

Рішення
разової спеціалізованої вченої ради PhD 13280
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Ростислав Дячук, 1998 року народження, громадянин України, освіта вища: закінчив у 2020 році Чернівецький національний університет імені Юрія Федьковича за спеціальністю Інженерія програмного забезпечення, працює асистентом кафедри програмного забезпечення комп'ютерних систем навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича, м. Чернівці, виконав акредитовану освітньо-наукову програму 38613 «Інженерія програмного забезпечення» (сертифікат №16846).

Разова спеціалізована вчена рада PhD 13280, утворена наказом Чернівецького національного університету імені Юрія Федьковича Міністерства освіти і науки України, м. Чернівці від «28» квітня 2026 року № 167 у складі:

- | | |
|--|--|
| Голови разової спеціалізованої вченої ради – | Сергія Баловсяка , доктора технічних наук (05.13.05 - Комп'ютерні системи та компоненти), доцента, доцента кафедри комп'ютерних систем та мереж навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича, |
| Рецензента – | Петра Шпатаря , кандидат технічних наук (05.27.01 – Твердотільна електроніка), доцента, директора навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича, |
| Офіційних опонентів – | Сергія Євсєєва , доктора технічних наук (21.05.01 – Інформаційна безпека держави), професор, завідувача кафедри кібербезпеки навчально-наукового інституту комп'ютерних наук та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут»,
Володимира Баранніка доктора технічних наук, (05.12.02 – Телекомунікаційні системи та мережі), професора, професора кафедри математичного моделювання та аналізу даних навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В.Н. Каразіна,
Олега Гарасимчука , кандидат технічних наук, (05.13.05 – Елементи та пристрої обчислювальної техніки та систем керування), доцента, доцента кафедри захисту інформації інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», |

на засіданні «18» червня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 «Інформаційні технології» Ростиславу Дячуку на підставі публічного захисту дисертації «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел» за спеціальністю «121 Інженерія програмного забезпечення».

Дисертацію виконано у Чернівецькому національному університеті імені Юрія Федьковича Міністерства освіти і науки України, м. Чернівці.

Науковий керівник Юрій Добровольський, доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича.

Дисертацію подано у вигляді спеціально підготовленого рукопису українською мовою. Дисертація Дячука Ростислава на тему «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел», що подана на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 121 «Інженерія програмного забезпечення», є самостійним завершеним дослідженням, має наукову новизну, практичну значущість і відповідає вимогам Наказу Міністерства освіти і науки України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації» (зі змінами, внесеними згідно з Наказом МОН України від 31.05.2019 р. № 579) та «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 № 341 від 21.03.2022 р., № 502 від 19.05.2023 р., № 507 від 03.03.2024 р.).

Здобувач має 11 наукових публікацій за темою дисертації, з них 4 праці у наукових фахових періодичних виданнях України, 1 в іноземному періодичному науковому виданні, індексованому в наукометричній базі даних Scopus та 7 праць, що засвідчують апробацію матеріалів дисертації.

1. Diachuk R., Dmytrashchuk K., Mazurets A., Prokhorov H., Yanushevskiy S. Photosensitive matrix as a source of entropy. Proceedings of SPIE. 13813, Seventeenth International Conference on Correlation Optics. 2025. 138132C. ISSN:0277-786X (Scopus)

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.

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.

4. Prokhorov H., Hanzhelo M., Diachuk 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.

5. Добровольський Ю., Дячук Р. Дослідження генерації випадкової послідовності чисел на основі темнового струму 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.

У дискусії взяли участь голова, рецензенти, офіційні опоненти та висловили зауваження:

Голова спеціалізованої вченої ради Сергій Баловсяк, доктор технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича. Зауваження до дисертаційного дослідження відсутні.

Опонент Сергій Євсєєв – доктор технічних наук, професор, Лауреат національної премії ім. Бориса Патона, завідувач кафедри кібербезпеки навчально-наукового інституту комп'ютерних наук та інформаційних технологій Національного технічного університету «Харківський політехнічний інститут». Зауваження:

1. У роботі висловлена гіпотеза про можливість довести продуктивність генерації ПВЧ аж до 10 Гбіт/с. Проте зовсім не приведено аргументацію про таке припущення.

