РЕЦЕНЗІЯ

Кандидата технічних наук, доцента
доцента кафедри захисту інформації
Совина Ярослава Романовича
Національного університету «Львівська політехніка»
на дисертаційну роботу
Балацької Валерії Сергіївни
«Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України»,
поданої на здобуття наукового ступеня доктора філософії за спеціальністю
125 «Кібербезпека»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертації.

В умовах масштабної цифровізації державних послуг, реєстрів та ідентифікаційних платформ гарантування достовірності персональних даних користувачів набуває стратегічного значення для забезпечення національної безпеки. Це особливо актуально на тлі зростання кількості цілеспрямованих кібератак, які проникають навіть у формально захищені системи, використовуючи прогалини у верифікації змісту транзакцій, правомірності дій та поведінкових відхилень користувачів.

Дисертаційна робота Балацької Валерії Сергіївни спрямована на вирішення комплексної науково-прикладної проблеми – розробку та впровадження багаторівневого методу верифікації достовірності транзакцій у державних інформаційних системах на основі дозвільного блокчейн-середовища. Сутність методу полягає в об'єднанні структурного аналізу, криптографічної перевірки з нульовим розголошенням та поведінкової оцінки на основі машинного навчання, що забезпечує багатоаспектну оцінку достовірності ще до моменту фіксації транзакції у блокчейн.

Обрана тематика є актуальною як у контексті впровадження принципів Privacy by Design, так і в контексті забезпечення відповідності чинному законодавству України (Закон № 4336-IX) та вимогам міжнародних стандартів у сфері захисту персональних даних (GDPR, ISO/IEC 27701).

Запропонований метод верифікації SC–ZKP–ML забезпечує новий рівень контекстно-чутливої перевірки транзакцій, який поєднує технічну, правову та поведінкову достовірність даних і відповідає викликам цифрової безпеки у державному секторі.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри .

Тематика дисертаційного дослідження відповідає науковим напрямам кафедри захисту інформації Національного університету «Львівська політехніка», зокрема дослідженню систем криптографічного захисту даних, архітектур цифрових платформ, механізмів достовірності інформації, а також технологій виявлення аномалій у поведінці користувачів. Робота спрямована на удосконалення методів верифікації персональних даних у державних реєстрах з використанням дозвільного блокчейн-середовища, смарт-контрактів, доведення з нульовим розголошенням та машинного навчання, що є актуальним у межах формування інформаційної безпеки держави, розвитку засобів протидії підробці цифрових транзакцій та побудови національних систем цифрової довіри.

Наукова новизна основних результатів дисертації полягає в розробленні методології перехресного впровадження провідних стандартів аудиту з кібербезпеки:

1. **Вперше розроблено** триетапну модель перевірки достовірності транзакцій у дозвільних блокчейн-середовищах за рахунок поєднання перевірки структури транзакції засобами смарт-контрактів, криптографічної валідації за допомогою протоколу доведення з нульовим розголошенням та поведінковим аналізом користувача з використанням алгоритмів машинного навчання. Розроблена триетапна модель перевірки достовірності транзакцій дозволила забезпечити багаторівневу перевірку достовірності даних до моменту запису у блокчейн та підвищило рівень захищеності від компрометації користувачів у цифрових державних платформах.

2. **Вперше розроблено** математичний апарат обчислення ризику недостовірності транзакцій у дозвільних блокчейн-середовищах на основі сигмоїдної функції з ваговими коефіцієнтами, що відображають вплив кожного етапу перевірки, структурного, криптографічного та поведінкового, на загальний рівень довіри до даних користувачів. Математичний апарат реалізовано через інтегровану логістичну функцію, що забезпечує ухвалення рішень у режимі реального часу, що підвищило точність автоматизованого відсіву транзакцій із високим ризиком та забезпечило підвищення захисту персональних даних у державних інформаційних системах в режимі реального часу.

