Голові разової спеціалізованої вченої ради
Національного університету «Львівська політехніка»
д.т.н., професору Нємковій Олені Анатоліївні

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
д.т.н., професора, Казакової Надії Феліксівни,
завідувача кафедри інформаційних технологій
Одеського національного університету імені І.І. Мечникова
на дисертаційну роботу
Горячого Олега Ярославовича
«Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки»,
подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

1. Актуальність теми дисертаційної роботи.

Дисертаційна робота Горячого О.Я., присвячена розв'язанню важливого наукового завдання, а саме: розробці та дослідженню генераторів псевдовипадкових послідовностей (ГПВП) для кібербезпеки (КБ) та захисту інформації (ЗІ), побудованих на основі вдосконалених методів наближеного обчислення елементарних функцій в арифметиці з рухомою комою (FP) і таких, що задовольняють вимогам статистичних тестів NIST. У сучасних інформаційних системах, від захищених каналів зв'язку до інтелектуальних інформаційних систем, систем штучного інтелекту, криптографічних протоколів, стеганографічних алгоритмів, систем автентифікації, симуляції загроз і виявлення аномалій, такі компоненти є критично важливими для забезпечення безпеки, надійності та ефективності функціонування, що підтверджує наукову та практичну актуальність дослідження.

Дисертаційна робота вирізняється високим рівнем наукової та прикладної актуальності, що обумовлено постійним зростанням потреб у надійних, продуктивних та статистично якісних генераторах псевдовипадкових чисел (ГПВЧ), а також у швидких і точних методах обчислення елементарних функцій для завдань кібербезпеки.

З урахуванням активного поширення пристроїв з обмеженими ресурсами, таких як мікроконтролери та IoT-платформи, актуальною є розробка легких у реалізації програмних і програмно-апаратних рішень, що дозволяють здійснювати обчислення функцій типу RCP, RSQRT, DIV, SQRT та генерації псевдовипадкових послідовностей без апаратної підтримки або з її мінімальним використанням. З огляду наявні бібліотечних реалізації можна зробити висновок, що вони часто не забезпечують належного балансу між точністю, продуктивністю та

використанням ресурсів, а частина існуючих генераторів псевдовипадкових чисел (ГПВЧ) має обмежену довжину періоду, слабкі статистичні характеристики або криптографічні вразливості, включно з можливістю вбудованих бекдорів.

У своїй роботі здобувач запропонував концептуально новий підхід до проєктування ГПВЧ – на основі швидких чисельних алгоритмів апроксимації елементарних функцій в арифметиці з рухомою комою, що дозволило досягти високої швидкодії, задовільних статистичних характеристик (зокрема відповідно до NIST STS) та придатності до реалізації на широкому спектрі платформ. Зокрема, для реалізації запропонованих здобувачем методів вимагається наявність ефективної реалізації лише базових операцій в арифметиці з рухомою комою. Отримані результати мають потенціал до практичного застосування в системах реального часу, захищених обчисленнях, стеганографічних системах, мобільних і вбудованих системах безпеки.

Таким чином, дисертаційне дослідження Горячого О. Я. є своєчасною науково обґрунтованою відповіддю на виклики сучасної кібербезпеки, спрямованою на створення ефективних, масштабованих та безпечних рішень для генерації псевдовипадкових послідовностей і обчислення елементарних функцій. Робота поєднує глибокий теоретичний аналіз з практичною реалізацією та апробацією на реальних апаратних платформах, що підсилює її значущість для галузі.

Дисертаційні дослідження Горячого О.Я. виконувались у відповідності до наукового напрямку кафедри безпеки інформаційних технологій Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», а також в межах науково-дослідних робіт кафедри за темами «Розробка та покращення ефективності алгоритмів обчислення елементарних функцій для задач захисту інформації» (№ держреєстрації 0120U103215), «Розроблення стеганографічних методів приховування даних у цифрових зображеннях» (№ держреєстрації 0120U100024) та «Розробка та дослідження генераторів псевдовипадкових чисел і послідовностей» (№ держреєстрації 0113U005267).

2. Аналіз змісту дисертаційної роботи.

Дисертація налічує 288 сторінок, із яких 168 – основний текст. Структура дисертаційної роботи включає анотацію, зміст, перелік умовних позначень, вступ, чотири розділи, висновки, список використаних джерел (225 позицій) та 8 додатків.

