ВІДГУК

офіційного опонента - доктора технічних наук, професора, завідувача кафедри кібербезпеки, національного технічного університету «Харківський політехнічний інститут» **ЄВСЕЄВА Сергія Петровича**

на дисертаційне дослідження

Дячука Ростислава Любомировича на тему **«Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел»**

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 121 - Інженерія програмного забезпечення

галузь знань 12 – Інформаційні технології

Актуальність дисертаційного дослідження.

Захист цифрової інформації, який будується на кибербезпеці, є надзвичайно актуальним завданням для інформаційних технологій загалом і програмної інженерії зокрема. Відомо багато засобів і технологій, направлених на вирішення цієї задачі. Зокрема це створення послідовностей випадкових чисел (ПВЧ), які часто застосовуються у криптографії. У представленому дисертаційному дослідженні розглядається саме цей напрямок, зокрема генерації ПВЧ із такого набору природних хаотичних процесів, як фотоелектричні явища. Дослідження Дячука Р.Л. в цьому напрямку, сприяють покращенню розуміння організації генерації високоентропійних ПВЧ для забезпечення захисту даних шляхом шифрування та кодування, зокрема створенням нових алгоритмів та програмного забезпечення на їх основі.

Виходячи з вище наведеного тема дисертаційної роботи Дячука Р.Л. є актуальним завданням програмної інженерії.

Існуючі в цьому напрямі технології, в яких застосовуються ПВЧ, залишають невивченими ряд питань. А саме як визначити оптимальне співвідношення між продуктивністю (швидкодією) генерації ПВЧ і їх надійністю. Також актуальним є питання на скільки ефективно може бути застосування клітинних автоматів для покращення хаотичності попередньо створеного ПВЧ. Доречним є питання швидкої перевірки ПВЧ не проводячи тести на відповідність вимогам стандартів NIST на ступінь хаотичності згенерованих ПВЧ. Актуальним є питання і пошуку нових джерел для генерації ПВЧ, здатних забезпечити максимальний рівень хаотичності та інші питання, які чекають своїх дослідників.

З огляду на вище наведене, дисертаційне дослідження Дячука Ростислава Любомировича «Розробка та дослідження інформаційної системи генерування

високоентропійної послідовності випадкових чисел», яка направлена на розв'язання вище перелічених питань, безумовно є актуальною.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконано на кафедрі програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича. Його зміст відповідає тематиці науково-дослідної роботи кафедри програмного забезпечення комп'ютерних систем: «Дослідження, моделювання та розробка програмного забезпечення складних динамічних систем» (Державний реєстраційний номер 0121U109232), а також у рамках акредитованої аспірантською програмою «Інженерія програмного забезпечення», яку закінчив дисертант. Тематика дослідження, висвітленого у опанованої дисертаційної роботи повністю відповідає згаданій освітньо-наукової програми III рівня вищої освіти та вище зазначеної теми науково-дослідної роботи кафедри.

Структура дисертації.

Дисертація є завершеної науково-дослідною роботою, що складається з анотації (українською та англійською мовами), змісту, переліку умовних скорочень, чотирьох розділів, висновків, списку використаних джерел та додатків.

У *вступі* обґрунтовано актуальність теми дисертаційного дослідження, визначено предмет і об'єкт дослідження, сформульовано мету та завдання дослідження, методи дослідження, наукову новизну, теоретичне та практичне значення отриманих результатів, подано відомості про апробацію роботи та наведено її структуру.

Перший розділ містить загальні відомості про теоретичні питання щодо генерації високоентропійних ПВЧ та дані про апаратні генератори ПВЧ. Показано їх переваги і недоліки. Показані відомі підходи до створення джерела ентропії та програмно-апаратного оточення генератора ПВЧ. Досліджено теоретичні засади оцінювання випадковості та ентропії. Здійснено детальний порівняльний аналіз найбільш відомих сучасних генераторів ПВЧ для систем криптобезпеки. Також, обґрунтовано доцільність проведення дослідження фото-електричних явищ (ФЕЯ) для застосування їх в якості джерела ентропії для генерації ПВЧ.

Матеріали розділу висвітлено у повній мірі, предметна галузь проаналізована ґрунтовно і достатньо глибоко, детально та всебічно обґрунтовано актуальність та завдання дисертаційного дослідження.