2. На рис. 2.1 дисертаційної роботи наведена технологія генерація ПВЧ з пікселів зображення, сформованого веб-камерою. При цьому не зовсім зрозуміло, чому автор не пояснює сутність наведеної технології. Також не визначені вхідні гіпотези – чому саме 100 мілісекунд автор вважає достатнім для проведення досліджень.

3. Для отримання випадкових чисел з цього процесу генерації шкалу фотоструму пропонується розділити на набір безперервних інтервалів, кожен з яких відповідає певному цілочисельному значенню (стор. 53, рис. 2.4), але не зрозуміло за який час та скільки потрібно отримати інтервалів, щоб забезпечити необхідний рівень безпеки згідно вимог НІСТ на конкурсі постквантових алгоритмів.

4. В розділі 2.6 наведений порівняльний аналіз розроблених генераторів ПВЧ, однак відсутність критеріїв оцінки та кількісних показників значно зменшують достовірність

результатів оцінки.

5. У табл. 3.1 наведено результати тестування згенерованої ПВЧ на відповідність вимогам NIST (SP 800-22). При цьому тест 7 та 15 мають замалі показники. Але ці результати не пояснені у тексті роботи, як і причини їх виникнення.

6. В розділі 3.2 запропонована інформаційна система для генерації ПВЧ на основі ФЕЯ, але відсутні структурна схема та опис її функціональності.

Опонент Володимир Бараннік, доктор технічних наук, професор, професор кафедри математичного моделювання та аналізу даних навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В.Н. Каразіна. Зауваження:

1. При викладенні матеріалу бажано пояснити принципову різницю між генерацією випадкових чисел та генерацією саме послідовностей випадкових чисел. Зокрема сучасні вимоги до довжини послідовності, продуктивність генерації, питанням безпеки, надійності та зручності використання (usability).

2. У заявленій у розділі 2 пункт 2.1 (стор. 46) цифровій веб-камері відсутні технічні характеристики, які унеможливають стверджувати про відсутність первинної пост-обробки всередині самої камери, а також дані про довгий час неперервної надійної роботи веб-камери. Бажано було б провести дослідження на веб-камері відомої марки смартфона чи айфона.

3. Аналізуючи відповідність згенерованої послідовності випадкових чисел вимогам NIST (SP 800-22) табл.3.1 не пояснено низький рівень проходження тесту 7. Non-overlapping Template Matching та тесту 15. Random Excursions Variant. Не вказано можливі причини, критичність та шляхи подолання.

4. Перевірка якості хешування проводилась на коротких фразах, проте саме об'єкти великого розміру являть науково-дослідницький інтерес. Логічно допустити, що запропонований алгоритм успішно справиться з таким завданням, проте необхідні дослідження не були проведені.

5. Деякі англійські наукові терміни перекладені не однозначно коректно. Наприклад, «seed» в одному місці трактується як «затравка», а в іншому як «початковий вектор».

Опонент Олег Гарасимчук, кандидат технічних наук, доцент, доцент кафедри захисту інформації інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка". Зауваження:

1. Автор розглядає веб-камеру як джерело ентропії, але не вказує, чи будь-яка веб-камера підходить для генерації ПВЧ? Які самі характеристики потрібно перевірити перед прийняттям рішення про доцільність її використання?

2. Стверджувати про "лавинний ефект" при кореляції сусідніх кадрів не зовсім коректно згідно визначення. Лавинний ефект це максимальна зміна наслідків (до 50%) при мінімальному відхиленні вхідних параметрів. Чи можна у вашому випадку стверджувати, що вхідним параметром є проміжок часу між сусідніми кадрами – досить хитка позиція, що потребує подальшої аргументації. На мій погляд краще ввести інший термін дуже близький до "лавинного ефекту".

3. Не продекларовано технічні вимоги для функціонування інформаційної системи (об'єм оперативної пам'яті, об'єм жорсткого диску, роздільна здатність монітора, швидкодія процесора, ширина USB каналу).

