовипадкових послідовностей, кібербезпека, генерування, вразливості, атаки, оцінювання якості
DOI	10.18372/2410-7840.25.18222
ISSN	–
Одноосібне авторство	ні
Містить державну	ні

таємницю / службову
інформацію

Посилання <https://jrn1.nau.edu.ua/index.php/ZI/article/view/18222>

Maksymovych V., Shabatura M., Harasymchuk O., Shevchuk R., Sawicki P., Zajac T. Combined Pseudo-Random Sequence Generator for Cybersecurity. Sensors. 2022. № 22. P. 9700. (Scopus, Q2 – <https://www.scimagojr.com/journalsearch.php?q=130124&tip=sid&clean=0>)

Рік 2022

Ключові слова authentication, encryption of information, pseudo-random number, pseudo-random sequence generators

DOI 10.3390/s22249700

ISSN 1424-8220

Одноосібне авторство ні

Містить державну
таємницю / службову
інформацію ні

Посилання <https://www.scopus.com/pages/publications/85144488213?origin=resultslist>

Підтвердження

Я підтверджую, що:

- я належним чином уповноважений/а закладом освіти/науковою установою на подання цього повідомлення, і за потреби надам документ, який підтверджує ці повноваження
- усі відомості, викладені у цьому повідомленні, є достовірними

Документ підписаний електронним підписом

ЯКУБОВСЬКА НАТАЛІЯ ОЛЕКСІЇВНА

29.04.2026