У другому розділі дисертаційного дослідження висвітлено результати дослідження фотоелектричних явищ, які запропоновано використовувати в якості джерел ентропії для генерації ПВЧ, а саме інтенсивності пікселів

зображення з веб-камери, або цифрової відеокамери, фото- та темнового струму фотодіода з високою квантовою ефективністю. Виявилося, що ПВЧ, згенерована за допомогою екстракції значень інтенсивності пікселів зображення відеокамери має непередбачуваний характер, а продуктивність у діапазоні від 85 до 288 Мбіт/сек, що, звісно не достатньо для сучасних криптографічних систем. Також така ПВЧ не пройшла тестування згідно вимогам стандартів NIST. Дослідження фотоструму фотодіода як джерела ентропії показало, що ПВЧ, створена на його основі, має продуктивність до 2 Мбіт/с і є непередбачуваною і частково відповідає тестам NIST. Дослідження темнового струму фотодіоду в якості джерела ентропії показало, що ПВЧ на його основі, має продуктивність до 980 Мбіт/сек та має високий рівень непередбачуваності. Автор також показує, що продуктивність такого способу створення ПВЧ можна збільшити, як що застосувати високочастотну апаратну частину. Вказується, що такі ПВЧ можна застосовувати як вектори ініціалізації для гібридних генераторів ПВЧ.

Досліджено гібридний генератора ПВЧ, який об’єднує усі три вище згаданих генератори, заснованих на фотоелектричних явищах і клітинних автоматів. Це об’єднання, як показує автор, забезпечує вирішення ряду питань. Зокрема питання швидкодії, надійності, контрольованості, відповідності статистичним вимогам та вимогам до безпеки і стабільності пост-обробки. Програмна частина розробленого гібридного генератора створює засади для масштабування та паралелізації процесу генерації, а також машинного навчання системи за допомогою нейронної мережи.

Третій розділ присвячено створенню інформаційної системи для генерації ПВЧ на основі усіх вище згаданих трьох генераторів із обробкою отриманих ПВЧ за допомогою клітинних автоматів. Використання у новоствореній інформаційній системі такого гібриду генераторів розв’язує питання про непередбачуваність, хаотичність, криптостійкість та ізольованість згенерованих послідовностей. Інтерфейс системи забезпечує керування процесом генерації ПВЧ, зокрема обирати джерело ПВЧ (база даних, файл, на основі відео-, або веб-камери, фото- та темнового струму фотодіода, гібридного з обробкою ПВЧ за допомогою клітинних автоматів); обирати між різними діапазонами значень (біти 0-1, стандартний діапазон 1-256, або користувацький діапазон); регулювати баланс між швидкістю генерації та рівнем безпеки (непередбачуваності), який забезпечує згенерована ПВЧ, зберігати отриману ПВЧ та аналізувати її.

Продуктивність генерації ПВЧ у межах створеної інформаційної системи знаходиться у межах 0,980 - 288 Мбіт/с і може бути суттєво збільшена при використанні високочастотної апаратної частини. Інформаційна система передбачає масштабування всієї програмної частини, або розпаралелювання

процесу обробки «сирої» ПВЧ всередині блоку програмної частини. З урахуванням вище вказаного, на прикладі ПВЧ, створених на основі відео-зображення або веб-камери, вдалося підвищити продуктивність у 4 рази.

У четвертому розділі висвітлено результати застосування розробленої інформаційної системи. А саме для формування вхідного вектора хеш-функції, для стеганографічних систем із підвищеними вимогами до прихованості та стійкості, а також для формування криптографічних ключів із високим рівнем ентропії та криптостійкості. Результати дослідження та розробки на їх основі інформаційної системи впроваджено у виробництво підприємств галузі. Зокрема удосконалений алгоритм створення хеш-функції, стеганографічні алгоритми та алгоритми генерації криптографічних ключів, впроваджені на ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» для підвищення криптостійкості програмного забезпечення.

Висновки дисертаційної роботи містять підсумок основних результатів дисертаційного дослідження. Вони сформульовані чітко, повністю охоплюють отримані результати і повністю задовольняють вимогам, що ставляться до результатів дисертації на здобуття наукового ступеня доктора філософії.

Список використаних джерел повністю охоплює предметну галузь і вказує на аналіз достатньої кількості літературних джерел, серед яких є роботи як українських, так і закордонних авторів.

Додатки містять список публікацій за темою дисертації, відомості про апробацію, акти впровадження результатів дисертаційної роботи та лістинг частини коду програмного забезпечення.

Наукова новизна одержаних результатів.