Рецензент Петро Шпатар, кандидат технічних наук, доцент, директор навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича. Зауваження:

1. Автор згадує, що в якості джерела ентропії використовує фотодіод з високою квантовою ефективністю, але не обґрунтовує це положення. А саме, як пов'язана квантова ефективність фотодіода із якістю (непередбачуваністю) створеної на його основі ПВЧ.

2. При розгляді темного струму фотодіода як джерела ентропії, показано, що найкращі результати отримані про 50°C. Але не досліджено як впливають на якість ПВЧ більші температури. Було би доцільно вивчити це питання.

3. Щодо вимірювання темного струму фотодіоду. На рис. 2.8 є позиція 4 "вольтметр постійного струму", а на рис. 2.11 присутній ППТН (поз. 7). З якою метою здійснені зміни і як вони впливають на генерацію ПВЧ?

4. Добре би було проаналізувати можливість роботи створеної інформаційної системи з існуючими криптографічними приладами, які використовують інші джерела ентропії.

На дисертацію Дячука Р. Л. надійшло три звернення. Вони позитивні та підкреслюють актуальність і значущість проведеного дослідження, хоча містять окремі зауваження та рекомендації щодо перспектив подальших досліджень:

Перше звернення:

Тетяна Говорущенко – доктор технічних наук, професор, декан факультету інформаційних технологій Хмельницького національного університету. У своєму зверненні Говорущенко Т. О. зазначила, що суттєвою ознакою роботи є створення інформаційної системи, яка забезпечує вибір способу генерації ПВЧ, перевірку та ступінь її хаотичності і потокової генерації ПВЧ з високим рівнем ентропії. Також суттєвим на її думку, є те що створена інформаційна система може створювати ПВЧ заданої продуктивності, що відрізняє її з поміж відомих аналогів.

До недоліків роботи Говорущенко Т. О. віднесла наявність орфографічних помилок у тексті дисертації, а також те, що з точки зору подальших досліджень, було би добре дослідити продуктивність ПВЧ при роботі з високочастотним обладнанням, як про це писав автор.

Друге звернення:

Володимир Мещеряков – доктор технічних наук, професор, професор кафедри Інформаційних технологій Одеського національного університету ім. І. І. Мечникова. Мещеряков В. І. відзначив, що суттєвими перевагами нової системи є вбудований модуль оцінки ступеня хаотичності згенерованих числових послідовностей власної розробки, а також новий підхід встановлення балансу між продуктивністю та надійністю отриманих послідовностей.

До зауважень Мещеряков В. І. відніс те, що в роботі не описано технічних вимог до апаратної частини для її коректного функціонування. Проте вважає, що недолік не є суттєвим і не спотворює високого наукового та прикладного рівня дисертації.

Третє звернення:

Денис Остапець – кандидат технічних наук, доцент, доцент кафедри електронних обчислювальних машин Українського державного університету науки і технологій. Автор відзначає, що створена інформаційна система забезпечує безперервне генерування ПВЧ заданої продуктивності та якості на широко доступному обладнанні, що є суттєвою перевагою у порівнянні із відомими аналогами.

Також, у якості недоліків, Остапець Д. О. відмітив, що в роботі варто було виконати дослідження ефективності генерування ПВЧ з використанням фотодіода не тільки при різних температурах, а і при впливі інших зовнішніх чинників. Проте вважає, що в цілому, зміст робота та отримані результати відповідають поставленим в ній завданням.

Результати відкритого голосування:

«За» – 5 (п'ять) членів ради,

«Проти» – 0 (нуль) членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада PhD 13280 присуджує Ростиславу Дячуку ступінь доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 121 «Інженерія програмного забезпечення».

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради

PhD 13280

доктор технічних наук,
доцент, доцент кафедри комп'ютерних
систем та мереж

навчально-наукового інституту фізико-
технічних та комп'ютерних наук

Чернівецького національного університету
імені Юрія Федьковича



Сергій БАЛОВСЯК