РЕЦЕНЗІЯ

на дисертаційну роботу
Горелікової Тетяни Олексіївни
на тему «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну»,
представлену на здобуття степеня доктора філософії
за спеціальність 122 Комп’ютерні науки

Актуальність теми дисертаційного дослідження. Дисертаційна робота Горелікової Т. О. присвячена вирішенню актуального науково-прикладного завдання у галузі комп'ютерних наук, пов'язаного із забезпеченням цілісності та захисту інформації в розподілених інформаційних системах на основі технології блокчейн. Актуальність обраної теми обумовлена стрімким розвитком децентралізованих цифрових платформ, широким впровадженням блокчейн-технологій у фінансовому секторі, державному управлінні, електронному документообігу та інших сферах, де висуваються підвищені вимоги до достовірності, незмінності та захищеності даних. Сучасні механізми консенсусу, що застосовуються у блокчейн-мережах, незважаючи на їх ефективність, мають певні обмеження щодо масштабованості, стійкості до окремих типів атак та забезпечення непередбачуваності процедур валідації. У зв'язку з цим дослідження, спрямоване на розроблення нових методів захисту інформації від підміни та видалення із застосуванням стохастичних алгоритмів і механізмів рандомізації, є своєчасним та відповідає сучасним напрямам розвитку інформаційних технологій і кібербезпеки.

Оцінка формулювання мети та завдань дослідження. Мета дисертаційної роботи сформульована чітко, логічно та відповідає предмету дослідження. Вона полягає у розробленні та науковому обґрунтуванні методів, стохастичних алгоритмів і програмно-технічних засобів захисту інформації від підміни та видалення у блокчейн-системах. Для досягнення поставленої мети авторкою сформульовано комплекс взаємопов'язаних наукових завдань, що охоплюють аналіз сучасного стану досліджуваної проблеми, побудову математичних моделей, розроблення алгоритмічного забезпечення, створення програмної реалізації та проведення експериментальної перевірки отриманих результатів. Завдання є достатньо повними, логічно взаємопов'язаними та послідовно реалізуються у структурі дисертаційної роботи. Такий підхід забезпечив досягнення поставленої мети та отримання нових наукових результатів.

Наукова новизна отриманих результатів. Наукова новизна дослідження полягає у системному розв'язанні актуальної науково-прикладної проблеми забезпечення цілісності даних шляхом створення рандомізованих алгоритмів,

математичних моделей та архітектурних підходів до захисту інформації від підміни та видалення в розподілених реєстрах.

Головним науковим здобутком авторки, який отримано вперше, є розроблена ймовірнісна модель рандомізованого підтвердження блоків і динамічного вибору вузлів-валідаторів. На відміну від існуючих детермінованих концепцій досягнення консенсусу, запропонований підхід ураховує нелінійну динаміку мережевих затримок та ймовірнісні характеристики компрометації вузлів, що усуває передбачуваність дій валідаторів і мінімізує вектор атак на процедури підтвердження даних. Важливим теоретичним результатом є виведені авторкою точні аналітичні та граничні ймовірнісні оцінки захищеності розподіленої системи за умов динамічної зміни конфігурації мережі, що дало змогу довести умови, за яких ймовірність успішної підміни чи видалення даних знижується.

Вагомий внесок здобувача полягає в удосконаленні методів формування криптографічно стійких випадкових послідовностей для валідації транзакцій шляхом інтеграції фізичних джерел ентропії. Це дозволило нівелювати вразливості, притаманні псевдовипадковим алгоритмам, та забезпечити принципово вищий рівень непередбачуваності вибірок. Крім того, у роботі зазнали суттєвого удосконалення алгоритми контролю цілісності, де застосування рандомізованого інспектування дозволило значно знизити комунікаційну складність досягнення консенсусу та обчислювальне навантаження на вузли мережі без зниження загального рівня довіри до системи.

Суттєвого подальшого розвитку в дисертації набув математичний апарат застосування марковських ланцюгів та теорії масового обслуговування для оцінки стійкості децентралізованих систем, що дало змогу формалізувати ймовірнісні переходи між безпечним і компрометованим станами реєстру. Дістали розвитку концептуальні засади побудови комп'ютерних систем із розподіленою архітектурою, у яких захист від викривлення даних розглядається не як сукупність ізольованих криптографічних засобів, а як фундаментальна системна властивість алгоритмів рандомізації та використовуваного ентропійного ресурсу.

Практичне значення одержаних результатів. Прикладна цінність здобутих результатів полягає у доведенні сформульованих теоретичних положень до рівня конкретних інженерно-програмних рішень, готових до розгортання в реальних інформаційно-комунікаційних середовищах.

