Голові разової спеціалізованої ради
Національного університету «Львівська політехніка»
д.т.н., професору
Пархуцю Любомиру Теодоровичу

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

кандидата технічних наук, доцента
завідувача кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка, факультету інформаційних технологій та математики, Київського столичного університету імені Бориса Грінченка
Складанного Павла Миколайовича
на дисертаційну роботу Балацької Валерії Сергіївни
«Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України»,
подану на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»)

1. Актуальність обраної теми дисертації

Цифрова трансформація державного управління та зростання обсягів персоніфікованих даних, що обробляються у державних реєстрах, висувають нові вимоги до забезпечення достовірності, цілісності та захищеності інформаційних транзакцій. Більшість наявних інформаційних систем державного сектору функціонують на централізованих архітектурах, які є вразливими до зовнішніх атак, внутрішніх зловживань і підробки даних, що у свою чергу може призвести до втрати довіри громадян, юридичних конфліктів та загроз національній безпеці.

В умовах підвищених кіберризиків і зростаючих вимог до прозорості публічних цифрових сервісів перспективним напрямом модернізації державних інформаційних ресурсів є впровадження дозвільних блокчейн-систем. Такі технології забезпечують незмінність даних, можливість формалізованого аудиту змін і контрольований доступ до реєстрових транзакцій. Разом із тим, використання блокчейн-технологій повинно бути доповнене ефективними методами перевірки достовірності інформації, з урахуванням ризиків, поведінкових особливостей користувача та контексту транзакцій.

Особливої актуальності набуває створення комплексного методу перевірки достовірності записів у державних реєстрах, що об'єднує криптографічні механізми (зокрема доведення з нульовим розголошенням), смартконтракти, поведінкову аналітику та машинне навчання. Такий підхід дозволяє не лише

забезпечити технічну цілісність даних, але й здійснювати семантико-контекстну оцінку правомірності змін, своєчасно виявляючи шахрайські або помилкові транзакції.

У зв'язку з цим, тема дисертаційного дослідження Балацької Валерії Сергіївни, присвячена розробці та впровадженню методу перевірки достовірності персональних даних у дозвільному блокчейн-середовищі на основі триетапної моделі SC–ZKP–ML, є актуальною та відповідає сучасним науковим і практичним запитам у сфері кібербезпеки державних інформаційних ресурсів.

Аналіз змісту дисертаційної роботи. Структура дисертації Балацької Валерії Сергіївни є традиційною та включає вступ, чотири розділи основного змісту, висновки, список використаних джерел та додатки. Кожен з розділів містить вагомий науковий внесок у розв'язання актуальної проблеми підвищення достовірності, надійності та безпеки транзакцій у державних інформаційних системах на основі дозвільного блокчейн.

У **вступі** чітко обґрунтовано актуальність теми в контексті цифровізації державного управління, зростання ризиків підробки персональних даних і недостатньої прозорості функціонування централізованих реєстрів. Сформульовано мету, завдання, об'єкт і предмет дослідження, визначено наукову новизну, методи дослідження, теоретичну й практичну значущість, а також наведено дані щодо апробації результатів.

У **першому розділі** подано аналітичний огляд сучасних підходів до забезпечення достовірності персональних даних у реєстрах, проаналізовано світовий досвід використання технологій блокчейн, смартконтрактів, криптографічних методів (включаючи ZKP), а також систем виявлення аномальної поведінки. Авторка обґрунтовує доцільність створення гібридного методу перевірки достовірності, що базується на поєднанні кількох механізмів контролю.

У **другому розділі** представлено теоретичні засади побудови триетапного методу SC–ZKP–ML, з описом кожного модуля: семантичного контролю (SC), криптографічного доведення (ZKP) та поведінкового аналізу (ML). Особливу увагу приділено математичній моделі оцінки довіри до транзакції на основі сигмоїдної функції, що враховує вагові коефіцієнти за результатами кожного з етапів перевірки. Запропоновано архітектуру взаємодії компонентів та логіку прийняття рішення в системі.

У **третьому розділі** розкрито реалізацію запропонованого методу в рамках програмного середовища Flask з використанням REST API, peer-інфраструктури на основі дозвільного блокчейн, смартконтрактів, криптографічних бібліотек та ML-модулів. Детально описано реалізацію логування, перевірки транзакцій, побудови peer-вузлів та маршрутизації запитів. Важливо, що реалізація демонструє не лише концепцію, а й практичну придатність запропонованої моделі.

Четвертий розділ присвячено експериментальній перевірці ефективності методу. Авторка провела серію тестів на моделюванні транзакцій у державному реєстрі, виявивши високу точність перевірки, стійкість до типових атак (включаючи підробку транзакції, неавторизоване внесення даних, перехоплення запитів), а також добру масштабованість peer-мережі. У роботі представлено численні графіки, діаграми, скріншоти та статистику, що підтверджують ефективність запропонованого підходу в порівнянні з традиційними схемами перевірки.