У **вступі** здобувачем обґрунтовано актуальність теми дисертаційного дослідження, сформульовано основну ідею, мету дослідження та науково-прикладні завдання, необхідні для її досягнення, показано зв'язок дослідження з науковими програмами та темами, наведено наукову новизну отриманих результатів, їх практичну цінність та особистий внесок.

У **першому розділі** здійснено огляд існуючих методів обчислення елементарних функцій в арифметиці з рухомою комою та методів генерації псевдовипадкових послідовностей (ПВП). Проведено аналіз вітчизняної і зарубіжної наукової літератури за тематикою дослідження, класифікацію та порівняння відомих алгоритмів, зокрема методу FISR і поширених підходів до генерації ПВП для криптографічних і некриптографічних задач. Визначено шляхи підвищення точності та швидкодії обчислень, а також проаналізовано методи оцінки якості генераторів з урахуванням вимог кібербезпеки. Сформульовано основні вимоги до розробки та вдосконалення алгоритмів для задач інформаційної безпеки та кібербезпеки, зокрема генерації ПВП, а також обґрунтовано вибір стандарту NIST STS як основи для подальшого тестування.

У **другому розділі** розроблено основну методику проєктування та дослідження вдосконалених алгоритмів обчислення елементарних функцій та генерації псевдовипадкових чисел на основі арифметики з рухомою комою. Сформульовано методи оцінки похибок та точності, вимірювання швидкодії та аналізу збіжності. Розглянуто методи проєктування та дослідження ГПВЧ на основі арифметики з рухомою комою для застосувань у сфері кібербезпеки та захисту інформації, зокрема методику дослідження статистичних характеристик, швидкодії та періоду повторення сформованих ПВП. Для визначення оптимальних значень коефіцієнтів розроблено набір алгоритмів рандомізованої чисельної багатовимірної оптимізації. Запропоновано новий підхід до генерації ПВП, що використовує рекурентне рівняння та чисельні методи в арифметиці з рухомою комою. Розроблено методи автоматизації їх статистичного тестування для задач кібербезпеки на основі тестів NIST та визначення періоду повторення для різних початкових значень та параметрів генерації ПВП.

У **третьому розділі** представлено новий підхід до генерації псевдовипадкових чисел і послідовностей, що базується на чисельних методах апроксимації в арифметиці з рухомою комою та орієнтований на застосування в інформаційній та кібербезпеці. Для проєктування ГПВЧ розроблено наступні ефективні методи обчислення функцій RCP, SQRT та RSQRT: на основі модифікованого методу Хаусхолдера 2-го порядку (Ho2), методи додаткових магічних констант (2MC/3MC) та методи переключення магічних констант (DC/8DC). Залежно від початкового значення та обраних параметрів генератора псевдовипадкових чисел формується рекурентна послідовність 64-бітових аргументів з рухомою комою та генерується псевдовипадкова байтова послідовність. Запропоновані алгоритми забезпечують якісний компроміс між точністю, швидкодією та розміром таблиці пошуку, а побудовані на їх основі прості генератори – задовільні статистичні властивості.

У **четвертому розділі** проведено тестування та аналіз ефективності запропонованих алгоритмів і ГПВЧ на процесорах Intel Core i5/i7, ARM Cortex-A53 та ESP-WROOM-32. Оцінювались точність, латентність і зворотна пропускна

здатність алгоритмів обчислення RCP та RSQRT (float та double), а також продуктивність апаратних і програмно-апаратних реалізацій. Досліджено статистичні характеристики з використанням тестів NIST STS, графічних тестів та ентропії, а також період повторення, обчислювальну складність та швидкодію при зміні початкових значень та параметрів генерації. Виявлено, що найкращі статистичні характеристики для застосувань у сфері кібербезпеки та захисту інформації має ГПВЧ rsqrt2dc_everyBit (1/0), для якого відсоток проходження всіх тестів NIST при зміні початкових значень складає 79,73% (середня кількість пройдених тестів 187,76). Здійснено порівняння з стандартними ГПВЧ з бібліотеки random та апаратними генераторами випадкових послідовностей. Найкращу продуктивність на Intel демонструють ГПВЧ rcp3_everyBit (3/0) та rsqrt1dc8_everyBit (3/0), що, зокрема, є швидшими за вихор Мерсена (mt19937) та у 1,5-7,5 рази швидші за апаратні генератори RDSEED та RDRAND. Запропоновано приклади практичного застосування розроблених ГПВЧ в задачах кібербезпеки та захисту інформації, зокрема в цифровій стеганографії.

