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

ВІДГУК
офіційного опонента
доктора технічних наук, професора Смірнова Олексія Анатолійовича
завідувача кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
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»)

1. Актуальність теми дисертації.

Однією з ключових умов успішного функціонування цифрової держави є забезпечення достовірності та захищеності персональних даних, які обробляються у державних інформаційних системах. У процесі розбудови електронного урядування, зокрема через масштабне впровадження цифрових сервісів, постає новий виклик – не лише зберегти конфіденційність даних, а й гарантувати їхню правдивість, цілісність і обґрунтованість в умовах зростаючих ризиків маніпуляцій та атак.

На сьогодні більшість державних цифрових реєстрів в Україні базуються на централізованих моделях з обмеженим рівнем гнучкості та прозорості. Традиційні підходи до контролю доступу (ACL, RBAC), а також застосування електронного підпису чи сертифікатів забезпечують лише технічну формальну валідацію транзакцій, не охоплюючи їхню логіку, правомірність чи поведінкові аномалії. Як наслідок, у системах з високим рівнем критичності – таких як реєстри нерухомості, виборців, соціальних виплат чи медичних даних – зберігається ризик появи недостовірної інформації, що може мати істотні правові, фінансові та соціальні наслідки.

Актуальність дослідження зумовлена потребою в інтеграції сучасних технологій – зокрема дозвільного блокчейн, смарт-контрактів, Zero-Knowledge Proof та алгоритмів машинного навчання – для створення нових, стійких до фальсифікацій методів перевірки достовірності персональних даних. У роботі запропоновано системний підхід до верифікації, який виходить за межі класичної перевірки цифрового сліду і орієнтований на змістовний, семантичний і поведінковий аналіз транзакцій у реальному часі. Це дозволяє не лише виявляти

підозрілі дії, а й прогнозувати потенційні загрози ще до внесення змін у розподілений реєстр.

З урахуванням сучасних вимог законодавства України (Закон № 4336-IX) та міжнародних нормативів (GDPR, ISO/IEC 27701), тема дослідження є надзвичайно важливою як для теорії кібербезпеки, так і для практики побудови цифрових державних сервісів. Результати, що викладені у дисертації, спрямовані на вирішення актуального міждисциплінарного завдання – підвищення ефективності захисту персональних даних шляхом комплексної, достовірної та ризик-орієнтованої верифікації у середовищі, яке підтримує контрольовану децентралізацію та довіру між суб'єктами.

2. Аналіз змісту дисертаційної роботи.

Дисертаційна робота Балацької Валерії Сергіївни «Підвищення ефективності захисту персональних даних користувачів в умовах цифрової інформатизації державних реєстрів України» має чітку структуру, високий ступінь логічної послідовності й узгодженості між окремими розділами, що свідчить про глибоке розуміння авторкою теми та системний підхід до вирішення поставленого наукового завдання.

У **вступі** обґрунтовано актуальність теми, чітко сформульовано мету, завдання, об'єкт і предмет дослідження, наведено стислий огляд нормативно-правових та технологічних передумов, а також висвітлено зв'язок роботи з науковими програмами й практичними ініціативами, у яких брала участь здобувачка. Вступ визначає теоретичні рамки і водночас містить обґрунтовану мотивацію щодо вибору технологічного стеку – блокчейн, ZKP, ML – для побудови системи верифікації.

У **першому розділі** авторкою проведено аналітичний огляд сучасного стану захисту персональних даних, особливо в контексті державних реєстрів. Значну увагу приділено аналізу міжнародних стандартів (GDPR, ISO/IEC 27001, 27701), українського законодавства (зокрема Закону № 4336-IX) та класифікації типів достовірності інформації. На основі огляду сформульовано ключову проблему: недостатність класичних засобів для забезпечення семантичної та поведінкової верифікації транзакцій.