У **висновках** підсумовано основні наукові результати, що досягнуті в межах дисертаційного дослідження, та наведено рекомендації щодо можливого впровадження запропонованого методу в державних інформаційних системах.

2. Наукова новизна одержаних результатів

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

- *вперше запропоновано* триетапну модель перевірки достовірності транзакцій у дозвільних блокчейн-системах, яка поєднує: семантичний аналіз структури транзакції засобами смартконтрактів (SC), криптографічну перевірку достовірності з використанням доведення з нульовим розголошенням (ZKP), а також поведінкову оцінку дій користувача на основі алгоритмів машинного навчання (ML). Такий підхід забезпечує багаторівневу перевірку до запису транзакції в блокчейн, що підвищує стійкість до компрометації та маніпуляцій.
- *вперше розроблено* математичний апарат оцінки ризику недостовірності транзакцій на основі сигмоїдної функції з ваговими коефіцієнтами, що дозволяє визначати інтегральну довіру до транзакції в режимі реального часу з урахуванням результатів кожного етапу перевірки. Це забезпечує ефективну автоматизовану фільтрацію підозрілих транзакцій і підвищує рівень захисту персональних даних.
- *отримав* подальший розвиток семантико-поведінковий підхід до верифікації транзакцій, який передбачає урахування часових, мережевих та історичних параметрів дій користувачів. Це дозволяє не лише оцінити зміст транзакції, а й ідентифікувати потенційні відхилення від нормативної поведінки, зокрема за умов внутрішніх загроз або участі ботів.
- *удосконалено* модель інтегральної оцінки достовірності транзакції, що передбачає використання узагальненої логістичної функції замість бінарної оцінки модулів SC, ZKP та ML. Такий підхід зменшує суб'єктивність рішень, знижує вплив людського фактору й дозволяє масштабувати модель на інші реєстрові системи.
- *удосконалено* математичний апарат перевірки, який поєднує логістичну регресію, теорію ймовірностей і нечітку логіку для моделювання рівня ризику транзакції у випадках обмеженого доступу до її повного змісту. Це забезпечує

гнучкість і адаптивність моделі до змінних загрозових сценаріїв.

• *удосконалено* метод виявлення фальсифікованих транзакцій шляхом інтеграції контекстних параметрів користувача, історії активності й поведінкових шаблонів. Це дозволило підвищити точність виявлення несанкціонованих дій і зменшити ризики втручання у цифрові реєстри державного значення.

Зазначені результати свідчать про суттєвий науковий внесок у розвиток сучасних підходів до забезпечення достовірності, цілісності та безпеки даних у державних цифрових системах на основі технологій дозвільного блокчейн.

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

Наукове значення проведеного дослідження полягає в обґрунтуванні та реалізації ефективного методу перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, який поєднує засоби смарт-контрактів, криптографічні протоколи доведення з нульовим розголошенням та поведінковий аналіз з використанням алгоритмів машинного навчання. Такий підхід дозволяє забезпечити більш високий рівень довіри до даних користувачів, зменшити ризики підробки транзакцій, унеможливити зовнішнє втручання у верифікацію та значно підвищити рівень кіберзахисту цифрових державних сервісів.

Результати, отримані в межах дисертаційної роботи, становлять цінність для наукових досліджень у галузях кібербезпеки, криптографічного захисту, цифрової ідентифікації, управління інформаційними ризиками, а також можуть бути практично використані в системах електронного врядування. Окрему значущість становить запропонований авторкою підхід до побудови сигмоїдної моделі інтегральної оцінки довіри на основі вагових коефіцієнтів, що відображають внесок кожного етапу перевірки – структурного, криптографічного та поведінкового – у загальну оцінку достовірності.

Одержані результати можуть бути впроваджені у навчальний процес для здобувачів спеціальності 125 «Кібербезпека та захист інформації», зокрема в курсах, що стосуються криптографічних протоколів, безпеки цифрових сервісів, архітектури захисту державних реєстрів та інтелектуальних методів аналізу подій інформаційної безпеки. Вони також можуть бути використані як основа для лабораторних робіт і практичних кейсів у межах функціонування кіберполігонів і тренажерів верифікації транзакцій з використанням блокчейн-середовищ.

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

Результати, викладені в дисертаційній роботі, ґрунтуються на чітко сформульованих завданнях та ретельно обґрунтованій методології дослідження. Кожне положення дисертації логічно випливає з поставлених цілей і базується на

відповідному математичному апараті, що забезпечує послідовність у побудові моделі перевірки достовірності транзакцій.

Особливістю роботи є вдало реалізований симбіоз трьох підходів до верифікації – структурного, криптографічного та поведінкового – який був інтегрований у математичну модель ризику на основі сигмоїдної функції. Така модель забезпечила логічно завершене прийняття рішень у дозвільному блокчейн-середовищі, що підтверджує її обґрунтованість і практичну релевантність.

Математичний апарат реалізований коректно, адекватно до завдань моделювання ризику недостовірності. Експериментальна перевірка в тестовому середовищі показала високу точність роботи моделі, що додатково підтверджує її достовірність. Новизна роботи проявляється у створенні інтегрованого методу верифікації транзакцій, здатного працювати в умовах змінних загроз із використанням даних у реальному часі.

5. Практичне значення одержаних результатів полягає у тому, що:

• розроблено метод перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, який реалізовано у вигляді REST API-сервісу в середовищі Flask із використанням технологій Hyperledger Fabric. Запропонована триетапна модель включає структурну, криптографічну та поведінкову перевірку транзакцій, що дає змогу інтегрувати її в цифрові державні сервіси, зокрема «Дія», ЄДДР, eHealth та інші реєстри, які працюють із персональними даними;

• експериментально підтверджено ефективність функціонування запропонованої моделі: зафіксовано можливість обробки до 4,8 транзакцій на секунду при середньому часі відповіді 0,21 с, що відповідає сучасним вимогам до продуктивності цифрових державних реєстрів. У тестовій мережі з 6 peer-вузлами досягнуто часу відповіді 0,063 с при обробці 300 транзакцій, що свідчить про високу масштабованість;

• реалізовано математичну модель інтегральної оцінки достовірності транзакцій, яка використовує сигмоїдну функцію з ваговими коефіцієнтами для прийняття автоматизованих рішень без участі оператора. Зазначений підхід забезпечує адаптивність до змін поведінкових шаблонів користувача та знижує частку хибнопозитивних результатів до 34%, що підвищує надійність верифікації в IT-системах державного сектору;

• впроваджено поведінкову перевірку транзакцій на основі методів машинного навчання, яка аналізує часові, мережеві та контекстуальні параметри користувача. Експериментальні дослідження показали, що модель ефективно виявляє фальсифіковані й аномальні транзакції, зокрема атаки Unauthorized Submit, Sniffed Replay та Brute-force Payload, що підвищує стійкість цифрових сервісів до кіберзагроз;

• запропоновано алгоритм ризик-орієнтованої верифікації, який поєднує логістичну регресію, теорію ймовірностей і елементи нечіткої логіки. Алгоритм забезпечив автоматизовану оцінку рівня довіри до транзакцій за часовими, мережевими та поведінковими характеристиками, знизивши рівень хибнопозитивних рішень до 3,7% і підвищивши точність верифікації на 15,1% у порівнянні з одноетапними моделями та на 6,7% – з двоетапними, що суттєво зменшує потребу в ручному контролі транзакцій у державних системах.

6. Повнота оприлюднення результатів дисертаційної роботи

Результати дисертаційного дослідження Балацької Валерії Сергіївни отримали належне представлення у відкритому науковому просторі. Здобувачкою підготовлено 23 наукові публікації за тематикою дисертації, з яких 11 статей (у тому числі 7 – у фахових наукових виданнях України та 4 – у періодичних виданнях, що виходять за кордоном) і 12 тез доповідей, оприлюднених на міжнародних та всеукраїнських науково-практичних конференціях. Це свідчить про ґрунтовну апробацію теоретичних положень і прикладних результатів дисертаційної роботи.

Особистий внесок здобувачки у колективних наукових публікаціях полягає у формуванні концепції дослідження, математичному та програмному обґрунтуванні запропонованих моделей, а також у реалізації і тестуванні запропонованого методу. У тексті дисертації використано лише ті результати, які були безпосередньо отримані авторкою самостійно.

7. Оцінка структури дисертації, її мови та стилю викладення

Структура дисертаційної роботи Балацької Валерії Сергіївни є логічно вибудуваною, узгодженою з вимогами Міністерства освіти і науки України до дисертацій на здобуття наукового ступеня. Зміст розділів послідовно розкриває мету, завдання, методологію, результати дослідження та їх практичне застосування.

Мова дисертації – грамотна, літературна, відповідає академічному стилю. Виклад матеріалу чіткий, науково обґрунтований і легко сприймається. Текст роботи відзначається використанням сучасної термінології у сфері інформаційної безпеки, криптографії, блокчейн-технологій та машинного навчання.