У **висновках** дисертаційної роботи узагальнено основні теоретичні та прикладні результати дослідження, відображено їх відповідність поставленій меті та завданням. Наведено систематизовані порівняння ефективності розроблених алгоритмів обчислення елементарних функцій та генераторів псевдовипадкових чисел з відомими аналогами, визначено їх переваги щодо точності, швидкодії та ресурсної оптимізації. Сформульовано рекомендації щодо практичного впровадження отриманих результатів, а також окреслено напрями подальших досліджень, зокрема у галузі інформаційної та кібербезпеки.

У **додатках** до дисертації подано акти впровадження; програмні коди основних розроблених алгоритмів і засобів дослідження, зокрема методів рандомізованої чисельної багатовимірної оптимізації та скриптів для автоматизації тестування ГПВЧ із використанням статистичних тестів NIST, що можуть бути безпосередньо застосовані іншими дослідниками; результати порівняння відомих і розроблених алгоритмів; програмні коди алгоритмів, використаних при проєктуванні запропонованих ГПВЧ, а також результати їх тестування на різних апаратних платформах. Додатки також містять перелік наукових публікацій автора.

3. Наукова новизна одержаних результатів.

Найсуттєвіші результати дослідження, що містять наукову новизну, полягають в тому, що:

1) ***вперше запропоновано*** спосіб ефективної генерації ПВП на основі чисельних методів в арифметиці з рухомою комою, що демонструє задовільні статистичні характеристики для задач кібербезпеки та захисту інформації, що підтверджено проходженням тестів NIST STS (75-81% ПВП проходять всі тести), високу швидкодію (до 40 Мб/с на Intel i5), забезпечує максимальний період

повторення до $5{,}3 \cdot 10^9$ біт (або $6{,}66 \cdot 10^8$ 8-бітових чисел), високу ентропію та достатню множину початкових значень (до 2^{60}). Запропоновані ГПВЧ забезпечують проходження статистичних тестів NIST STS на рівні найкращих програмних ГПВЧ бібліотеки random (70–79%) з подібною швидкодією на Intel, а також у порівнянні з апаратними генераторами істинно випадкових послідовностей (70–82%) перевершують їх у 1,5–7,5 раза за пропускною здатністю. Вони призначені, в першу чергу, для стеганографії, криптографії, комп'ютерних ігор, моделювання та симуляції.

2) ***вдосконалено*** прості стеганографічні методи приховування даних у цифрових зображеннях на основі методу заміни найменш значущих бітів (LSB) та використання запропонованих ГПВЧ, що дозволило підвищити рівень безпеки вдосконаленої стеганографічної системи – зокрема за показниками конфіденційності, цілісності та стійкості до виявлення – шляхом аналізу висококонтрастних і граничних ділянок зображень, а також зменшити розмір стеганоключа на 94%.

3) ***вперше запропоновано*** методи покращення точності та швидкодії функцій RSQRT та RCP на основі алгоритму FISR, що через використання додаткових магічних констант (методи 2MC та 3MC) на основі цілочислових операцій дозволяють зменшити на 1–2 кількість використаних операцій множення в арифметиці з рухомою комою. Вони забезпечують спрощення апаратної реалізації та підвищення продуктивності обчислень, зокрема для пристроїв з обмеженими ресурсами, мікроконтролерів, ПЛІС та високопродуктивних систем. Запропоновані методи двох та трьох магічних констант дозволяють зменшити максимальні відносні похибки в 11,9 та в 21,2 раза порівняно з відомими алгоритмами.

4) ***вперше запропоновано*** ефективні методи переключення магічних констант (DC), зокрема для функцій RSQRT та SQRT, що передбачає розбиття області визначення функцій на піддіапазони з вибором оптимізованих констант. Розроблені для задач захисту інформації методи мають невелику надлишковість порівняно з алгоритмом FISR та забезпечують якісний компроміс між точністю, розміром таблиці пошуку (LUT) та швидкодією, використовуючи пам'ять для зберігання констант. Вони призначені, в першу чергу, для мікроконтролерів, персональних комп'ютерів та ПЛІС. Порівняно з методом Вальчика та ін. для функції RSQRT метод переключення магічних констант для двох та восьми піддіапазонів (методи DC та 8DC) має в 11,8 та в 101,2 раза меншу максимальну відносну похибку.