У **другому розділі** дисертації висвітлено концептуальні засади побудови моделі виявлення загроз у дозвільному блокчейн-середовищі. Авторка, здійснила критичний аналіз традиційних підходів до аналізу загроз (зокрема STRIDE, DREAD, NIST SP 800-30, MITRE ATT&CK) і обґрунтувала їхню обмежену придатність у контексті децентралізованих систем, що не мають єдиного контрольного центру. Враховуючи специфіку обробки персональних даних у дозвільних блокчейн, здобувачкою запропоновано адаптивну поведінкову модель ідентифікації загроз, яка ґрунтується на комплексному аналізі часових параметрів транзакцій, мережевих характеристик та динаміки дій користувачів. Важливою особливістю цієї моделі є використання механізмів токенізації на основі NFT для гнучкого управління доступом, що дозволяє поєднати контрольовану прозорість із захистом чутливих даних.

У **третьому розділі** реалізовано головну наукову ідею дисертації – метод багаторівневої перевірки достовірності транзакцій (SC–ZKP–ML), який включає: смарт-контрактну перевірку структури запису; доказ із нульовим розголошенням для підтвердження правомірності дій; поведінкову перевірку за допомогою алгоритмів машинного навчання.

Окремо слід відзначити математичну модель інтегральної оцінки довіри до транзакції, запропоновану здобувачкою: вона використовує сигмоїдну функцію для агрегування результатів трьох перевірок і ухвалення автоматизованого рішення в реальному часі.

У **четвертому розділі** дисертаційної роботи зосереджено увагу на експериментальній перевірці ефективності запропонованого методу верифікації достовірності транзакцій. Балацькою В.С. реалізовано прототип системи у Flask-середовищі з використанням REST API та дозвільного блокчейн-платформи Hyperledger Fabric. Для підтвердження працездатності триетапної моделі було змодельовано 300 транзакцій із різним ступенем ризику, на основі яких проведено кількісний аналіз за основними критеріями: точність, швидкодія та стійкість до атак. Середній час обробки однієї транзакції склав 0,066 секунди, а досягнутий рівень точності перевірки становив 93,4%, що є переконливим результатом для систем реального часу.

Окрему цінність має моделювання п'яти типів потенційно небезпечних впливів (DoS, Brute-force Payload, Unauthorized Submit, Sniffed Replay, підміна транзакції), що дозволило оцінити стійкість архітектури до різнотипних загроз. Авторка також здійснила порівняльний аналіз із одно- та двоетапними підходами до верифікації, продемонструвавши переваги запропонованого методу за інтегральними показниками достовірності, швидкодії та гнучкості контролю. Запропоновано методику масштабування рішення та його інтеграцію з цифровими платформами публічного сектору, що підтверджує практичну придатність і перспективність розробки.

Таким чином, дисертаційна робота має логічно завершену структуру, достатній обсяг теоретичних обґрунтувань, інноваційних технічних рішень та експериментальних результатів. Здобувачка продемонструвала здатність поєднувати сучасні концепції кібербезпеки з технологіями блокчейн і машинного навчання, формуючи нову архітектуру довіри в державних реєстрах.

3. Наукова новизна одержаних результатів. Основні наукові положення, результати та висновки дисертації, отримані здобувачкою Балацькою Валерією Сергіївною самостійно, є новими, достатньо обґрунтованими й підтверджуються результатами експериментального моделювання, логічного аналізу та комп'ютерної реалізації прототипу розробленого методу. Достовірність положень і висновків забезпечена коректним використанням сучасного математичного апарату, принципів поведінкової аналітики, методології блокчейн-моделювання, а також практичними результатами тестування системи. У дисертаційній роботі отримано наступні результати, що мають наукову новизну:

1. **Вперше запропоновано** триетапну модель перевірки достовірності транзакцій у дозвільному блокчейн-середовищі, яка включає послідовне застосування: перевірки структури транзакції засобами смарт-контрактів; криптографічної перевірки з використанням доведення з нульовим розголошенням; та поведінкової перевірки на основі алгоритмів машинного навчання. Такий підхід дозволяє реалізувати глибоку верифікацію перед записом транзакції в реєстр та мінімізує ризики компрометації даних.