До нових та найбільш суттєвих наукових результатів дисертаційного дослідження Дячука Р.Л., на мою думку, можна віднести наступне:

1. 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;

2. 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 продуктивністю і низькою ресурсоємності функціоналу на КА; технологія генерації ПВЧ, що переходить на якісний рівень – неперервна генерація ПВЧ заданої продуктивності та якості.

На підставі вище наведеного вважаю, що наукові результати, отримані дисертантом під час виконання дисертаційного дослідження, є вагомим науковим внеском у технології та засоби генерації високоентропійних ПВЧ.

Достовірність отриманих результатів та висновків.

Достовірність результатів, висвітлених в дисертаційній роботі Дячука Р.Л., забезпечено коректним формулюванням мети та завдань дослідження, аргументованим вибором методів та засобів дослідження та розробки, послідовним їх розв'язанням поставлених завдань.

Достовірність наукових положень, висновків та рекомендацій, обґрунтовується та підтверджуються сучасними методами досліджень, які відповідають поставленій задачі, глибоким аналізом об'єкта та предмета дослідження за допомогою адекватних та актуальних методів, а також успішною апробацією отриманих результатів на всеукраїнських та міжнародних конференціях.

Практична цінність одержаних результатів.

Практична цінність наукових результатів дисертаційної роботи Дячука Р.Л. полягає у практичному застосуванні на сучасних українських підприємствах теоретичних положень методів та технологій ТДВ ЗАВОД «Кварц», Kaskad Developers Group та «Datawiz. Зокрема технологію екстракції ПВЧ з інтенсивності пікселів веб-камери, фото- та темнового струму фотодіода, оброблених за технологією клітинних автоматів та технологію генерації вхідного вектора геш-функцій, стеганографічних алгоритмів та алгоритмів генерації криптографічних ключів.

Результати дисертаційного дослідження використовуються у навчальних курсах кафедри програмного забезпечення комп'ютерних систем та кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича, а саме: «Криптографічний захист інформації», «Безпека в цифровому просторі», «Безпека програм та даних».

Оформлення результатів, дотримання вимог академічної доброчесності, повнота викладу наукових положень та результатів у публікаціях.

Дисертація має повний обсяг 260 сторінок друкованого тексту, при чому основна частина викладена на 137 сторінках. Список використаних джерел є репрезентативним.

Дисертація відповідає вимогам, які висуваються до її оформлення, відповідно до "Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)", що затверджений постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426), й "Вимог до оформлення дисертації" затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. У цілому зміст дисертації викладено послідовно та логічно..

Висока індивідуальність дисертаційної роботи підтверджується результатами перевірки на наявність академічного плагіату. Авторський стиль простежується по всьому тексту дисертації. Відсутні запозичення і використання результатів інших авторів без посилання на їхні джерела. Це підтверджує, що дисертаційна робота Дячука Р.Л. відповідає нормам академічної доброчесності.

Основні положення дисертації опубліковані у 1 статті, що індексується у наукометричній базі SCOPUS; 4 статтях, включених до переліку наукових фахових видань України; 7 робіт – у збірниках матеріалів міжнародних та всеукраїнських наукових конференцій. Отже, вимоги щодо кількості та якості наукових публікації автором виконано.

Зауваження по дисертаційній роботі:

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 НИСТ 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 відсутня структурна схема та опис її функціональності.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку виконаного дисертаційного дослідження та не зменшують її наукову новизну та практичну значущість і не знижують загального позитивного сприйняття проведеного обсягу досліджень.

Загальні висновки.

На основі критичного вивчення дисертації та праць здобувача, які опубліковані за темою дисертації, об’єктивно встановлено:

- дисертаційна робота Дячука Ростислава Любомировича відповідає чинним вимогам, які встановлені у «Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженого постановою Кабінету Міністрів України від 19 травня 2023 року № 502, та “Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії”, що затверджений постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами від 08 квітня 2025 року № 426).

- використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

- дисертаційна робота Дячука Ростислава Любомировича є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, які дозволяють підвищити ефективність виявлення та прогнозування інсайдерських загроз у хмарних сервісах інформаційних систем;

- автор дисертаційної роботи Дячука Ростислава Любомировича заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 «Інформаційні технології» за спеціальністю 121 – Інженерія програмного забезпечення.

Офіційний опонент:
Доктор технічних наук, професор,
Лауреат національної премії ім. Бориса Патона
завідувач кафедри кібербезпеки,
Національний технічний університет
«Харківський політехнічний інститут» Сергій ЄВСЕЄВ

Підпис
ЗАСВІДЧУЮ:
ЧЕНИЙ СЕКРЕТАР
ЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
" 20 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *