ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора Шевченко Анатолія Івановича на дисертаційну роботу Горелікової Тетяни Олексіївни на тему «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну», представлену на здобуття степеню доктора філософії за спеціальність 122 Комп'ютерні науки

Актуальність теми дисертаційного дослідження. Тема дисертаційної роботи присвячена розв'язанню важливого науково-прикладного завдання, що перебуває на перетині інформаційної безпеки, криптографії, розподілених інформаційних систем та сучасних блокчейн-технологій. В умовах стрімкого розвитку цифрової економіки, поширення децентралізованих сервісів і розширення сфер використання блокчейну – питання забезпечення цілісності інформації набуває особливого значення, оскільки саме достовірність і незмінність даних визначають рівень довіри до таких систем. Незважаючи на значну кількість наукових досліджень, присвячених механізмам консенсусу, проблема протидії підміні та несанкціонованому видаленню інформації шляхом удосконалення процедур валідації досі не має універсального вирішення. Саме тому обраний напрям дослідження є своєчасним і відповідає тенденціям розвитку комп'ютерних наук та інформаційної безпеки. Позитивне враження справляє те, що в роботі запропоновано розглядати забезпечення захисту даних не лише через удосконалення криптографічних механізмів, а й шляхом підвищення стійкості самого процесу прийняття рішень у блокчейн-мережі. Такий підхід дозволяє змістити акцент із традиційного захисту інформації на запобігання можливості компрометації процесів підтвердження даних, що є перспективним напрямом розвитку сучасних децентралізованих систем. Заслуговує на увагу поєднання математичного моделювання, стохастичних методів, криптографічних підходів та фізичних джерел ентропії в межах єдиної концепції підвищення безпеки блокчейн-систем. Така інтеграція різних наукових напрямів свідчить про комплексний характер проведеного дослідження та прагнення вирішити поставлену проблему не

локальними вдосконаленнями, а шляхом формування нового підходу до організації процесу валідації. Результати роботи потенційно можуть бути використані не лише у фінансових блокчейн-платформах, а й у державних інформаційних ресурсах, корпоративних системах, медичних інформаційних середовищах та системах штучного інтелекту, для яких гарантування цілісності інформації має критичне значення. Запропоновані у дисертації рішення спрямовані одночасно на підвищення захищеності, масштабованості, продуктивності та енергоефективності розподілених систем, що повністю відповідає сучасним вимогам до розвитку блокчейн-архітектур. Проблема досліджена з позицій не лише прикладного впровадження, а й розвитку теоретичних засад побудови механізмів консенсусу, що істотно розширює наукову значущість отриманих результатів. Сукупність наведених обставин свідчить про те, що тема дисертації є актуальною, відповідає сучасному рівню розвитку інформаційних технологій, має безперечне наукове та практичне значення, а виконане дослідження спрямоване на розв'язання важливої проблеми сучасної комп'ютерної науки.

Оцінка наукової новизни отриманих результатів. Наукова новизна дисертаційної роботи полягає у формуванні нового підходу до забезпечення цілісності інформації у блокчейн-системах шляхом удосконалення механізмів валідації блоків і транзакцій. На відміну від більшості сучасних досліджень, які переважно зосереджені на вдосконаленні окремих алгоритмів консенсусу або криптографічних методів, у роботі запропоновано інтегровану концепцію використання рандомізованого вибору валідаторів із застосуванням криптографічно захищених та фізичних джерел випадковості. Такий підхід дозволяє розширити існуючі уявлення про можливості підвищення безпеки блокчейн-мереж за рахунок зменшення передбачуваності процесів підтвердження даних. Важливою складовою наукової новизни є розроблення формалізованої моделі оцінювання ймовірності компрометації мережі, яка враховує параметри функціонування блокчейн-системи та характеристики випадкового вибору вузлів-валідаторів. Практичний інтерес становить також запропоноване авторкою використання фізичних джерел ентропії для формування випадкових послідовностей, що дозволяє підвищити криптографічну стійкість механізмів

рандомізації. Запропоновані рішення не обмежуються вдосконаленням окремого алгоритму, а формують концептуальні засади побудови більш адаптивних та стійких до компрометації децентралізованих інформаційних систем. Отримані результати доповнюють сучасний науковий напрям розвитку блокчейн-технологій і розширюють методологічний апарат досліджень у сфері інформаційної безпеки розподілених систем. У цілому представлені у дисертації наукові результати характеризуються достатнім рівнем новизни, відповідають заявленим авторкою положенням щодо одержання нових наукових результатів і становлять внесок у розвиток сучасних досліджень у галузі комп'ютерних наук.

Оцінка теоретичного та практичного значення результатів дослідження. Теоретичне значення дисертаційної роботи полягає у подальшому розвитку наукових засад забезпечення інформаційної безпеки розподілених систем шляхом застосування стохастичних механізмів керування процесами валідації. Запропоновані моделі та алгоритми розширюють існуючі підходи до побудови блокчейн-систем і дозволяють по-новому розглядати роль випадковості як одного з фундаментальних чинників підвищення стійкості механізмів консенсусу. Важливо, що результати дослідження мають не локальний характер, а можуть бути використані як теоретична основа для подальших наукових розробок у сфері криптографії, інформаційної безпеки, математичного моделювання та розподілених інформаційних технологій. Розроблені формальні моделі створюють підґрунтя для подальшого дослідження залежності між параметрами функціонування блокчейн-мереж та їх стійкістю до різних типів атак. Практичне значення роботи визначається можливістю використання запропонованих алгоритмів під час створення нових або модернізації існуючих блокчейн-платформ без необхідності принципової зміни їх архітектури. Практичну цінність підсилює орієнтація запропонованих механізмів на одночасне підвищення рівня безпеки, скорочення обчислювальних витрат, покращення масштабованості та підвищення продуктивності мережі. Результати дослідження можуть бути використані у фінансовому секторі, державних інформаційних системах, медичних інформаційних платформах, корпоративних мережах та сучасних системах штучного інтелекту, де вимоги до цілісності інформації постійно зростають.

Одержані результати мають достатній рівень універсальності та можуть бути адаптовані до різних архітектур розподілених систем, що істотно підвищує їх практичну цінність. Сукупність отриманих теоретичних положень, математичних моделей, алгоритмічних рішень та результатів експериментальних досліджень свідчить про вагоме теоретичне і практичне значення дисертаційної роботи для подальшого розвитку сучасних інформаційних технологій, криптографічних методів захисту даних і блокчейн-систем.

Оцінка повноти викладення результатів дисертації в наукових публікаціях. Основні результати дисертаційного дослідження достатньою мірою відображені у наукових публікаціях здобувачки. Результати роботи опубліковані у фахових наукових виданнях, що відповідають вимогам до публікації результатів дисертаційних досліджень, а також апробовані на міжнародних та всеукраїнських науково-практичних конференціях. Аналіз наведеного переліку праць свідчить, що публікації охоплюють основні етапи дослідження, відображають теоретичні положення, результати моделювання та запропоновані алгоритмічні рішення. Зміст опублікованих праць узгоджується з матеріалами дисертації, а основні наукові положення, висновки та результати отримали належне висвітлення та апробацію у науковому середовищі. Таким чином, повнота опублікування результатів дисертації відповідає вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії.

Оцінка дотримання вимог академічної доброчесності. Під час ознайомлення з дисертаційною роботою не виявлено ознак порушення принципів академічної доброчесності, визначених чинним законодавством України та нормативними документами Міністерства освіти і науки України. Структура дисертації характеризується логічною цілісністю, а виклад матеріалу має системний і послідовний характер, що свідчить про самостійне виконання дослідження. Зміст дисертації не справляє враження компілятивного викладу вже відомих наукових результатів, оскільки основна увага приділена обґрунтуванню власних наукових підходів та отриманих результатів. Використання загальновідомих положень сучасної теорії блокчейн-технологій, криптографії та інформаційної безпеки здійснюється виключно як теоретична основа для

формування власної концепції дослідження. Наведені у дисертації висновки відповідають отриманим результатам проведених досліджень і не містять необґрунтованих тверджень або висновків, які не підтверджуються змістом роботи. Особистий внесок здобувачки у виконання дисертаційного дослідження є чітко визначеним, а опубліковані у співавторстві наукові праці містять конкретизацію авторського внеску, що відповідає загальноприйнятій академічній практиці.

Зауваження та дискусійні положення. Оцінюючи науковий рівень дисертаційної роботи, її актуальність, новизну та практичну значущість, доцільно висловити окремі зауваження і міркування.

У роботі виконано порівняння запропонованого підходу з класичними механізмами консенсусу. Разом із тим для повнішого обґрунтування практичних переваг розробленого рішення доцільним могло б бути розширення порівняльного аналізу із сучасними модифікаціями консенсусних алгоритмів, що активно використовуються у новітніх блокчейн-платформах.

У дисертації розглянуто перспективи використання запропонованого підходу для захисту медичних даних та інтеграції із системами штучного інтелекту. Водночас зазначений напрям доцільно було б доповнити більш детальним аналізом особливостей практичного впровадження запропонованих рішень саме у таких прикладних інформаційних системах.

Окремі використані терміни та скорочення доцільно було б уніфікувати впродовж усього тексту дисертації, що сприяло б покращенню цілісності викладення матеріалу.

Викладені зауваження мають рекомендаційний характер, вони підтверджують перспективність запропонованого наукового напряму та доцільність його подальшого розвитку у майбутніх дослідженнях.

Загальний висновок. Дисертаційна робота є завершеним самостійним науковим дослідженням, у якому отримано нові науково обґрунтовані результати, що мають істотне значення для розвитку методів забезпечення цілісності інформації в блокчейн-системах та розширюють сучасні підходи до побудови захищених розподілених інформаційних систем.

За результатами аналізу змісту дисертації можна зробити висновок, що поставлену мету досягнуто, усі визначені завдання виконано, а сформульовані наукові положення, висновки та рекомендації є достатньо обґрунтованими, взаємопов'язаними та підтверджуються результатами проведених теоретичних і експериментальних досліджень.

Отримані результати характеризуються науковою новизною, мають теоретичне та практичне значення, достатньою мірою висвітлені у наукових публікаціях здобувачки та відповідають заявленому предмету дослідження. Під час ознайомлення з дисертаційною роботою не виявлено ознак порушення принципів академічної доброчесності. Висловлені у відгуку зауваження мають рекомендаційний та дискусійний характер, не впливають на загальну позитивну оцінку роботи та не знижують наукової цінності отриманих результатів.

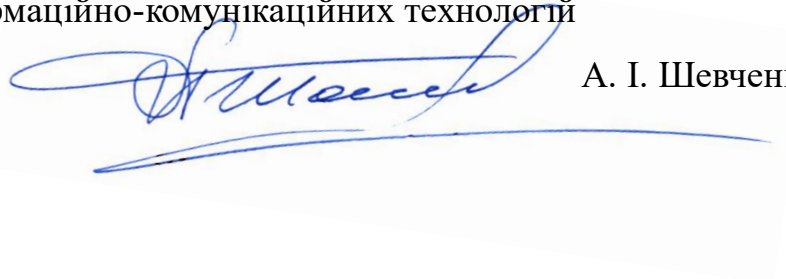
За актуальністю, науковою новизною, рівнем теоретичного опрацювання, практичною значущістю отриманих результатів, обґрунтованістю сформульованих висновків та відповідністю встановленим вимогам дисертаційна робота Горелікової Тетяни Олексіївни «Методи захисту особистої інформації від підміни та видалення з використанням технології блокчейну» відповідає вимогам 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 року № 44 (зі змінами), а її авторка Горелікова Т. О. заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології».

Офіційний опонент:

доктор технічних наук, професор,

професор Навчально-наукового інституту інформаційних технологій

Державного університету інформаційно-комунікаційних технологій



А. І. Шевченко