

РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента кафедри технологій цифрового розвитку Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій,

Аронова Андрія Олексійовича на дисертаційну роботу **Шахматова Івана Олександровича «Моделі та методи забезпечення довіри й цілісності у вебсистемах»** подану на здобуття наукового ступеня доктора філософії за спеціальністю 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології»

Актуальність теми дисертаційної роботи. Актуальність теми дисертаційної роботи Шахматова І.О. «Моделі та методи забезпечення довіри й цілісності у вебсистемах» не викликає сумнівів, оскільки сучасні вебсистеми є основою функціонування електронної комерції, корпоративних інформаційних сервісів, онлайн-оплат, державних електронних послуг та інших цифрових платформ, що обробляють значні обсяги критично важливих даних. За таких умов особливого значення набувають питання забезпечення довіри до результатів обробки інформації, збереження цілісності даних, перевірюваності критичних дій користувачів і адміністраторів, а також можливості доказового аудиту після інцидентів. У сучасних умовах вебсистеми функціонують у середовищі постійного зростання кількості та складності кіберзагроз. Порушення цілісності даних, прихована модифікація журналів подій, неправомірний доступ, SQL-ін'єкції, DDoS-атаки, компрометація облікових записів і масовий вебспам можуть призводити не лише до технічних збоїв, а й до фінансових втрат, репутаційних ризиків, зниження доступності сервісів та втрати довіри до результатів їх роботи. Особливо важливою є проблема забезпечення такого рівня контролю, за якого критичні події можуть бути не лише зафіксовані, а й надалі перевірені, відтворені та використані як доказова основа для аналізу інцидентів. Традиційні засоби захисту, моніторингу та журналювання залишаються необхідними, однак не завжди забезпечують достатній рівень незмінності записів, простежуваності дій і підтвердження коректності прийнятих рішень у багатокомпонентних вебархітектурах. Водночас окреме використання блокчейн-технологій або методів машинного навчання не повністю розв'язує проблему забезпечення довіри й цілісності, оскільки потребує їх узгодженого поєднання в межах єдиної архітектурної моделі вебсистеми.

З огляду на це, обрана здобувачем тема є своєчасною та науково обґрунтованою. Вона спрямована на розробку моделей і методів, які поєднують криптографічну фіксацію критичних подій, блокчейн-верифіковане журналювання, контроль доступу, аудит змін і графово-нейромережеве

виявлення вебспау та підозрілої активності. Такий напрям дослідження відповідає сучасним потребам інженерії програмного забезпечення, оскільки орієнтоване на підвищення довіри до даних, рішень і механізмів їх перевірки у вебсистемах. Актуальність дисертаційної роботи додатково підтверджується її зв'язком із науково-дослідними роботами Державного університету інформаційно-комунікаційних технологій, спрямованими на забезпечення функціональної стійкості інформаційних систем та побудову захищених інформаційних систем із централізованим управлінням. Це свідчить про відповідність теми дисертації сучасним науковим і практичним завданням у галузі інформаційних технологій та спеціальності 121 «Інженерія програмного забезпечення».

Оцінка наукової новизни результатів дисертаційного дослідження.

До основних результатів, слід віднести *вперше* розроблену модель інтегрованого контуру довіри й цілісності у вебсистемі, що ґрунтується на кортежно-графовому поданні критичних подій і криптографічних принципах їх верифікації. Запропонована модель забезпечує формалізоване подання зв'язків між вебформами, SQL-операціями, рішеннями аналітичного модуля, політиками реагування та незмінним журналюванням, що створює єдине інформаційне середовище для контролю цілісності даних, аудитної перевірки та відтворюваності рішень.

Важливим науковим результатом є також *вперше* розроблений метод блокчейн-верифікованого журналювання критичних подій і контролю доступу у вебсистемах. Метод ґрунтується на моделі ІКДЦ, криптографічно зв'язаному ланцюгу подій, хешуванні, цифровому підписі та пороговому правилі прийняття рішень щодо доступу. Його застосування спрямоване на зменшення ризику прихованої модифікації інформації, підвищення доказовості журналів і посилення контролю цілісності даних під час аналізу інцидентів.

Окремої уваги заслуговує *вперше* розроблений метод графово-нейромережевого виявлення вебспау та підозрілої активності у вебсистемах. Його новизна полягає у використанні багатопредставленого графового опису подій із урахуванням технічних, змістовних, часово-поведінкових і контекстних ознак, а також зв'язків між подіями й результатами аналітичного оцінювання. Це дозволяє розрізняти легітимні, підозрілі та шкідливі звернення, підвищувати точність виявлення вебспау і зменшувати частку хибних спрацювань.

Завершальним науковим результатом є *вперше* розроблений метод інтегрованого забезпечення довіри й цілісності у вебсистемах, який поєднує модель ІКДЦ, блокчейн-верифіковане журналювання критичних подій і графово-нейромережеве виявлення вебспау та підозрілої активності. Наукова новизна цього методу полягає в узгодженні фіксації подій, аналітичного оцінювання, прийняття рішень, політик реагування та доказового журналювання в межах єдиного контуру.

Заявлена наукова новизна відповідає фактичному змісту дисертаційної роботи. Отримані результати є взаємопов'язаними, логічно впливають із поставлених завдань і формують цілісний науковий підхід до забезпечення довіри, цілісності, простежуваності та точності прийняття рішень у вебсистемах.

Практична цінність отриманих результатів.

Практичне значення дисертаційної роботи полягає у можливості використання запропонованої моделі ІКДЦ та розроблених методів для побудови або модернізації вебсистем із підвищеними вимогами до захищеності, контролю цілісності, простежуваності подій і аудитної перевірки.

