ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Дячука Ростислава Любомировича на тему:
“ Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел ”,
поданої на здобуття ступеня доктора філософії
за спеціальністю 121 – Інженерія програмного забезпечення
з галузі знань 12 – Інформаційні технології

1. Обґрунтування вибору теми дослідження та її зв’язок із планами наукових робіт Університету.

Суттєвою ознакою сучасного стану суспільства є створення, обробка, накопичення, передача та отримання величезних інформаційних потоків, які повинні мати достатній рівень кибербезпеки, бути захищені для забезпечення як приватності даних, власниками яких є звичайні громадяни, бізнес об’єднання та держави. З точки зору захисту інтересів людини, держави і суспільства в цілому одним з напрямків розвитку програмної інженерії згідно указу президента України №37/2022 “Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про План реалізації Стратегії кібербезпеки України", є створення алгоритмів та програмного забезпечення для кібербезпеки, яка, зокрема ґрунтується на генерації ПВЧ. Цей напрям програмної інженерії є одним із визначальних компонентів забезпечення кібербезпеки, а саме - забезпечення безпеки вхідних та вихідних потоків даних. Сучасні процесори не можуть самостійно генерувати ПВЧ достатнього рівня надійності, тому, для виконання такої задачі, їм потрібно відповідне програмне забезпечення. Результативні дослідження в цієї галузі сприяє кращому розумінню організації безпеки потоків даних шляхом шифрування та кодування. інтенсивності пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темнового струму фотодіода з високою квантовою ефективністю. З огляду на

існуючий математичний, алгоритмічний апарати та програмне забезпечення у галузі захисту інформації, залишається не до кінця зрозумілими цілий ряд питань, а саме: оптимальний вибір співвідношення між продуктивністю генерації ПВЧ і їх надійністю (стійкістю до зламу), ефективності застосування клітинних автоматів для підвищення рівня хаотичності ПВЧ, методики експрес діагностики рівня хаотичності згенерованих ПВЧ, пошук нових джерел ПВЧ, максимально наближених за своєю природою до дійсно хаотичної структури, совтрення вхідного вектора хеш-функції, тощо.

Зважаючи на вище наведене, розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел є актуальною задачею.

Мета і завдання дисертаційного дослідження. Метою дослідження є розробка інформаційної системи генерування високоентропійних послідовності випадкових чисел та оцінювання ступеня їх хаотичності на основі програмного забезпечення власної розробки та нових підходів для визначення балансу між продуктивністю на надійністю створених послідовності випадкових чисел.

.**Об’єкт дослідження.** Хаотичні системи, які забезпечують генерацію послідовності випадкових чисел.

Предмет дослідження. Моделі та методи для генерації високоентропійної послідовності випадкових чисел.

Методи дослідження. В основу дисертаційної роботи покладені методи інтелектуального аналізу даних, а саме: отримання та аналіз ПВЧ за допомогою технологій екстракції даних, обробки даних за допомогою КА хаотичного типу, спрощені методи оцінки статистичних характеристик ПВЧ.

Дисертаційне дослідження виконано відповідно до планів науково-дослідницьких робіт:

– кафедри програмного забезпечення комп’ютерних систем Чернівецького національного університету імені Юрія Федьковича за держбюджетною тематикою: «Дослідження, моделювання та розробка програмного забез-

печення складних динамічних систем» (Державний реєстраційний номер 0121U109232);

2. Формулювання наукового завдання, нове розв'язання якого отримано в дисертації.

Наукові завдання, розв'язання яких отримано у дисертації, полягають у наступному:

-провести аналітичний огляд існуючих програмних та апаратних засобів та методів генерації високоентропійних ПВЧ;

- розробити та дослідити технологію генерації ПВЧ з пікселів зображення фоточутливої матриці відео, або веб-камери;

- розробити та дослідити технологію генерації ПВЧ з фотоструму фотодіода;

- розробити та дослідити технологію генерації ПВЧ з темнового струму фотодіода;

- розробити та дослідити технологію гібридної генерації ПВЧ із застосуванням клітинних автоматів;

- розробити інформаційну систему для генерації ПВЧ на основі створених генераторів, в основу якої має бути покладено можливість обрання балансу між швидкість генерації ПВЧ та її надійністю, а також перевірку ПВЧ на відповідність критеріям хаотичності;

- провести порівняльні дослідження характеристик створеної інформаційної системи та відомих аналогів;

- запропонувати приклади застосування створеної інформаційної системи для синтезу криптографічних алгоритмів для хеш-функцій, стеганографії та криптографічних ключів на основі ПВЧ і КА;