5) ***вдосконалено*** методи чисельної багатовимірної оптимізації з елементами випадковості на основі ГПВЧ, методу прямого пошуку та методу золотого перетину, що використовуються для визначення таких коефіцієнтів модифікованих алгоритмів, що мінімізують максимальну відносну похибку для визначених типів. Запропонований метод рандомізованої багатовимірної жадібної

оптимізації дозволяє підвищити швидкість пошуку оптимізованих параметрів та покращити їх результати.

6) ***вдосконалено*** набір модифікованих алгоритмів для швидкої апроксимації операції ділення, степеневих, логарифмічних та показникових елементарних функцій для чисел у форматі з рухомою комою для задач у сфері кібербезпеки та захисту інформації, що завдяки використанню оптимізації дозволяють досягти підвищеної точності. Розроблені алгоритми базуються на комбінації наступних методів з модифікованими параметрами: алгоритму FISR, ітераційних методів Ньютона-Рафсона і Хаусхолдера, методу мінімаксної поліноміальної апроксимації, швидких наближених апаратних інструкцій Intel та ARM. Вони забезпечують високу точність та/або швидкодію обчислень, похибку на рівні 1 ULP або повну точність з коректним заокругленням для чисел одинарної (тип float) та подвійної (тип double) точності.

7) ***отримали подальший розвиток*** методи автоматизації статистичного тестування ПВП для задач кібербезпеки, що включає використання пакету тестів NIST STS, визначення періоду повторення, застосування графічних тестів, оцінку ентропії, аналіз кореляції, аналіз продуктивності ГПВЧ і генераторів істинно випадкових послідовностей на різних платформах. Запропоновані методи призначені для комплексної оцінки якості генераторів та криптографічних алгоритмів.

4. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних дисциплін, де можуть бути застосовані отримані результати.

Виконане дослідження має значне наукове та практичне значення для галузі інформаційних технологій і кібербезпеки. Розроблені методи високошвидкісної апроксимації елементарних функцій, зокрема на базі алгоритму FISR, дозволяють створювати генератори псевдовипадкових послідовностей із задовільними статистичними характеристиками. Запропоновані алгоритми придатні для реалізації як у програмному, так і в апаратному вигляді на мікроконтролерах, CPU, FPGA і GPU. Їх використання є актуальним для побудови сучасних систем захисту інформації, таких як криптографічні протоколи, стеганографічні рішення, біометричні системи та системи виявлення вторгнень.

Наукові результати, отримані автором, можуть бути використані під час розроблення новітніх простих та ефективних генераторів псевдовипадкових чисел та послідовностей із покращеними статистичними, або навіть криптографічними властивостями, а також великим періодом повторення, придатних для застосування як у криптографічних, так і некриптографічних задачах кібербезпеки. А також під час проєктування високоточних простих та ефективних реалізацій методів обчислення елементарних функцій в арифметиці з рухомою комою.

Основні положення та результати дисертації були впроваджені в навчальний процес для здобувачів спеціальності 125 «Кібербезпека та захист інформації» Національного університету «Львівська політехніка», зокрема під час викладання дисциплін: «Прикладна криптологія», «Архітектура комп'ютерних систем», «Комп'ютерні методи дослідження інформаційних процесів і систем» та «Технології програмування», а також використовувались при виконанні науково-дослідних робіт кафедри безпеки інформаційних технологій. Запропоновані алгоритми використовувались при підготовці лабораторних і курсових робіт, а також для формування індивідуальних завдань і вибору тем кваліфікаційних робіт.

5. Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна.

Достовірність і обґрунтованість наукових результатів дисертації забезпечуються системним і професійним підходом до постановки завдань, ретельним вибором і обґрунтуванням методів дослідження, а також глибоким теоретичним опрацюванням базових математичних положень. Автором виконано аналіз сучасних наукових публікацій, застосовано кілька незалежних методів оцінки та проведено порівняльний аналіз запропонованих рішень з найкращими відомими аналогами. Висновки та рекомендації підтверджені результатами комп'ютерного моделювання, експериментальних досліджень і практичного тестування алгоритмів на різних обчислювальних платформах – від високопродуктивних процесорів Intel i5 та Intel i7 до мінікомп'ютера Raspberry Pi 3 і мікроконтролера ESP-WROOM-32. Представлені таблиці, графіки та ілюстрації демонструють повну відповідність отриманих результатів заявленим науковим положенням.

Основна ідея дисертації, що визначає її наукову новизну та актуальність, полягає у дослідженні застосування арифметики з рухомою комою та вдосконалених методів швидкої апроксимації нелінійних елементарних функцій (RCP, SQRT, RSQRT тощо) на основі методу FISR для проєктування новітніх методів генерації псевдовипадкових чисел, придатних для задач кібербезпеки та захисту інформації та таких, що відповідають вимогам статистичних тестів NIST STS. Запропонований підхід може слугувати основою для створення модифікованих генераторів псевдовипадкових чисел і генераторів псевдовипадкових бітових послідовностей з покращеними статистичними характеристиками, а також криптостійких варіантів таких генераторів.

Наявні в додатках до дисертації акти впровадження також підтверджують актуальність, достовірність і наукову новизну отриманих результатів.

6. Практичне значення одержаних результатів.

1) Розроблені методи та програмні реалізації покращених алгоритмів обчислення елементарних функцій і ГПВЧ можуть бути ефективно

імплементовані як програмно, так і апаратно на різних обчислювальних платформах, зокрема на мікроконтролерах, CPU, GPU та ПЛІС. Запропоновані ГПВЧ призначені насамперед для некриптографічних задач для застосування на 64-бітних пристроях, що підтримують основні операції з рухомою комою.

2) Запропоновані ГПВЧ використано для вдосконалення методів LSB-стеганографії у випадку приховування даних у цифрових зображеннях. Застосування вдосконаленої моделі стеганосистеми дозволило підвищити рівень безпеки стеганографічних методів шляхом аналізу висококонтрастних і граничних ділянок зображень, а також зменшити розмір стеганоключа на 94% без послаблення конфіденційності, цілісності та стійкості до виявлення вбудованих даних.

3) Проведено статистичне тестування запропонованих ГПВЧ пакетом тестів NIST STS, отримані залежності періоду повторення сформованих ПВП від вибору початкового значення ГПВЧ, визначено прийнятні діапазони початкових значень і встановлено генератори з найкращими характеристиками для застосування у сфері кібербезпеки та захисту інформації. Розроблені інструменти автоматизованого тестування, що включають перевірку статистичних властивостей за стандартом NIST STS, визначення періоду повторення, вимірювання швидкодії та продуктивності ГПВЧ, можуть бути використані дослідниками для комплексної оцінки якості генераторів та криптографічних алгоритмів.

4) Показано, що найкращі характеристики щодо випадковості згенерованих ПВП при різних початкових значеннях мають ГПВЧ rsqrt2dc_everyBit (1/0), rsqrt1dc8_everyBit (2/0) та rcp3_everyBit (3/0), доля проходження тестів NIST яких складає відповідно 79%, 78% та 75%. Найвищу швидкість генерації ПВП має найпростіший варіант ГПВЧ x_xored (2/1), хоча він має статистичні недоліки. Рекомендованими для застосувань у сфері кібербезпеки щодо статистичних характеристик та ефективності реалізації є ГПВЧ rsqrt1dc8_everyBit (2/0) та rcp3_everyBit (3/0). Вони є швидшими за найшвидші ГПВЧ random_device та mt19937 бібліотеки random на Intel (швидкість генерації до 40 Мб/с), а також апаратні генератори істинно випадкових послідовностей RDSEED та RDRAND (у 1,5-7,5 раза вища швидкість генерації), не вимагаючи значних обсягів пам’яті, зовнішніх джерел ентропії та тривалих термінів реініціалізації.

5) Сформульовано вимоги та розроблено методику проектування високоточних і швидкодіючих алгоритмів обчислення елементарних функцій у арифметиці з рухомою комою, орієнтовану на потреби інформаційної та кібербезпеки. Запропоновані математичні моделі та інструменти для модифікації та вдосконалення алгоритмів. Вони можуть бути застосовані науковцями у сфері кібербезпеки та комп’ютерними інженерами на практиці для розробки нових модифікацій алгоритмів на основі методів магічної константи, кусково-поліноміальних, дробово-раціональних методів або спеціалізованих апаратних інструкцій сучасних платформ, а також модифікованих ітераційних методів різного порядку збіжності.

