Голові разової спеціалізованої вченої ради

Національного університету «Львівська політехніка»

д.т.н., професору Нємковій Олені Анатоліївні

ВІДГУК

офіційного рецензента – к.т.н., доцента, Гарасимчука Олега Ігоровича,
доцента кафедри захисту інформації
Національного університету «Львівська політехніка»
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.

Актуальною задачею досліджень у сфері кібербезпеки та захисту інформації є розробка новітніх інформаційних систем, технологій і комплексів створення, обробки, аналізу, передавання, зберігання, відображення та захисту даних, а також автоматизованих систем управління інформаційною безпекою. Під час проєктування таких систем виникає потреба у використанні наявних або розробленні нових ефективних методів генерації псевдовипадкових чисел (ПВЧ) і послідовностей (ПВП), а також методів обчислення елементарних функцій, що задовольняють необхідним вимогам щодо точності, безпеки, захисту інформації, надійності, продуктивності та використання ресурсів. Ця задача є особливо актуальною для високопродуктивних обчислень, систем реального часу та використання пристроїв з обмеженими ресурсами, зокрема мікроконтролерів. Прикладами таких систем кібербезпеки та захисту інформації, де глибоко поєднуються обидва типи згаданих методів, є криптографічні протоколи захищених багатокористувацьких обчислень, стеганографічні методи приховування даних, а також застосування нейронних мереж, моделювання та симуляція в задачах кібербезпеки.

Актуальність теми дисертаційної роботи зумовлена потребою у розробці та дослідженні ефективних і простих у реалізації підходів до проєктування генераторів псевдовипадкових чисел (ГПВЧ) на основі покращених методів обчислення елементарних функцій в арифметиці з рухомою комою для застосування в задачах інформаційної та кібербезпеки. Основні вимоги до

розроблених ГПВЧ – легкість реалізації, висока швидкодія та відповідність статистичним критеріям, зокрема вимогам тестів NIST Statistical Test Suite. Багато з наявних генераторів псевдовипадкових та істинно випадкових чисел характеризуються низкою істотних недоліків і вразливостей, серед яких – незадовільні статистичні характеристики згенерованих послідовностей, обмежена довжина періоду, низька продуктивність, надмірне споживання ресурсів, а також уразливість до алгебраїчних і криптографічних атак. Зазначені фактори значно обмежують можливість їх ефективного використання в реальних системах інформаційної безпеки. Основні вимоги до покращених методів обчислення елементарних функцій – легкість реалізації, висока точність та швидкодія.

Здобувачем запропоновано низку ефективних алгоритмів швидкої апроксимації елементарних функцій, зокрема RCP та RSQRT, на основі методу магічних констант, які дозволяють формувати послідовності ПВЧ з покращеними статистичними характеристиками. На відміну від генераторів істинно випадкових послідовностей, використання ГПВЧ суттєво спрощує процес генерації, обміну та оновлення ключових послідовностей у стеганографічних і криптографічних системах, генераторах шуму, а також на пристроях з обмеженими ресурсами без потреби у захищеному високошвидкісному каналі зв'язку. У більшості завдань, що виникають у сфері кібербезпеки та захисту інформації, необхідним є досягнення оптимального балансу між рівнем захисту, точністю обчислень, продуктивністю, вартістю реалізації та обсягом використаних ресурсів. Запропоновані здобувачем прості та ефективні ГПВЧ, побудовані на основі чисельних методів в арифметиці з рухомою комою, не використовують складних симетричних або асиметричних криптографічних перетворень.

2. Зв'язок теми дисертації з науковими програмами, планами і темами.

Наведені у дисертації дослідження виконувались автором відповідно науковому напрямку «Виконання наукових досліджень та практичних розробок у галузі інформаційних технологій, а саме: пристроїв опрацювання вихідних сигналів дозиметричних детекторів; генераторів псевдовипадкових чисел і бітових послідовностей та потокових шифрів на їх основі; алгоритмів та пристроїв обчислення елементарних функцій для чисел з рухомою комою» кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка».

Дисертацію виконано в межах науково-дослідних робіт кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка»: «Розробка та покращення ефективності алгоритмів обчислення елементарних функцій для задач захисту інформації» (№ держреєстрації

0120U103215, термін виконання 2020-2021), «Розробка та дослідження генераторів псевдовипадкових чисел і послідовностей» (№ держреєстрації 0113U005267, термін виконання 2017-2018) та «Розроблення стеганографічних методів приховування даних у цифрових зображеннях» (№ держреєстрації 0120U100024, термін виконання 2019-2024).

3. Наукова новизна основних результатів дисертації.

Новизна результатів та основних положень дисертації Горячого О.Я. зумовлена тим, 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, підтверджені проходженням тестів NIST STS (близько 80% згенерованих ПВП проходять всі тести), високу швидкодію (до 40 Мб/с на Intel i5), забезпечує максимальний період повторення до 5,3· біт (або 6,66· 8-бітових чисел), високу ентропію та достатню множину початкових значень для застосування у стеганографії, моделюванні та симуляції, нейронних мережах, комп'ютерних іграх, а також для інших некриптографічних та криптографічних задач кібербезпеки.

2) ***Вдосконалено*** прості стеганографічні методи приховування даних у цифрових зображеннях на основі методу найменш значущого біту 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*** метод переключення магічних констант (DC/8DC) для функцій RSQRT та SQRT, що передбачає розбиття проміжку визначення функції на дві, чотири або більше нерівних частин та оптимізує коефіцієнти алгоритмів на кожній з них. Розроблені для задач захисту інформації алгоритми забезпечують якісний компроміс між точністю, швидкодією та використанням пам'яті для збереження констант, призначені в першу чергу для мікроконтролерів, персональних комп'ютерів та програмованих логічних інтегральних схем (ПЛІС). Методи DC та 8DC дозволяють зменшити відносну похибку в 11,8 та 101,2 раз у порівнянні з методом Вальчика та ін. при використанні відповідно двох та восьми магічних констант.

4) ***Вперше запропоновано*** метод використання додаткових магічних констант (2MC та 3MC) для підвищення ефективності обчислення функцій RCP та RSQRT на основі модифікованого алгоритму швидкого зворотного квадратного кореня (FISR) та використання додаткових цілочислових операцій.

Цей метод дозволяє підвищити точність алгоритму FISR та зменшити кількість необхідних операцій множення в арифметиці з рухомою комою, що забезпечує спрощення апаратної реалізації та підвищення продуктивності алгоритмів для задач кібербезпеки, зокрема на мікроконтролерах, IoT пристроях, FPGA та високопродуктивних системах.

5) ***Вдосконалено*** методи чисельної багатовимірної оптимізації з елементами випадковості на основі ГПВЧ, методу прямого пошуку та методу золотого перетину, що використовуються в дисертації для визначення коефіцієнтів вдосконалених 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.

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

Наукові результати дисертації володіють достатнім ступенем достовірності та обґрунтованості, що базується на застосуванні професійного підходу до вибору методів і розроблення методики дослідження відповідно до поставленої мети та завдань дослідження, а також підтверджується результатами моделювання та експериментальних досліджень. У більшості випадків автор здійснює аналіз кількох альтернативних підходів до розв'язання поставленої задачі, виконує їх порівняльну оцінку з огляду на ключові переваги та недоліки, обґрунтовуючи вибір оптимального рішення.

Наукова новизна полягає у використанні арифметики з рухомою комою та вдосконалених методів апроксимації (наприклад, RCP, SQRT, RSQRT) для побудови новітніх методів генерації псевдовипадкових послідовностей, орієнтованих на потреби інформаційної безпеки, їх аналізу та дослідження. Тестування відомих та запропонованих алгоритмів виконувалось на платформах з різними характеристиками, зокрема на CPU Intel i5 та Intel i7, мінікомп'ютері Raspberry Pi 3 та мікроконтролері ESP-32. Слід відзначити

аналіз точності та швидкодії методів обчислення елементарних функцій, ретельне статистичне тестування генераторів з використанням набору тестів NIST STS, а також їх продуктивності на різних платформах.

Актуальність, достовірність та наукова новизна основних результатів дисертації додатково підтверджуються актами їх практичного впровадження.

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

Запропоновані в дисертації Горячого О.Я. методи та розроблені на їх основі алгоритми, зокрема прості та швидкі генератори псевдовипадкових чисел, побудовані із використанням покращених методів обчислення функцій RCP, RSQRT та SQRT в арифметиці з рухомою комою, можуть бути ефективно застосовані під час проєктування сучасних інформаційних систем, технологій та комплексів створення, обробки, аналізу, передачі, зберігання та захисту інформації, а також автоматизованих систем управління інформаційною та кібербезпекою. Отримані здобувачем наукові положення, висновки та практичні результати можуть бути використані у сфері кібербезпеки та захисту інформації під час розроблення стеганографічних, криптографічних, біометричних систем, нейронних мереж, систем виявлення вторгнень, моделювання, тестування та симуляції, захисту баз даних, їх статистичного та інтелектуального аналізу, а також протоколів захищеного багатокористувацького обчислення.

Запропонований здобувачем підхід до генерації псевдовипадкових чисел із використанням удосконалених методів обчислення елементарних функцій в арифметиці з рухомою комою може слугувати основою для створення генераторів із покращеними статистичними та криптографічними властивостями, орієнтованих на потреби кібербезпеки та захисту інформації. Для підвищення якості генерації обґрунтовано застосування хаотичних відображень і механізмів реініціалізації. Запропоновані методи обчислення елементарних функцій підвищеної точності та швидкодії (зокрема RCP, DIV, RSQRT, SQRT, RCBRT, CBRT, логарифмічних та експоненційних) мають перспективу використання в чисельних методах та комп'ютерній інженерії.

Основні положення та результати дисертаційного дослідження були впроваджені в навчальному процесі кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка», зокрема з курсів «Прикладна криптологія», «Архітектура комп'ютерних систем» та «Комп'ютерні методи дослідження інформаційних процесів і систем» для студентів спеціальності 125 «Кібербезпека та захист інформації», а також використовувались при виконанні науково-дослідних робіт кафедри.

6. Практичне значення одержаних результатів.

1) Розроблені в дисертації методи та програмні реалізації покращених алгоритмів обчислення елементарних функцій і генераторів псевдовипадкових чисел 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) 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.

3) Сформульовано вимоги та розроблено методику проєктування високоточних і швидкодіючих алгоритмів обчислення елементарних функцій у арифметиці з рухомою комою, орієнтовану на потреби інформаційної та кібербезпеки. Для апаратної реалізації та пристроїв з обмеженими обчислювальними ресурсами доцільним є використання спрощених оптимізованих алгоритмів на основі цілочислових та базових операцій у фіксованій або рухомій комі, з мінімізацією застосування ділення. 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.

4) 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. 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) Запропоновані ГПВЧ на основі чисельних методів в арифметиці з рухомою комою є придатними для застосування в задачах чисельної оптимізації з елементами стохастичності та в методах цифрової стеганографії. Їх використання сприяє підвищенню ефективності пошуку оптимальних рішень у сфері кібербезпеки, покращує конфіденційність, цілісність і стійкість до виявлення прихованих даних, а також дозволяє зменшити розмір стеганоключа.

6) Розроблені алгоритми можуть слугувати основою для побудови спеціалізованої математичної бібліотеки ефективного обчислення операції ділення, степеневих (наприклад, RCP, RSQRT, SQRT, RCBRT, CBRT), логарифмічних (наприклад, LOG2, LN, LOG10) та показникових (наприклад, EXP) елементарних функцій із регульованою точністю (для швидкої апроксимації, грубого обчислення та з коректним заокругленням), а також бібліотеки легких і швидких ГПВЧ, що мають задовільні статистичні властивості відповідно до тестів NIST STS, для застосування в кібербезпеці та захисті інформації.

7) Наведено приклад практичного застосування розробленого ГПВЧ rsqrt2dc_everyBit (1/0) на основі запропонованого методу DC апроксимації функції RSQRT у цифровій стеганографії. Цей генератор використано під час проєктування вдосконаленої моделі стеганосистеми на основі аналізу висококонтрастних та контурних ділянок цифрового зображення з використанням псевдовипадкової бітової маски, псевдовипадкового вибору пікселів, шифрування даних, перевірки їх цілісності та мінімізації довжини стеганографічного ключа.

8) 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 (залежно від алгоритму, типів даних та кількості ітерацій) в 2,2-21,2 раза (13-14 біт точності) порівняно з відомими алгоритмами, зокрема методами Мороза та ін., а для функції RSQRT – відповідно, в 2,2-32,9 раза (10-15 біт точності) порівняно з відомими алгоритмами, зокрема найкращими модифікаціями алгоритму FISR.

9) Завдяки використанню покращених алгоритмів на основі методу переключення магічних констант (DC) досягнуто зменшення максимальних відносних похибок у 11,8 раза у випадку двох піддіапазонів (13 біт точності) та 101,2 раза у випадку восьми піддіапазонів (16 біт точності) у порівнянні з методом Вальчика та ін. Показано, що у випадку програмної реалізації на

Raspberry Pi та ESP-32 метод DC демонструє у 1,8-3,6 раза кращу швидкодію за використання бібліотечних функцій, за винятком типу double на ESP-32. Ці алгоритми будуть особливо ефективними під час апаратної реалізації на ПЛІС та у вигляді швидких апаратних інструкцій математичних співпроцесорів, зокрема для мікроконтролерів та персональних комп'ютерів, забезпечуючи якісний компроміс між точністю, швидкодією та розміром пам'яті (таблиць пошуку).

10) 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 дисертації доповідалися здобувачем особисто та обговорювались на 5 міжнародних науково-технічних і науково-практичних конференціях, симпозіумах та консорціумах.

Загальна кількість наукових публікацій за темою дисертації становить **15**, з них **6** статей, у тому числі: **3** статті у періодичних фахових виданнях України з технічних наук, **1** з яких проіндексовано міжнародною наукометричною базою SCOPUS (квартиль Q3), **1** стаття у науковому періодичному виданні іншої держави, проіндексована міжнародними наукометричними базами SCOPUS та WEB OF SCIENCE (квартиль Q2), **1** розділ колективної монографії, опублікованої за кордоном за матеріалами конференції, **1** стаття в науковому нефаховому виданні України, та **9** публікацій в збірниках матеріалів і тез міжнародних науково-практичних конференцій, **2** з яких проіндексовано міжнародними наукометричними базами SCOPUS та WEB OF SCIENCE.

8. Короткий аналіз структури та змісту дисертаційної роботи.

Дисертаційна робота викладена на 288 сторінках, включаючи 168 сторінок основного тексту, та містить анотацію, зміст, перелік умовних позначень, вступ, чотири основних розділи, висновки, список використаних джерел, а також 8 додатків.

Робота написана грамотною українською мовою з використанням наукового стилю та коректної термінології. За своєю структурою, мовою та стилем викладення дисертація відповідає вимогам МОН України.

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 проведено огляд відомих методів обчислення елементарних функцій в арифметиці з рухомою комою та методів генерації псевдовипадкових послідовностей. Проведено огляд вітчизняної та закордонної наукової літератури за тематикою дослідження, здійснено аналіз, класифікацію та порівняння відомих методів, зокрема алгоритму FISR та відомих способів генерації ПВП для криптографічних та некриптографічних цілей. Визначено способи підвищення точності та швидкодії алгоритмів, а також здійснено аналіз методів оцінки якості ГПВЧ з урахуванням вимог кібербезпеки, сформульовано основні вимоги до проєктування нових та розробки вдосконалених алгоритмів для задач інформаційної та кібербезпеки, зокрема для генерації ПВП. Сформульовано вимоги до вдосконалених ГПВЧ та обґрунтовано вибір тестів NIST STS для подальшого дослідження.

У другому розділі розроблено основну методику проєктування та дослідження вдосконалених алгоритмів для обчислення елементарних функцій та для генерації ПВЧ на основі арифметики з рухомою комою. Застосовувалось імітаційне моделювання і модифікація параметрів алгоритмів з використанням чисельної багатовимірної оптимізації. Сформульовано методи оцінки похибок та точності алгоритмів, вимірювання швидкодії та аналізу збіжності. Запропоновано новий підхід до генерації ПВП для застосувань у сфері кібербезпеки та захисту інформації, що використовує рекурентне рівняння та чисельні методи в арифметиці з рухомою комою. Розроблено також методи автоматизації досліджень запропонованих ГПВЧ, зокрема статистичних характеристик, швидкодії та періоду повторення сформованих ПВП для різних початкових значень та параметрів генерації ПВП.

У третьому розділі запропоновано новий підхід до генерації псевдовипадкових чисел та послідовностей на основі чисельних методів апроксимації в арифметиці з рухомою комою, що орієнтовані на застосування в інформаційній та кібербезпеці. Для проєктування ГПВЧ розроблено наступні ефективні методи обчислення RCP, SQRT та RSQRT: на основі модифікованого методу Хаусхолдера 2-го порядку (Ho2), методи додаткових магічних констант (2MC/3MC), методи переключення магічних констант (DC/8DC). В залежності від початкового значення та обраних параметрів ГПВЧ 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 здійснено тестування та аналіз ефективності для задач інформаційної та кібербезпеки запропонованих алгоритмів та ГПВЧ на процесорах Intel Core i5/i7, одноплатних комп'ютерах із процесором ARM Cortex-A53 та мікроконтролерах ESP-WROOM-32. Зокрема, наведено результати практичного тестування точності, латентності та зворотної пропускної здатності запропонованих алгоритмів на прикладі функцій RCP та RSQRT. 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 раза швидші за апаратні генератори RDSEED та RDRAND. В кінці розділу досліджено сфери застосування та перспективні напрямки подальших досліджень. Запропоновано приклади практичного застосування розроблених ГПВЧ в задачах кібербезпеки та захисту інформації, зокрема в цифровій стеганографії.

У висновках було узагальнено основні наукові та практичні результати дисертації, наведено порівняння ефективності запропонованих методів, а також сформульовано рекомендації щодо впровадження та подальших досліджень, зокрема у сфері кібербезпеки та захисту інформації.

Список використаних джерел складається з 225 елементів.

9. Зауваження та дискусійні положення щодо змісту дисертації.

Незважаючи на загальне позитивне враження від дисертаційної роботи, варто відзначити деякі зауваження та дискусійні положення:

1) У вступі дисертації, у п.1. наукової новизни отриманих результатів, зазначено, що використання запропонованих ГПВЧ сприяло підвищенню рівня безпеки вдосконаленої стеганографічної системи, зокрема – забезпеченню цілісності даних. Водночас з тексту дисертації не зрозуміло, які саме механізми контролю або гарантування цілісності були застосовані, а також не розкрито, чи є запропоновані стеганографічні методи стійкими до активних атак, пов'язаних із спотворенням інформації.

2) Наукова новизна сформульована надто деталізовано, зокрема у частині, що стосується розробки удосконалених методів обчислення елементарних функцій. Доцільно об'єднати близькі за змістом положення для уникнення надмірної ієрархічної структури.

3) Усі реалізації запропонованих генераторів, що наведені в роботі, виконані з використанням чисельних методів в арифметиці з рухомою комою на основі чисел подвійної точності стандарту IEEE 754, що, зокрема, обмежує розрядність початкових значень до 64 біт. Такий розмір значення ініціалізації не забезпечує достатнього рівня захисту від атаки методом повного перебору. У роботі доцільно було б запропонувати також модифікації даних алгоритмів для початкових значень вищої розрядності.

4) У висновках до деяких розділів прослідковується повторення формулювань або злиття окремих результатів у складні конструкції. Було б доцільно зробити акценти більш чіткими відповідно до поставлених завдань. З іншого боку, у вступі формулювання деяких завдань є занадто детальним.

5) У роботі здійснено детальне статистичне тестування випадковості згенерованих ПВП на основі тестів NIST STS, графічних тестів, гістограм розподілу та ентропії, проте варто було б додатково дослідити проходження альтернативних статистичних тестів, зокрема DieHarder і TestU01.

6) Хоча здобувач не позиціонує запропоновані методи генерації ПВП як криптографічно стійкі, доцільно було б провести більш глибокий аналіз потенційної ефективності практичної реалізації основних типів атак на розроблені ГПВЧ, що базуються на основі покращених методів обчислення елементарних функцій в арифметиці з рухомою комою.

7) Під час оцінки прийнятної множини початкових значень запропонованих ГПВЧ враховувались результати статистичного тестування NIST STS, період повторення генераторів і кореляція згенерованих ПВП для близьких початкових значень. Водночас у роботі не наведено докладних кількісних результатів аналізу функцій кореляції та автокореляції залежно від величини ULP початкових значень.

Слід відзначити, що наведені зауваження не носять принципового характеру, не знижують наукової новизни та практичної значущості результатів дисертаційного дослідження, і не впливають на загальну позитивну оцінку дисертаційної роботи.

Загальні висновки щодо дисертаційної роботи.

Аналіз дисертаційної роботи Горячого Олега Ярославовича дозволяє дійти висновку, що дана робота є актуальним дослідженням щодо можливості використання арифметики з рухомою комою та методів швидкої апроксимації елементарних функцій у сфері кібербезпеки та захисту інформації, зокрема для генерації псевдовипадкових послідовностей на їх основі, що задовольняють вимогам статистичних тестів NIST STS. Вважаю, що одержані наукові результати можуть вплинути на подальший прогрес у сфері інформаційної та кібербезпеки, мають міждисциплінарне значення, оскільки можуть бути використані в інших галузях науки й техніки.

Дисертаційна робота Горячого О.Я. на тему «Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки» є завершеною, самостійною науково-дослідною роботою, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 «Інформаційні технології»). За своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає 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 рецензент:
кандидат технічних наук, доцент
доцент кафедри захисту інформації
Національного університету
«Львівська політехніка» _____ Олег ГАРАСИМЧУК

Підпис к.т.н., доцента Гарасимчука О.І.
засвідчую:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ • НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА" • ЗКПО 02071010

Проректор _____ Микола ЛОГОЙДА