3. Наукові положення, розроблені особисто дисертантом, та їх новизна. Дисертант особисто сформулював наукову ідею дослідження, розробив запропоновані методики, виконав їх програмну реалізацію, організував та провів експериментальні дослідження, здійснив обробку й аналіз

отриманих результатів, а також сформулював висновки та основні наукові положення :

Вперше:

- Запропоновано метод генерації ПВЧ, особливістю якого є використання фотоелектричних явищ, що, на відміну від існуючих методів, забезпечує швидкість генерації ПВЧ від 0,288 до 1 Гбіт/сек при високому рівні випадковості, є доступними, високопродуктивними, здатними для гнучкого налаштування, що дозволяє підвищити ефективність генерації ПВЧ;
- розроблено інформаційну систему екстракції ПВЧ з стохастичних фізичних явищ, а саме, інтенсивності пікселів зображення веб-камери, фото- та темнового струму фотодіода, яка, на відміну від аналогів, містить модуль обробки отриманих ПВЧ за допомогою технології КА та аналітичний модуль інтелектуальної спрощеної статистичної оцінки згенерованих ПВЧ, що дозволяє пройти перевірку 12 тестів NIST з 15 можливих;
- запропоновано метод балансу між продуктивністю та якістю генерації ПВЧ, яка на відміну від аналогів, може працювати у режимі неперервного потоку, що дозволяє у процесі генерації ПВЧ віддавати перевагу або швидкодії, або випадковості, що дозволяє керувати рівнем надійності згенерованої ПВЧ

Набуло подальшого розвитку:

- методика використання КА: створено бібліотеку на мові програмування Java по роботі з лінійними КА на основі примітивних побітових операцій низького рівня, запропоновано і експериментально доведено високу продуктивність, низьке ресурсоспоживання і високу якість генерації і обробки ПВЧ запропонованим функціоналом лінійних клітинних автоматів хаотичного типу (правила 30, 90, 105), що дозволило скоротити час обробки майже на порядок у порівнянні з парадигмою об’єктноорієнтованого програмування;

– оптимізація балансу між високою продуктивностю і низькою ресурсоємності функціоналу на КА; технологія генерації ПВЧ, що переходить на якісний рівень – неперервна генерація ПВЧ заданої продуктивності та якості

4. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій, які захищаються.

Достовірність наукових положень та висновків обґрунтовані тим, що для розробки програмного забезпечення використані сучасні методи та середовище розробки; програмне забезпечення протестоване стандартними методами тестування; отримані за допомогою розробленої інформаційної технології дані не суперечать загальноприйнятим міркуванням і принципам, а теоретичні положення, розроблені дисертантом із застосуванням добре апробованих теоретичних методів,

Дисертаційна робота є самостійним науковим дослідженням, що має завершений характер, цілісну структуру та логічну послідовність викладу матеріалу. Робота складається зі вступу, чотирьох розділів, висновків до розділів, загальних висновків, списку використаних джерел та чотирьох додатків. Усі наукові положення, що становлять новизну дослідження, розроблені автором особисто.

Повнота висвітлення результатів підтверджується 4 публікаціями у провідних наукових виданнях: (1 з яких – в журналі, що індексується у наукометричній базі SCOPUS, 4 – в українських фахових виданнях). А також ще 7 тез у збірниках матеріалів міжнародних та всеукраїнських наукових конференцій.

Апробація основних наукових результатів відбулася у формі доповідей та тез на 7 Всеукраїнських та Міжнародних наукових і науково-практичних конференціях.

5. Рівень теоретичної підготовки здобувача та рівень його обізнаності з результатами наукових досліджень інших науковців.

Здобувач володіє високим рівнем теоретичної та практичної підготовки в галузі інформаційних технологій, що забезпечує ефективне та системне вирішення складних наукових завдань. Він продемонстрував глибоку обізнаність із сучасними науковими досягненнями інших дослідників у межах теми дисертаційної роботи. Проведений ним аналіз наукової літератури дозволив істотно розширити розуміння актуальних тенденцій розвитку галузі та сприяв удосконаленню існуючих підходів для досягнення нових результатів.

Особистий внесок здобувача у розв'язання конкретних наукових завдань є суттєвим і визначальним. Зокрема:

- Дисертант брав безпосередню участь у постановці задач дослідження, виборі методів їх розв'язання, аналізі та інтерпретації отриманих результатів
- особисто розробив програмне забезпечення для генерації та дослідження випадкових послідовностей;
- самостійно провів серію експериментальних досліджень ентропійних джерел (фоточутливих матриць, темнового струму фотодіодів, відеопотоку вебкамер);
- самостійно дослідив можливі використання запропонованої інформаційної системи в криптографічних алгоритмахі

6. Наукове та практичне значення роботи.

Наукове значення дисертації полягає у розвитку методології екстракції хаосу з таких стохастичних фізичних явищ як інтенсивність пікселів з зображення веб-камери, фото- та темновий струм фотодіода, а також методології використання клітинних автоматів для забезпечення високої якості хаотичності та оптимізація високої продуктивності і низької ресурсоємності функціоналу, які можуть застосовуватись для досліджень у галузі програмної інженерії.

Практичне значення отриманих результатів підтверджується створенням інформаційної системи для генерації послідовностей випадкових чисел, яка може в подальшому використовуватися для практичної реалізації. Також були

запропоновані підходи до генерації вхідного вектора хеш-функцій із використанням клітинних автоматів та послідовностей випадкових чисел, стеганографічні алгоритми та алгоритми генерації криптографічних ключів.

7. Використання результатів роботи.

Запропонована автором інформаційна система використовуються у компанії ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» – для розробки власного програмного забезпечення підвищеної криптостійкості.

Теоретичні та практичні результати дисертаційного дослідження використовуються у навчальному процесі кафедр радіотехніки та інформаційної безпеки та програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича при викладанні дисциплін «Криптографічний захист інформації», «Безпека в цифровому просторі» та «Безпека програм та даних».

8. Повнота викладу матеріалів дисертації в публікаціях та особистий внесок здобувача в публікації, виконані у співавторстві.

За темою дисертації опубліковано 11 робіт, в яких подано результати досліджень. З них 4 статті у рецензованих виданнях (1 з яких – в журналі, що індексується у наукометричній базі SCOPUS, 4 – в українських фахових виданнях), у збірниках матеріалів міжнародних та всеукраїнських наукових конференцій – 7 робіт.

Дисертант брав безпосередню участь у постановці задач дослідження, виборі методів їх розв'язання, аналізі та інтерпретації отриманих результатів, а також у підготовці матеріалів до публікації в усіх працях [1–12]. Основний внесок здобувача полягає у розробці програмного забезпечення для генерації та дослідження випадкових послідовностей, проведенні експериментальних досліджень ентропійних джерел (фоточутливих матриць, темнового струму фотодіодів, відеопотоку вебкамер), статистичному аналізі отриманих послідовностей, зокрема із застосуванням клітинних автоматів та тестів NIST, а також у розробці та дослідженні алгоритмів і моделей генераторів випадкових

чисел. Результати досліджень [6–12] доповідались та обговорювались на міжнародних і всеукраїнських наукових та науково-практичних конференціях.

Результати перевірки тексту дисертації за допомогою антиплагіатної системи TURNITIN показали 4% схожості з джерелами з Інтернету, що підтверджує дотримання принципів академічної доброчесності та самостійність виконання наукової праці.

Результати дисертації повною мірою викладені в зазначених публікаціях.

Наукові праці, в яких опубліковані основні наукові результати дисертації

Наукові праці у періодичних наукових виданнях,

проіндексованих у наукометричних базах даних Scopus:

1. Diachuk R., Dmytrashchuk K., Mazurets A., Prokhorov H., Yanushevskyi S. Photosensitive matrix as a source of entropy. *Proceedings of SPIE.* 13813, Seventeenth International Conference on Correlation Optics. 2025. 138132C. ISSN:0277-786X (Scopus) (*Внесок авторів: Diachuk R. – програмна реалізація збору та обробки даних, експериментальні дослідження ентропійних характеристик, аналіз результатів, підготовка початкового варіанту статті; Dmytrashchuk K. – апаратна реалізація та налаштування фоточутливої матриці, збір експериментальних даних; Mazurets A. – аналіз літературних джерел, статистична обробка результатів; Prokhorov H. – методологія дослідження, формалізація моделі джерела ентропії; Yanushevskyi S. – концептуалізація, наукове керівництво, рецензування та редагування рукопису.)*

Наукові праці у виданнях, включених до переліку

наукових фахових видань України:

2. 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. (*Внесок авторів: Dobrovolsky Y. – концептуалізація; Prokhorov H. – методологія та дослідження, Diachuk R. – програмна розробка, та експеременти; Hanzhelo D. – статистичні дослідження; Trembach D. – концептуалізація та написання).*
3. Добровольський, Ю., Дячук, Р. Дослідження зворотного струму фотодіода для генерації надійної випадкової послідовності чисел. *Вісник Хмельницького національного університету. Серія: Технічні науки.* 2025. Том 357, № 5.1. С. 126-132. (*Внесок авторів: Добровольський Ю. – концептуалізація, методологія, аналіз результатів, редагування; Дячук Р. – аналіз джерел, програмна розробка, дослідження результатів та написання).*
4. Prokhorov H., Hanzhelo M., Diachuk R., Yanushevskyi 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. (*Внесок авторів: Prokhorov H. – концептуалізація, дослідження, нагляд; Hanzhelo M., Diachuk R. – програмне забезпечення, ресурси, підготовка початкового варіанту рукопису, візуалізація, валідація; Yanushevskyi S.– методологія, концептуалізація, рецензування та редагування рукопису, нагляд, дослідження).*
5. Добровольський Ю., Дячук Р. Дослідження генерації випадкової послідовності чисел на основі темнового струм фотодіода при різних

температурах. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2025. Том 36 (75), № 4. Частина 2. С. 119-126. (*Внесок авторів: Добровольський Ю. – концептуалізація, методологія, написання; Дячук Р. – аналіз джерел, програмна розробка, аналіз результатів та редагування).*

Наукові праці, які засвідчують апробацію матеріалів дисертації:

6. Дячук Р.Л., Павлюченко О.С., Прохоров П.А., Прохоров Г.В., Добровольський Ю.Г. Клітинні автомати як генератори Хаосу в криптографічних алгоритмах. Проблеми інформатики та комп'ютерної техніки : матеріали XI міжнар. наук.-практ. конф., м. Чернівці, 10–13 лист. 2022 р. Черн. нац. ун-т ім. Ю Федьковича, Чернівці, 2022. – С. 44-46. (*Внесок авторів: Дячук Р.Л. – концептуалізація, програмна реалізація моделі, експериментальні дослідження, написання рукопису; Павлюченко О.С. – аналіз літератури, дослідження параметрів клітинних автоматів; Прохоров П.А., Прохоров Г.В. – методологія, формалізація моделі, валідація результатів; Добровольський Ю.Г. – наукове керівництво, узагальнення результатів, редагування).*
7. Prokhorov G., Dobrovolsky Y., Dyachuk R. Hash-Function Algorithms Balanced on Reliability and Data Processing Speed. IEEE 4th International Conference on Advanced Trends in Information Theory, 15-16 December, 2022, Kyiv, UKRAINE. P.111-114. (Scopus). (*Внесок авторів: Prokhorov G. – концептуалізація, методологія, постановка задачі; Dobrovolsky Y. – аналіз надійності, редагування, наукове керівництво; Dyachuk R. – програмна реалізація алгоритмів, експериментальні дослідження швидкодії, візуалізація результатів, підготовка початкового варіанту статті).*
8. Дячук Р.Л., Добровольський Ю.Г. Алгоритм хеш-функції з підвищеною криптостійкістю. Покращення лавинного ефекту. Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXXI міжнар. наук.-практ. конф., MicroCAD-2023, 17-20 травня 2023. Харків: НТУ «ХПІ».

С. 1113. (*Внесок авторів: Дячук Р.Л. – розробка алгоритму, програмна реалізація, експериментальна перевірка лавинного ефекту, написання рукопису; Добровольський Ю.Г. – концептуалізація, аналіз криптостійкості, редагування, наукове керівництво).*

9. Дячук Р.Л., Комісарчук В.В., Прохоров П.А., Прохоров Г.В., Добровольський Ю.Г. Вдосконалення функції стискання хеш-функції з застосуванням клітинних автоматів. Проблеми інформатики та комп'ютерної техніки: матеріали XII міжнар. наук.-практ. конф., м. Чернівці, 10–12 лист. 2023. Чернівці: Черн. нац. ун-т, 2023. - С. 82-83. (*Внесок авторів: Дячук Р.Л. – програмна модифікація функції стискання, експериментальні дослідження; Комісарчук В.В. – аналіз літератури, підготовка теоретичного обґрунтування; Прохоров П.А., Прохоров Г.В. – методологія, математичне моделювання, валідація; Добровольський Ю.Г. – концептуалізація, узагальнення результатів, редагування).*
10. Добровольський Ю.Г, Прохоров Г.В., Янушевський С.В., Прохоров П.А, Дячук Р.Л., Трембач Д. В. Оцінка надійності програмного забезпечення з точки зору його довговічності. Проблеми інформатики та комп'ютерної техніки: матеріали XII міжнар. наук.-практ. конф., м. Чернівці, 01–03 лист. 2024. Чернівці: Черн. нац. ун-т, С. 36-37. (*Внесок авторів: Добровольський Ю.Г. – концептуалізація, методологія оцінювання, редагування; Прохоров Г.В. – математична модель довговічності, аналіз результатів; Янушевський С.В. – статистична обробка даних, валідація; Прохоров П.А. – аналіз показників надійності; Дячук Р.Л. – програмна реалізація моделі, експериментальні дослідження, візуалізація; Трембач Д.В. – збір даних, підготовка матеріалів).*
11. Добровольський Ю.Г., Прохоров Г.В., Дячук Р.Л. Генерація послідовності випадкових чисел на основі темнового струму фотодіода. Current trends in scientific research development. Proceedings of the 13th International scientific and practical conference. BoScience Publisher. Boston, USA. 2025. P. 65-67. (*Внесок авторів: Добровольський Ю.Г. – концептуалізація, постановка*