6) В дисертації розроблено покращені оптимізовані алгоритми мовою C/C++ на основі модифікацій алгоритму FISR для обчислення елементарних функцій в арифметиці з рухомою комою, зокрема RCP, RSQRT, DIV та SQRT, що широко використовуються в сфері кібербезпеки та інформаційної безпеки. Зокрема, для функції RCP запропоновані алгоритми дозволяють зменшити максимальні відносні похибки результату в 2,2-21,2 раза (13-14 біт точності) порівняно з відомими алгоритмами, зокрема методами Мороза та ін., а для функції RSQRT – в 2,2-32,9 раза (10-15 біт точності) порівняно з відомими алгоритмами, зокрема найкращими модифікаціями алгоритму FISR.

7) На основі отриманих алгоритмів можна реалізувати спеціалізовану математичну бібліотеку, що буде підтримувати ефективні обчислення елементарних функцій з різною точністю (наприклад, 13 або 14 біт для функції RCP; 10, 13 або 15 коректних біт для функції RSQRT). Також можна розробити відповідну бібліотеку запропонованих легких та швидких ГПВЧ на їх основі для застосувань у сфері кібербезпеки та захисту інформації, що мають задовільні статистичні характеристики відповідно до тестів NIST.

8) Основні теоретичні та практичні результати дисертаційного дослідження використані при виконанні науково-дослідних робіт та у навчальному процесі кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка», а також впроваджені в науково-виробничому приватному підприємстві «Спаринг-Віст Центр» під час розроблення захищеного програмного забезпечення для моделювання та симуляції роботи вимірювальних пристроїв, що підтверджено відповідними актами впровадження.

7. Повнота оприлюднення результатів дисертаційної роботи.

Результати дисертаційного дослідження були особисто представлені здобувачем та обговорені на **5** міжнародних науково-технічних і науково-практичних конференціях, симпозіумах та консорціумах.

Основні результати дослідження оприлюднено у **15** наукових публікаціях, серед яких **3** статті у фахових наукових виданнях (включно з **1**, що індексується в Scopus), **1** стаття у науковому періодичному виданні іншої держави, що індексується в Scopus, **1** розділ монографії, **1** стаття в науковому нефаховому виданні України та **9** тез доповідей та матеріалів науково-технічних і науково-практичних конференцій, симпозіумів та консорціумів (включно з **2**, що індексується в Scopus), що засвідчують апробацію положень дисертації та додатково відображають наукові результати дисертації.

Можна стверджувати, що основні положення та результати дисертаційної роботи висвітлені у публікаціях в достатньому обсязі. Основні результати дисертації відображені в публікаціях високого рівня, зокрема у фахових наукових виданнях і виданнях, які входять до міжнародних наукометричних баз. Особистий

внесок здобувача у колективно опублікованих працях полягає у формуванні та розробці ключових ідей, одержані та аналізі результатів.

8. Оцінка структури дисертації, її мови та стилю викладення.

Структура дисертаційної роботи є логічно вибудуваною та повністю відповідає встановленим вимогам Міністерства освіти і науки України до дисертаційних досліджень на здобуття наукового ступеня доктора філософії. Розділи роботи взаємопов'язані та послідовно висвітлюють актуальність теми, мету й завдання дослідження, детальний огляд сучасного стану проблеми, обґрунтування обраних методів і підходів, результати експериментальних досліджень, тестування та аналіз результатів, а також можливості практичного застосування та подальших досліджень. Така структурованість дозволяє чітко простежити логіку наукового пошуку та послідовність отримання результатів.

Мова і стиль викладення відповідають нормам академічного письма та відзначаються науковою виваженістю, точністю й коректністю використання термінології у сферах кібербезпеки, чисельних методів, обчислювальної математики, архітектури комп'ютерних систем, програмування та інформаційних технологій. Матеріал подано чітко й структуровано, у роботі переважає формалізований стиль із належним використанням графічних матеріалів, таблиць і схем, які підсилюють розуміння результатів.

Дотримання академічної доброчесності підтверджується тим, що усі використані літературні джерела оформлені відповідно до чинних стандартів та коректно процитовані з посиланням на першоджерела. Анотація роботи повно та адекватно відображає її зміст, основні результати, наукову новизну та основні висновки проведеного дослідження.

9. Зауваження та дискусійні положення щодо змісту роботи.

Загалом позитивно оцінюючи дисертаційне дослідження, також доречно висловити певні зауваження та вказати на окремі положення роботи, що викликають дискусію:

1) У розділі 4.5 наведено два приклади практичного застосування запропонованих ГПВЧ на основі чисельних методів в арифметиці з рухомою комою: для генерації та випадкового розподілу між студентами варіантів завдань, а також при розробці простих стеганографічних методів приховування та захисту інформації на основі методу заміни найменш значущих бітів та використання ГПВЧ. Варто було б також детальніше розглянути приклади застосувань запропонованих ефективних методів апроксимації елементарних функцій в арифметиці з рухомою комою для задач кібербезпеки, наприклад для інтелектуального аналізу даних та систем виявлення вторгнень.

2) У розділі 4.5.2 запропонована модифікована модель стеганосистеми, а також набір простих стеганографічних методів на основі методу заміни

найменш значущих бітів, порівняння ефективності яких наведено на рис. 4.13. Проте, не всі з розглянутих методів детально описані в роботі, зокрема не наведено конкретні значення всіх параметрів для різних варіантів реалізації.

3) Механізм вибору конкретних методів обчислення функцій для розробки алгоритмів генерації псевдовипадкових чисел, зокрема апроксимації функцій RCP, SQRT та RSQRT, у роботі описано недостатньо детально. У розділі 3.4.2 досліджується лише використання бібліотечної функції SQRT подвійної точності. Проте, не досліджувалось використання інших розглянутих у розділах 1 та 3 методів наближення цієї функції, а також популярного методу генерації псевдовипадкових чисел на основі обчислення з довільною точністю функції SQRT від простого числа.

4) Дослідження методів покращення статистичних властивостей та стійкості запропонованих генераторів до різноманітних атак також розглянуто досить поверхнево, зокрема що стосується модифікації запропонованих ГПВЧ на основі використання логістичного відображення. Наприклад, не проведено детального аналізу чутливості вибору окремих параметрів базового та модифікованого алгоритму апроксимації функцій на статистичні характеристики, період повторення, кореляцію згенерованих послідовностей тощо.

5) Основним методом для практичного визначення похибок алгоритмів є повний перебір всіх можливих вхідних значень з певного діапазону чисел у форматі з рухомою комою, наприклад для функції RSQRT це проміжок $x \in [1; 4]$. Проте, для чисел з рухомою комою у форматі високої точності, зокрема binary128, цей метод має обмежені можливості щодо практичного вимірювання точності алгоритмів через його повільну швидкодію. Аналогічно, ускладнюється задача оптимізації їх параметрів на основі чисельних методів.

6) У роботі запропоновано набір методів чисельного багатовимірного пошуку для визначення оптимальних практичних значень магічних констант та параметрів алгоритмів, зокрема метод рандомізованої багатовимірної жадібної оптимізації. Водночас не подано порівняльного аналізу їх ефективності з уже відомими, наприклад, евристичними методами. Доцільним також було б продемонструвати на прикладі ефективність застосування запропонованих методів оптимізації для розв’язання інших задач у сфері кібербезпеки.

Слід зазначити, що виявлені недоліки та зауваження не є визначальними та не зменшують наукової та практичної значущості роботи.

Загальні висновки щодо дисертаційної роботи.

Варто відзначити високу глибину та повноту досліджень Горячого О. Я. Дисертація охоплює повний цикл: від огляду літератури та аналізу існуючих методів до проєктування, математичного моделювання, програмної реалізації, тестування на різних апаратних платформах (зокрема Intel, ARM, ESP32) та практичного застосування в задачах кібербезпеки. Здійснено аналіз відомих методів і

запропоновано шляхи їх удосконалення, зокрема щодо підвищення точності, швидкодії, статистичних властивостей і спрощення апаратної та програмної реалізації для застосування у сфері кібербезпеки та захисту інформації. Особливу увагу приділено тестуванню якості генераторів із використанням тестів NIST STS, а також аналізу періоду повторення, ентропії, графічних тестів, продуктивності та обчислювальної складності.

Дисертаційна робота Горячого Олега Ярославовича на тему «Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки» є завершеною науковою працею, що представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 125 «Кібербезпека та захист інформації» та чинним вимогам, які встановлені у «Порядку присудження ступеня доктора філософії та скасування рішень разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 зі змінами згідно з Постановою КМ №9341 від 21.03.2022, а її автор Горячий Олег Ярославович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації».

Офіційний опонент:
доктор технічних наук, професор,
завідувач кафедри інформаційних технологій
Одеського національного університету
імені І.І. Мечникова Надія КАЗАКОВА