Порушення академічної доброчесності у роботі не виявлено. Усі використані джерела належним чином процитовані, наведено відповідні посилання на роботи інших авторів. Анотація повно та коректно відображає основний зміст, наукову новизну й висновки дисертації.

8. Зауваження та дискусійні положення щодо змісту роботи

Загалом, позитивно оцінюючи дисертаційне дослідження Балацької Валерії Сергіївни, доцільно висловити низку зауважень, що мають уточнювальний або дискусійний характер:

1. У розділі 3, присвяченому математичному моделюванню ризику недостовірності транзакцій, не наведено достатнього обґрунтування вибору саме сигмоїдної функції як основи моделі інтегральної довіри. Доцільно було б розширити аналіз шляхом порівняння з іншими можливими підходами, такими як дерева рішень або баєсівські моделі, з метою виявлення переваг саме запропонованого підходу.

2. У загальних висновках дисертації (стор. 207–210) подано значущі метрики ефективності реалізованої SC–ZKP–ML моделі, зокрема підвищення точності до 93,4% та зменшення хибнопозитивних рішень до 3,7%. Проте чітко не вказано, у порівнянні з якими альтернативними підходами отримано такі показники, та в якому саме тестовому середовищі вони є релевантними. Це ускладнює повноцінне трактування ефективності моделі в прикладному контексті.

3. У підрозділі 4.2.3 подано опис захисту від типових атак на блокчейн-середовище, зокрема Unauthorized Submit і Brute-force Payload. Водночас методика вимірювання ефективності захисту та точність виявлення залишаються недостатньо деталізованими. Доцільно було б вказати конкретні значення хибнопозитивних і хибнонегативних спрацьовувань, що дозволило б точніше оцінити якість запропонованих механізмів.

4. Значна частина практичних експериментів реалізована у Flask-середовищі з використанням peer-вузлів Hyperledger Fabric. Водночас відсутній аналіз ефективності впровадженої моделі на інших блокчейн-платформах, таких як Ethereum, Corda чи Quorum, що обмежує можливість масштабування або адаптації до альтернативних середовищ.

5. У підрозділі 3.2.3, де аналізуються ризик-орієнтовані алгоритми верифікації, авторка вдало поєднує логістичну регресію, нечітку логіку та ймовірнісні підходи. Проте обґрунтування переваг саме такої комбінації над класичними rule-based або деревовидними системами прийняття рішень є недостатньо повним. Доцільним було б коротко пояснити, в чому полягає виграш такої інтеграції з позиції точності, адаптивності або стійкості до аномалій.

Зазначені зауваження мають дискусійний характер і не впливають на загальну позитивну оцінку дисертаційної роботи, яка вирізняється високим рівнем теоретичної обґрунтованості, інноваційною методичною базою та прикладною цінністю для галузі кібербезпеки.

Загальні висновки щодо дисертаційної роботи

Дисертаційна робота Балацької Валерії Сергіївни на тему «Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України» є завершеним, самостійним дослідженням, що відповідає паспорту спеціальності 125 «Кібербезпека». Робота містить як наукову новизну, так і практичну цінність одержаних результатів, які

спрямовані на підвищення рівня достовірності та безпеки персональних даних у цифрових державних системах.

Запропонований здобувачкою метод перевірки достовірності транзакцій із використанням триетапної моделі (структурна перевірка, криптографічна верифікація, поведінковий аналіз на основі машинного навчання) дозволяє суттєво підвищити точність і надійність обробки персональних даних у дозвільному блокчейн-середовищі. Побудована математична модель інтегральної оцінки довіри до транзакцій на основі сигмоїдної функції дозволяє адаптивно реагувати на аномальні дії та зменшує ризик прийняття недостовірних даних. Ефективність розробленого підходу підтверджено експериментальними тестами у середовищі Flask та Hyperledger Fabric із використанням REST API.

Отримані результати можуть бути впроваджені в державні інформаційні системи, зокрема в реєстри, що містять критичну персональну інформацію (наприклад, «Дія», ЄДДР, eHealth), забезпечуючи підвищений рівень їх стійкості до типових кіберзагроз, таких як несанкціоноване втручання, повторне відтворення, підробка транзакцій тощо.

Враховуючи актуальність теми, наукову новизну, глибину проведеного аналізу, обґрунтованість отриманих результатів і їх практичну значущість, вважаю, що дисертаційна робота Балацької Валерії Сергіївни повністю відповідає вимогам «Порядку присудження ступеня доктора філософії» (Постанова Кабінету Міністрів України від 12.01.2022 № 44), а її авторка заслуговує на присудження наукового ступеня доктора філософії зі спеціальності 125 «Кібербезпека».

Офіційний опонент:
завідувача кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного
університету імені Бориса Грінченка
кандидат технічних наук, доцент Павло СКЛАДАННИЙ