3. **Отримав подальший розвиток** семантико-поведінковий метод верифікації транзакцій у дозвільних блокчейн-середовищах, за рахунок введення часових характеристик запитів, мережевих характеристик, історії змін, а також процесу перевірки типових дій користувачів. Удосконалений семантико-поведінковий метод верифікації транзакцій дає змогу аналізувати транзакцію не лише за змістом, а й за контекстом її створення, що дозволяє підвищити

ефективність виявлення фальсифікацій та аномалій, зокрема в умовах атак із внутрішнього середовища або за участі автоматизованих ботів.

Ступінь обґрунтованості наукових положень дисертації і їх достовірність та новизна.

Наукові положення, сформульовані у дисертації, відзначаються достатнім рівнем обґрунтованості, що базується на глибокому аналізі сучасних нормативних вимог, моделюванні ризиків та використанні інструментів криптографічного і поведінкового контролю транзакцій. Запропонований триетапний метод перевірки достовірності включає формалізовані алгоритми структурної валідації, доведення з нульовим розголошенням та машинного навчання, що підтверджує комплексний підхід до оцінки достовірності персональних даних.

Архітектурні та алгоритмічні рішення дисертації реалізовані у вигляді прототипу з REST API, що дозволило здійснити апробацію запропонованих підходів у дозвільному блокчейн-середовищі. Новизна результатів полягає у поєднанні декількох незалежних рівнів перевірки в єдину модель прийняття рішень, здатну реагувати на поведінкові аномалії та криптографічні порушення в реальному часі. Достовірність наукових положень підтверджується логічною завершеністю дослідження та результатами імітаційного моделювання.

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

Отримані результати автором, мають значення для розвитку наукових підходів до забезпечення достовірності персональних даних у державних інформаційних системах, з урахуванням сучасних викликів у сфері цифрової безпеки, побудови довірчих платформ, а також реалізації принципів кібергігієни в архітектурах на базі дозвільного блокчейн-середовища.

Результати дисертаційної роботи Балацької Валерії Сергіївни впроваджені у навчальний процес кафедри «Захист інформації» Національного університету «Львівська політехніка» при вивченні дисципліни «Нормативно-правове забезпечення та міжнародні стандарти кібербезпеки» для студентів першого рівня вищої освіти напрямку підготовки 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів полягає у можливості безпосереднього застосування запропонованого триетапного методу перевірки достовірності транзакцій у дозвільному блокчейн-середовищі державних інформаційних систем, зокрема таких, що працюють із критично важливими персональними даними.

1. Експериментально підтверджено, що триетапна модель перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, яка впроваджена у Flask-середовищі з використанням REST API та платформи Hyperledger Fabric, на відміну від централізованих, дозволяє забезпечити модульну побудову системи перевірки достовірності транзакцій та швидше масштабування при інтеграції з державними інформаційними платформами. За результатами тестування проваджена модель перевірки достовірності транзакцій продемонструвала ефективну роботу з обробкою до 4,8 транзакцій на секунду та середнім часом відповіді 0,21 с, що відповідає вимогам до цифрових державних реєстрів у публічному секторі.

2. Реалізована математична модель інтегральної оцінки достовірності транзакцій, що експериментально впроваджена у дозвільному блокчейн-середовищі на основі сигмоїдної функції з ваговими коефіцієнтами, забезпечила автоматизоване ухвалення рішень без участі оператора. Застосування математичної моделі інтегральної оцінки достовірності транзакцій, дозволило зменшити кількість транзакцій із хибно позитивними результатами до 34% та забезпечило адаптивну реакцію системи на зміну поведінкових шаблонів користувачів, що у свою чергу, підвищило точність і надійність функціонування механізмів перевірки у державних реєстрах.

3. Проведена тестова реалізація моделі поведінкової перевірки достовірності транзакцій в дозвільному блокчейн-середовищі на основі Flask-додатку та алгоритмів машинного навчання, які аналізують часові, мережеві та типові сценарії поведінки користувача, забезпечує виявлення усіх фальсифікованих та аномальних транзакцій включно зі сценаріями атак Unauthorized Submit, Sniffed Replay та Brute-force Payload, у порівнянні з результатами структурної та криптографічної перевірки, що дозволило підвищити рівень захисту від компрометації персональних даних у державних цифрових системах.

4. Впроваджена гібридна модель триетапної перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, яка включає модулі структурної перевірки, криптографічної перевірки на основі доведення з нульовим розголошенням та поведінкової перевірки із застосуванням методів машинного навчання, дала змогу адаптувати систему перевірки достовірності транзакцій до змінних сценаріїв загроз, що підтверджено в межах експериментального тестування. Під час тестування з обробкою 300 транзакцій у мережі з 6 peer-вузлами модель продемонструвала високу продуктивність із середнім часом відповіді 0,063 секунди, що підтверджує її ефективність для використання у масштабованих державних реєстрах із підвищеними вимогами до захищеності.

5. Експериментально підтверджено, що алгоритм ризик-орієнтованої верифікації реалізований на основі REST API та платформи Hyperledger Fabric, який поєднує елементи логістичної регресії, теорії ймовірностей і нечіткої логіки, забезпечив можливість автоматизованої оцінки рівня довіри до транзакції з урахуванням її часових, мережевих і поведінкових параметрів. Впроваджений алгоритм ризик-орієнтованої верифікації дозволив знизити рівень хибнопозитивних рішень до 3,7% і підвищив точність оцінки достовірності транзакцій до 15,1% у повірянні з одноетапним та до 6,7% з двоетапним, що дозволяє зменшити навантаження на операторів ручної перевірки у державних системах, орієнтованих на обробку персональних даних.

Запропонований метод верифікації транзакцій, який об'єднує криптографічну, структурну та поведінкову перевірку, дозволяє державним реєстрам, таким як ЄДДР, eHealth, Реєстр виборців та ін., досягти вищого рівня стійкості до цілеспрямованих атак, підвищити прозорість доступу та зменшити кількість фальсифікованих або ризикованих записів у базах персональних даних. Запропоновані технічні рішення забезпечують скорочення часу перевірки, автоматизацію модерації та можливість масштабування на інші платформи цифрового урядування, що свідчить про реальну прикладну цінність дисертаційного дослідження.

Результати дисертаційної роботи впроваджено з метою покращення внутрішніх процесів, пов'язаних з інформаційною безпекою, і сприяння забезпеченню статусу відповідності міжнародним стандартам інформаційної безпеки в організаціях Національний університет «Львівська політехніка», Львівський державний університет безпеки життєдіяльності, УАРНЕТ, Навчально-методичний центр цивільного захисту та безпеки життєдіяльності Львівської області.

Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дослідження оприлюднено у 23 наукових публікаціях, серед яких 11 статей у фахових наукових виданнях (включно з тими, що індексуються в Scopus) та 12 тез доповідей на міжнародних науково-практичних конференціях, що засвідчують апробацію положень дисертації.

Статті у наукових фахових виданнях України:

1. Балацька В. С., Опірський І. Р. (2023) Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну // Кібербезпека: освіта, наука, техніка. – 2023. – № 4 (20). – С. 6-19. DOI: https://doi.org/10.28925/2663-4023.2023.20.619

2. Opirskyy I., Balatska V., Poberezhnyk V. (2023) Modern possibilities of use blockchain technology in the education system // Ukrainian Scientific Journal of

Information Security. – 2023. – Vol. 29, issue 3. – P. 138-146. DOI: https://doi.org/10.18372/2225-5036.29.18073

3. Балацька В. С., Побережник В. О., Опірський І. Р. (2024) Використання Non-Fungible Tokens та блокчейн для розмежування доступу до державних реєстрів // Кібербезпека: освіта, наука, техніка. – 2024. – № 4 (24). – С. 99-114. DOI: https://doi.org/10.28925/2663-4023.2024.24.99114

4. Balatska V., Opirskyy I. (2024) Blockchain as a tool for transparency and protection of government registries // Ukrainian Scientific Journal of Information Security. – 2024. – Vol. 30, issue 2. – P. 221-230. DOI: https://doi.org/10.18372/2225-5036.30.19211