2. **Вперше розроблено** математичну модель інтегральної оцінки довіри до транзакції на основі логістичної сигмоїдної функції, яка враховує ваговий вплив кожного етапу перевірки. Це забезпечує автоматизоване ухвалення рішень у режимі реального часу, з підвищеною точністю відсіву транзакцій із високим ризиком та посиленням захисту персональних даних у державних ІТ-системах.

3. **Удосконалено** метод семантико-поведінкової верифікації транзакцій, шляхом урахування часових і мережевих характеристик, історії змін і шаблонів дій користувача. Це дозволяє аналізувати не лише вміст транзакції, а й контекст її створення, що підвищує здатність системи виявляти фальсифікації та аномалії, зокрема в умовах внутрішніх або автоматизованих атак.

4. **Удосконалено** модель інтегральної перевірки достовірності даних у дозвільному блокчейн-середовищах за рахунок використання узагальненої функції прийняття рішень, що враховує не бінарну оцінку, а вагову релевантність кожного з трьох етапів перевірки. Це зменшує залежність результату від людського втручання та покращує надійність оцінки.

5. **Удосконалено** математичний апарат ризик-орієнтованої перевірки транзакцій, який базується на поєднанні логістичної регресії, ймовірнісних методів і нечіткої логіки. Запропонований підхід дозволяє адаптувати систему до динамічних умов цифрового середовища та враховує багатофакторний вплив на ступінь довіри до кожної транзакції.

6. **Удосконалено** метод виявлення фальсифікованих транзакцій шляхом використання поведінкових шаблонів і контекстних перевірок параметрів користувачів, що забезпечує ефективну фільтрацію підозрілих звернень і підвищує рівень захищеності цифрових державних реєстрів від спроб несанкціонованого доступу.

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

Наукове значення виконаного дисертаційного дослідження полягає у розробці ефективного методу перевірки достовірності транзакцій у дозвільних блокчейн-середовищах, який забезпечує підвищену точність верифікації даних користувачів, а також стійкість до різних типів атак. Запропоновані підходи до інтеграції смарт-контрактів, протоколів доведення з нульовим розголошенням і машинного навчання мають міждисциплінарний характер і можуть бути використані у наукових дослідженнях із захисту персональних даних, цифрової ідентифікації, ризик-орієнтованого управління даними та безпечного

електронного врядування.

У навчальних програмах ці результати можуть бути інтегровані в курси з інформаційної безпеки, криптографії, інтелектуального аналізу даних, а також у спеціалізовані дисципліни, присвячені архітектурі захисту державних реєстрів. Зокрема, результати дослідження можуть бути використані в освітньому процесі при вивченні дисциплін «Інформаційна безпека в державному секторі», «Криптографічні протоколи», «Захист інформації в розподілених системах», «Безпека цифрових сервісів», що викладаються у межах підготовки здобувачів за спеціальністю 125 «Кібербезпека та захист інформації».

Отримані в дисертації результати можуть бути також корисними для розробки практичних кейсів і лабораторних робіт у віртуальних полігонах кіберзахисту, що моделюють роботу блокчейн-платформ із розподіленою автентифікацією і збереженням персональних даних. У галузі машинного навчання результати дослідження можуть використовуватись як приклади реалізації поведінкових моделей перевірки достовірності, що враховують часові, мережеві та контекстні характеристики, з можливістю адаптації до сценаріїв реального часу.

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

При вирішенні поставлених завдань Балацька Валерія Сергіївна проаналізувала значний масив сучасної літератури з кібербезпеки, блокчейн-технологій та методів машинного навчання. Для формалізації результатів застосовано підходи системного аналізу, криптографічного моделювання, теорії ймовірностей і поведінкової аналітики.

Наукові положення обґрунтовано на основі моделювання в дозвільному блокчей-середовищі, з подальшою валідацією результатів у Flask-прототипі. Достовірність забезпечується кількісними експериментами, а також публікаціями у фахових виданнях і апробацією на конференціях. Отримані результати свідчать про новизну і практичну цінність запропонованого підходу.