задачі, редагування; Прохоров Г.В. – методологія експерименту, аналіз фізичних параметрів; Дячук Р.Л. – програмна обробка сигналу, реалізація генератора, статистичне тестування випадковості, написання рукопису).

12. Prokhorov G.V., Diachuk R.L., Hanzhelo M.G,, Yanushevskyi S.V. New approaches to the design of a hybrid random sequence generator. Physical and technological problems of transmission, processing and storage of information in infocommunication systems: Proceedings of Xth International Scientific-Practical Conference. Chernivtsi : Yuriy Fedkovych Chernivtsi National University, 2025. P. 134-136. (*Внесок авторів: Prokhorov G.V. – концептуалізація, методологія гібридної моделі; Diachuk R.L. – програмна реалізація генератора, експериментальні дослідження, візуалізація результатів, підготовка початкового варіанту статті; Hanzhelo M.G. – аналіз існуючих підходів, валідація; Yanushevskyi S.V. – рецензування та редагування, наукове керівництво).*

9. Апробація матеріалів дисертації.

Основні результати роботи доповідались та обговорювались на наукових семінарах кафедри програмного забезпечення комп'ютерних систем, а також на Всеукраїнських та Міжнародних наукових і науково-практичних конференціях: «Проблеми інформатики та комп’ютерної техніки» (Чернівці, 2022, 2023, 2024), «IEEE 4th International Conference on Advanced Trends in Information Theory» (Kyiv, 2022), «Інформаційні технології: наука, техніка, технологія, освіта, здоров’я» (MicroCAD)» (Харків, 2023), «Current trends in scientific research development» (Boston, 2025), «Physical and technological problems of transmission, processing and storage of information in infocommunication systems» (Чернівці, 2025).

10. Оцінка мови і стилю дисертації.

Дисертація написана чіткою мовою, відповідає критеріям науковості, забезпечуючи логічність, послідовність і об'єктивність викладення результатів

дослідження. Зазначене свідчить про відповідність вимогам, що висуваються до праць такого рівня.

11. Відповідність змісту дисертації спеціальності з відповідної галузі знань, з якої вона подається до захисту.

Зміст дисертації відповідає чинним вимогам до оформлення дисертації, встановленим освітньо-науковою програмою «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології», спеціальності 121 – Інженерія програмного забезпечення.

12. Дотримання нормативних вимог щодо оформлення дисертації.

Нормативні вимоги щодо оформлення дисертації дотримані повністю.

13. Рекомендації дисертації до захисту.

Дисертаційна робота Дячука Ростислава Любомировича «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел», подана на здобуття ступеня доктора філософії (PhD) у галузі знань 12 – Інформаційні технології за спеціальністю 121 – Інженерія програмного забезпечення, за її актуальністю, науково-технічним рівнем, новизною постановки та розв’язання проблем, практичним значенням отриманих результатів відповідає вимогам пунктів 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. №44 (зі змінами, внесеними згідно з Постановою Кабінету Міністрів України №507 від 03.05.2024 р.).

За результатами публічної презентації результатів дисертації та їх обговорення на засіданні кафедри програмного забезпечення комп’ютерних систем Навчально-наукового інституту фізико-технічних та комп’ютерних наук Чернівецького національного університету імені Юрія Федьковича 13 березня 2026 року дисертацію Дячука Ростислава Любомировича рекомендовано до захисту в разовій спеціалізованій вченій раді для здобуття ступеня доктора

філософії (PhD) з галузі знань 12 – Інформаційні технології за спеціальністю 121 – Інженерія програмного забезпечення.

Голова засідання Катерина ГАЗДЮК

доктор філософії, доцент,
завідувач кафедри програмного
забезпечення комп'ютерних систем
Чернівецького національного університету
імені Юрія Федьковича