Розроблені алгоритми рандомізованого вибору валідаторів та процедури підтвердження блоків дозволяють безпосередньо оптимізувати обчислювальне навантаження на вузли мережі й мінімізувати комунікаційні затримки при досягненні консенсусу. Запропоновані програмно-апаратні підходи до залучення фізичних джерел ентропії створюють практичне підґрунтя для побудови

високозахищених вузлів генерації випадкових послідовностей, стійких до спроб зовнішнього прогнозування чи маніпуляцій.

Отримані методичні інструменти та алгоритмічні специфікації можуть бути ефективно застосовані під час проектування, розробки та модернізації:

- державних електронних реєстрів, де критично важливо унеможливити заднім числом підміну або приховане видалення юридично значущих записів;
- банківських та фінансово-розрахункових платформ, які потребують високої швидкості обробки транзакцій при збереженні гарантованого рівня розподіленої довіри;
- корпоративних сховищ даних та систем електронного документообігу, які функціонують в умовах високих ризиків компрометації окремих сегментів мережі;
- об'єктів критичної цифрової інфраструктури, включно з медичними та логістичними інформаційними комплексами.

Крім того, сформульовані алгоритмічні схеми та результати симуляційного моделювання є повністю сформованими для використання у навчальному процесі закладів вищої освіти – зокрема при розробці спеціальних навчальних курсів із комп'ютерних наук, архітектури розподілених систем та сучасних методів криптографічного захисту інформації.

Оцінка змісту дисертаційної роботи. Зміст роботи повністю відповідає поставленій меті та сформульованим завданням дослідження. У першому розділі виконано ґрунтовний аналіз сучасного стану проблеми та існуючих методів забезпечення інформаційної безпеки у блокчейн-системах. Наступні розділи містять результати власних теоретичних і прикладних досліджень, математичне обґрунтування запропонованих методів, опис алгоритмів та результати їх експериментальної перевірки. Висновки до розділів є обґрунтованими та логічно випливають із проведених досліджень, а загальні висновки повною мірою відображають основні результати дисертаційної роботи.

Повнота викладу наукових положень, висновків і рекомендацій, сформульованих у дисертації, в опублікованих працях. Основні наукові результати дисертаційної роботи достатньою мірою висвітлені у семи наукових публікаціях авторки. Результати дослідження апробовані на міжнародних та всеукраїнських наукових конференціях, що свідчить про їх фахове обговорення. Публікації відображають основні положення дисертації, її наукову новизну, практичне значення та результати експериментальних досліджень. Обсяг і рівень апробації відповідають вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії.

Дискусійні положення та зауваження. Загалом позитивно оцінюючи дисертаційну роботу, вважаю за доцільне висловити окремі зауваження, які мають

рекомендаційний характер і не впливають на загальну позитивну оцінку дослідження.

1. Недостатньо чітко простежується специфіка саме захисту особистої інформації. Поняття «особиста інформація» винесено в назву роботи, однак по тексту майже не зустрічається.
2. Порівняння існуючих блокчейн-платформ переважно якісне. Відсутні чіткі кількісні критерії порівняння.
3. У другому розділі не достатньо детально описано експериментальне середовище. Не вказано інформацію про апаратну платформу, програмну реалізацію блокчейну, не наведено вихідні коди експерименту. Програмні коди з додатків є прикладом спрощеної демонстративної програмної реалізації.
4. Доцільно було б навести статистичний аналіз окремо для кожної метрики та кожної пари методів, а також розрахунки довірчих інтервалів.
5. На стор. 87 наведено ряд числових результатів у відсотках, але не вказано фактичних даних, звідки отримані такі результати.
6. Формула ефективного числа валідаторів потребує теоретичного обґрунтування. Чому саме така форма адекватно описує статистичну залежність вибору вузлів?

Загальний висновок. Дисертаційна робота Горелікової Тетяни Олексіївни тему «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну», є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають значення для розвитку комп'ютерних наук та інформаційної безпеки. За актуальністю, рівнем наукової новизни, обґрунтованістю отриманих результатів, їх теоретичним і практичним значенням, повнотою висвітлення результатів у наукових публікаціях та відповідністю встановленим вимогам дисертація відповідає вимогам Порядку присудження ступеня доктора філософії та вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії. Авторка дисертації, Горелікова Т. О., заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

Рецензент:
кандидат фізико-математичних наук, доцент,
професор кафедри програмної інженерії
Запорізького національного університету

О. В. Кудін