6. 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 платформи Hyperledger Fabric. Запропонована триетапна модель забезпечує структурну, криптографічну та поведінкову перевірку транзакцій, що дозволяє інтегрувати її в цифрові державні сервіси, зокрема платформу «Дія», ЄДДР, eHealth та інші реєстри, які працюють з персональними даними.
- експериментально підтверджено ефективність функціонування системи: зафіксовано можливість обробки до 4,8 транзакцій на секунду зі середнім часом відповіді 0,21 с, що відповідає вимогам до продуктивності цифрових державних реєстрів. У тестовій мережі з 6 peer-вузлами модель продемонструвала високу масштабованість, забезпечивши час відповіді 0,063 с при обробці 300 транзакцій.

• реалізовано математичну модель інтегральної оцінки достовірності транзакцій, яка використовує сигмоїдну функцію з ваговими коефіцієнтами для прийняття автоматизованих рішень без участі оператора. Модель забезпечує адаптивність до змін поведінкових шаблонів користувача та зменшує кількість хибно позитивних результатів до 34%, що покращує надійність верифікації в державних ІТ-системах.

• впроваджено поведінкову перевірку на основі машинного навчання, яка аналізує часові, мережеві та контекстуальні параметри користувача. Результати експериментів засвідчили ефективне виявлення фальсифікованих і аномальних транзакцій, включно з атаками Unauthorized Submit, Sniffed Replay та Brute-force Payload, що підвищує стійкість цифрових сервісів до типових кіберзагроз.

• запропонований алгоритм ризик-орієнтованої верифікації, що поєднує логістичну регресію, теорію ймовірностей та елементи нечіткої логіки, забезпечив автоматизовану оцінку рівня довіри до транзакцій за їх часовими, мережевими та поведінковими характеристиками. Алгоритм зменшив рівень хибнопозитивних рішень до 3,7% та підвищив точність верифікації на 15,1% у порівнянні з одноетапними моделями та на 6,7% – з двоетапними, що значно скоротило потребу в ручному контролі при обробці персональних даних.

7. Повнота оприлюднення результатів дисертаційної роботи.

Основні результати дисертаційного дослідження Балацької Валерії Сергіївни достатньо повно відображено у 23 наукових публікаціях, зокрема: в одинадцяти статтях (із них сім – у фахових виданнях України та чотири – у періодичному виданні закордоном), а також у дванадцяти тезах доповідей на міжнародних і всеукраїнських науково-практичних конференціях. Це свідчить про належну апробацію положень дисертації.

Особистий внесок здобувачки у колективно опублікованих працях полягає у формуванні ідеї дослідження, розробці моделей, обґрунтуванні методів верифікації та практичній реалізації результатів. У дисертації використано лише ті наукові результати, які здобувачка отримала самостійно.

8. Оцінка структури дисертації, її мови та стилю викладення.

Дисертаційна робота має чітко визначену структуру, що логічно відображає етапи наукового дослідження та відповідає вимогам Міністерства освіти і науки України. Розділи подані послідовно – від вступу з обґрунтуванням мети й завдань дослідження до загальних висновків. Кожен розділ містить завершену змістовну частину, яка розкриває окремий аспект дослідження, забезпечуючи логічну єдність усього тексту.

У роботі використано сучасну фахову термінологію з кібербезпеки, блокчейн-технологій і захисту персональних даних. Текст викладено зрозуміло, грамотно, без надмірної описовості, з чітким дотриманням стилістичної єдності та академічної мови.

У дисертації дотримано принципів академічної доброчесності: усі використані джерела коректно процитовано, наведено посилання на наукові

публікації, програмні реалізації та нормативно-правові документи, що свідчить про повагу здобувачки до авторського права та стандартів академічної етики.

9. Зауваження та дискусійні положення щодо змісту роботи.

Незважаючи на загальне позитивне враження від дисертаційної роботи, слід зазначити деякі зауваження та виокремити окремі положення, що викликають наукову дискусію:

1. У підрозділі 1.3.1 наведено характеристику вимог до систем захисту персональних даних у державних реєстрах згідно із законом № 4336-IX та принципами Privacy by Design. Проте, авторці слід було б докладніше розглянути потенційні конфлікти між вимогами законодавства щодо захисту даних та технічними обмеженнями дозвільного блокчейн-середовища, зокрема в аспекті обмеження права на забуття.

2. У підрозділі 2.2 представлено архітектуру достовірності у вигляді трирівневої SC–ZKP–ML моделі, однак не подано чіткої формалізації процесу взаємодії модулів за умов неповного або спотвореного вхідного вектора. В подальших дослідженнях доцільно розширити математичний опис поведінки системи при часткових втратах даних.

3. У підрозділі 4.2.2 авторка детально дослідив масштабованість peer-мережі на базі Hyperledger Fabric при зміні кількості вузлів. Водночас залишаються відкритими питання щодо впливу асиметричного розподілу транзакцій на пропускну здатність системи в умовах реального навантаження. Цей аспект потребує глибшого аналізу.

4. У підрозділі 4.2.3 надано результати моделювання типових атак, зокрема Unauthorized Submit та Sniffed Replay, однак не представлено окремий розгляд складних сценаріїв багатоетапних комбінованих атак, що характерні для сучасних кібервикликів на державні платформи.

5. У підрозділі 4.3 виконано порівняльний аналіз розробленого методу з існуючими, однак критерії відбору аналогів не повною мірою відображають актуальні державні платформи, наприклад, не враховано механізми перевірки транзакцій у системі «Дія».

Вказані положення мають дискусійний характер та можуть слугувати підґрунтям для подальших досліджень, не знижуючи наукової цінності та практичної значущості виконаної роботи.

Загальні висновки щодо дисертаційної роботи.

Аналіз дисертаційної роботи Балацької Валерії Сергіївни дозволяє дійти висновку, що представлена праця є актуальним і завершеним дослідженням, спрямованим на вирішення однієї з ключових проблем сучасної кібербезпеки — захисту достовірності та конфіденційності персональних даних у державних інформаційних системах. Робота відзначається високим рівнем наукової обґрунтованості, інноваційністю обраного підходу та практичною спрямованістю запропонованих рішень.

Отримані в дисертації результати мають важливе значення для розвитку методів ризик-орієнтованої верифікації користувачів, побудованої на триетапній

моделі перевірки (SC–ZKP–ML) у дозвільному блокчейн-середовищі. Запропонована методика дозволяє істотно підвищити достовірність транзакцій, забезпечити виявлення аномалій, мінімізувати ймовірність кіберзагроз і забезпечити відповідність вимогам нормативних актів (GDPR, ISO/IEC 27701, Закон України №4336-IX).

Розроблений метод продемонстрував ефективність у реальних тестових сценаріях, зокрема в середовищі Flask та мережі Hyperledger Fabric, що дозволяє рекомендувати його до впровадження у державні реєстрові системи. Практичне впровадження підкріплене апробацією результатів у понад 20 наукових публікаціях, включаючи фахові журнали та міжнародні конференції.

Беручи до уваги актуальність, наукову новизну, обґрунтованість висунутих положень, повноту дослідження та значущість отриманих результатів, вважаю, що дисертаційна робота Балацької Валерії Сергіївни повністю відповідає вимогам наказу МОН України № 40 від 12.01.2017 р. та Постанови Кабінету Міністрів України № 44 від 12 січня 2022 р., а її авторка заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека».

Офіційний опонент:

завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнського національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис доктора технічних наук, професора,
завідувача кафедри кібербезпеки та програмного
забезпечення Центральноукраїнського національного
технічного університету Смірнова Олексія
Анатолійовича засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного
університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
“ 28 ” 07 2025 року