5. Балацька В. С., Побережник В. О. (2024) Концепція застосування блокчейн-технологій для підвищення захищеності персональних даних платформи «Дія»: відповідність вимогам GDPR та українському законодавству // Кібербезпека: освіта, наука, техніка. – 2024. – № 2 (26). – С. 268-290. DOI: https://doi.org/10.28925/2663-4023.2024.26.681

6. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. (2024) Методи та моделі проєктування системи автоматизованого пошуку вразливостей у Web-додатках // Вісник Львівського державного університету безпеки життєдіяльності. – 2024. – № 30. – С. 110-122. DOI: https://doi.org/10.32447/20784643.30.2024.11

7. Балацька В. С., Побережник В. О., Стефанків А. В., Шевчук Ю. А. Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. Комп'ютерні системи та мережі. 2025. Т. 7, № 1. С. 1–16. DOI: https://doi.org/10.23939/csn2025.01.001

Статті у наукових періодичних виданнях інших держав, що включені до міжнародної наукометричної бази даних (Scopus):

8. Poberezhnyk V., Balatska V., Opirskyy I. (2023) Development of the learning management system concept based on blockchain technology // CEUR Workshop Proceedings. – 2023. – Vol. 3550 : Cybersecurity providing in information and telecommunication systems II 2023. – P. 38-49. URL: https://ceur-ws.org/Vol-3550/

9. Balatska V., Poberezhnyk V., Petriv P., Opirskyy I. (2024) Blockchain application concept in SSO technology context // CEUR Workshop Proceedings. – 2024. – Vol. 3654 : Cybersecurity Providing in Information and Telecommunication Systems. – P. 38-49. URL: https://ceur-ws.org/Vol-3654/

10. Balatska V., Poberezhnyk V., Opirskyy I. (2024) Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR // CEUR Workshop Proceedings. – 2024. – Vol. 3800 : Cyber Security and Data Protection. – P. 70-80. URL: https://ceur-ws.org/Vol-3800/

11. Balatska V., Opirskyy I., Slobodian N. (2024) Blockchain for enhancing transparency and trust in government registries // CEUR Workshop Proceedings. –

2024. – Vol. 3826 : Cybersecurity Providing in Information and Telecommunication Systems II. – P. 50-59. URL: https://ceur-ws.org/Vol-3826/

Наукові публікації у збірниках матеріалів та тез конференцій:

12. Балацька В. С., Опірський І. Р. Механізми досягнення надійності в блокчейні для захисту персональних даних // Захист інформації і безпека інформаційних систем : матеріали IX Міжнародної науково-технічної конференції (Львів, 25–26 травня 2023 р.). – 2023. – С. 17-18.

13. Балацька В. С., Побережник В. О., Опірський І. Р. Потенційне використання технології блокчейн в уряді // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. – 2023. – С. 228-230.

14. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція використання технології блокчейн у сфері освіти // Інформаційна безпека та інформаційні технології : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. – 2023. – С. 386-388.

15. Балацька В. С., Побережник В. О., Опірський І. Р. Технології блокчейн, NFT та IPFS для підвищення ефективності та безпеки державних реєстрів України // Безпека інформаційних технологій : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (9–11 травня 2024, Львів, Україна). – 2024. – С. 51-52.

16. Балацька В. С., Опірський І. Р. Підвищення безпеки державних реєстрів України за допомогою трьохфакторної аутентифікації на основі блокчейн // Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів : тези доповідей Всеукраїнської науково-практичної конференції (21 червня 2024, Вінниця, Україна). – 2024. – С. 585-588.

17. Побережник В. О., Балацька В. С., Опірський І. Р. Адаптація блокчейн облікових даних до вимог GDPR // Інноваційні технології у розвитку сучасного суспільства : тези доповідей VI Міжнародної науково-практичної конференції, 10–11 жовтня 2024 року, Львів. – 2024. – С. 39-41.

18. Балацька В. С., Опірський І. Р. Впровадження блокчейн-технологій для забезпечення безпеки та прозорості державних реєстрів // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези доповідей III Міжнародної науково-практичної конференції, 21 листопада 2024 року, Хмельницький. – 2024. – С. 1094-1096.

19. Балацька В. С., Побережник В. О. Використання технологій блокчейн та NFT для розмежування доступу до державних реєстрів // Інформаційна безпека

та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 6–8.

20. Балацька В. С., Опірський І. Р. Технологія блокчейн для забезпечення довіри та прозорості у державних реєстрах // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 251-253.

21. Побережник В. О., Балацька В. С., Опірський І. Р. Концепція самосуверенної ідентичності як альтернатива традиційним методам автентифікації // Інформаційна безпека та інформаційні технології, ІБІТ 2024 : збірник доповідей V Міжнародної науково-практичної конференції, м. Львів, 27 листопада 2024 року. – 2024. – С. 262-265.

22. Балацька В. С., Побережник В. О. Інформаційна безпека державних реєстрів: потенціал блокчейну для захисту критично важливих даних // Міжнародна та національна безпека: теоретичні і практичні аспекти : матеріали IX Міжнародної науково-практичної конференції, 21 березня 2025 р., м. Дніпро. Ч. 2. – Дніпро, 2025. – С. 468–471.

23. Побережник В. О., Балацька В. С. Концепція цифрового суверенітету в умовах розвитку блокчейн-економіки // Матеріали Міжнародної науково-практичної конференції «Blockchain Technologies and Engineering 2025» (BTE 2025), м. Київ, 26 березня 2025 р. – Київ: ІПМЕ НАН України, 2025. – С. 75–76.

Зауваження по дисертації.

1. У першому розділі доцільно було б детальніше представити порівняльний аналіз існуючих підходів до перевірки достовірності транзакцій у державних реєстрах, включаючи аналіз сильних і слабких сторін сучасних моделей у контексті цифрового врядування.

2. Важливою складовою представленого методу є математична модель інтегральної оцінки достовірності транзакцій. Однак у дисертації недостатньо обґрунтовано вибір вагових коефіцієнтів у сигмоїдній функції, що визначають вплив структурного, криптографічного та поведінкового компонентів. Відсутність емпіричних або аналітичних критеріїв визначення цих ваг знижує прозорість і повторюваність результатів. Для підвищення наукової валідності слід було б подати більше аргументів щодо методики їхнього встановлення, наприклад – через апроксимацію на основі експериментальних даних або використання статистичних підходів.

3. У підрозділі, присвяченому реалізації поведінкової перевірки, доцільно розширити опис характеристик тестового набору транзакцій, зокрема методику його генерації, щоб повніше оцінити узагальнювальну здатність моделі.

4. У частині з описом моделювання атак бажано додати пояснювальні підписи до деяких графіків і таблиць, оскільки окремі зображення мають недостатній рівень самодостатності для читача без звернення до тексту.

5. У тексті роботи зустрічаються абревіатури, які не завжди пояснені при першому використанні, що може ускладнити розуміння при ознайомленні з матеріалом читачам, не знайомим із термінологією в галузі блокчейн та кібербезпеки.

Слід відзначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок.

Не зважаючи на виявлені недоліки, дисертаційна робота Балацької Валерії Сергіївни на тему «Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України» є завершеною науковою працею, яка представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека» (галузь знань 12 «Інформаційні технології»), яка за своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає паспорту спеціальності 125 «Кібербезпека» та чинним вимогам, які встановлені у «Порядку присудження ступеня доктора філософії», який затверджений Постановою Кабінету Міністрів України від 12.01.2022 р. №44, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний рецензент
Кандидат технічних наук, доцент,
Доцент кафедри захисту інформації
Національного університету
«Львівська політехніка» Ярослав СОВИН

Підпис к.т.н, доцента Совина Я.Р. засвідчую
Вчений секретар
Національного університету
«Львівська політехніка»
к.т.н., доцент Роман БРИЛИНСЬКИЙ