Результати роботи можуть бути використані у вебзастосунках, корпоративних інформаційних системах, системах електронної комерції, платіжних сервісах, інформаційних порталах та інших програмних комплексах, де важливими є фіксація критичних подій, контроль SQL-операцій, виявлення підозрілої активності та зменшення навантаження на адміністраторів під час аналізу інцидентів.

Практична цінність роботи підтверджується реалізацією програмного прототипу, експериментальною перевіркою запропонованих рішень та впровадженням результатів у діяльність ТОВ «ШЛІФАРБ», ТОВ «АРМА МОТОРС КИЇВ», Інституту програмних систем НАН України, а також в освітній процес Державного університету інформаційно-комунікаційних технологій. Отримані результати мають значення для спеціальності 121 «Інженерія програмного забезпечення», оскільки спрямовані на розроблення архітектурних, алгоритмічних і програмних рішень для підвищення довіри, цілісності та надійності вебсистем.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана в межах науково-дослідної роботи кафедри Інженерії програмного забезпечення Державного університету інформаційно-комунікаційних технологій на тему «Забезпечення функціональної стійкості інформаційних систем підприємства в умовах впливу дестабілізуючих факторів із застосуванням нейронних мереж» (державний реєстраційний номер 0226U000249) та науково-дослідної роботи «Методи побудови функціонально стійких захищених інформаційних систем з централізованим управлінням» (державний реєстраційний номер 0125U002823).

Повнота викладу основних результатів дисертації в публікаціях.

Основні результати дисертаційної роботи достатньо повно оприлюднені у наукових публікаціях здобувача. За результатами дослідження опубліковано 19 наукових праць:

- 6 статей у наукових фахових виданнях України категорії Б;
- 4 публікації у виданнях, що індексуються у наукометричній базі Scopus;

- 9 публікацій у збірниках матеріалів міжнародних і всеукраїнських наукових конференцій.

Публікації відображають ключові положення дисертації, забезпечують апробацію отриманих результатів та підтверджують їх відповідність тематиці дослідження.

Отже, кількість і зміст публікацій свідчать про належний рівень оприлюднення основних наукових результатів дисертаційної роботи.

Загальна характеристика дослідження.

Дисертаційна робота Шахматова Івана Олександровича «Моделі та методи забезпечення довіри й цілісності у вебсистемах» є завершеним науковим дослідженням, виконаним у межах спеціальності 121 «Інженерія програмного забезпечення». Робота присвячена розв'язанню актуального науково-практичного завдання, що полягає у підвищенні рівня довіри, цілісності та захищеності архітектури вебсистем шляхом розроблення моделей і методів контролю критичних подій, перевірки цілісності даних, виявлення підозрілої активності та забезпечення доказового журналювання.

Мета дисертаційного дослідження сформульована коректно і відповідає заявленій темі роботи. Вона полягає у підвищенні рівня довіри, цілісності та захищеності архітектури вебсистем за рахунок обґрунтування та побудови моделей і методів, що забезпечують контроль цілісності даних, визначення критичних подій і адаптивне виявлення підозрілої активності у вебсередовищі на основі технологій блокчейну та машинного навчання.

Об'єктом дослідження визначено процеси забезпечення довіри і цілісності вебсистем, а предметом - моделі та методи забезпечення довіри, цілісності та надійності вебсистем на рівні архітектури. Визначені об'єкт і предмет дослідження є взаємопов'язаними, відповідають меті роботи та дозволяють розглядати проблему забезпечення довіри й цілісності саме з позицій інженерії програмного забезпечення. Для досягнення поставленої мети здобувачем сформульовано комплекс наукових завдань, пов'язаних з аналізом існуючих підходів до забезпечення безпеки вебсистем, формалізацією задачі довіри й цілісності, розробленням моделі інтегрованого контуру довіри й цілісності, побудовою методу блокчейн-верифікованого журналювання критичних подій, розробленням методу графово-нейромережевого виявлення вебспаму та підозрілої активності, а також експериментальною перевіркою запропонованих рішень.

Оцінка змісту дисертації та аналіз основних розділів.

У вступі дисертаційної роботи обґрунтовано актуальність теми, визначено мету, завдання, об'єкт і предмет дослідження, розкрито наукову новизну та практичне значення отриманих результатів. Також наведено відомості про апробацію результатів, публікації здобувача, структуру та обсяг

дисертації. Загалом вступ містить усі необхідні елементи та відповідає вимогам до кваліфікаційної наукової праці.

У *першому* розділі проведено аналіз сучасного стану забезпечення довіри й цілісності у вебсистемах. Здобувач розглянув наявні підходи до захисту вебсистем, журналювання критичних подій, застосування блокчейн-технологій, методів машинного навчання для виявлення атак, вебспаму та підозрілої активності. Важливим результатом розділу є встановлення обмежень традиційних механізмів захисту та обґрунтування потреби в інтегрованому підході.

У *другому* розділі розроблено модель інтегрованого контуру довіри й цілісності у вебсистемах та метод блокчейн-верифікованого журналювання критичних подій і контролю доступу. Запропонована модель дозволяє формалізувати зв'язки між критичними подіями, вебформами, SQL-операціями, рішеннями аналітичного модуля, політиками реагування та аудитними записами. Матеріал розділу логічно пов'язаний із поставленими завданнями дослідження.

У *третьому* розділі запропоновано метод графово-нейромережевого виявлення вебспаму та підозрілої активності у вебсистемах. Здобувач обґрунтував підхід до підготовки даних, формування ознак і побудови багатопредставленого графового опису подій. Розроблений метод спрямований на підвищення точності виявлення небажаних і підозрілих звернень та зменшення частки хибних спрацювань.

У *четвертому* розділі розроблено метод інтегрованого забезпечення довіри й цілісності у вебсистемах, який поєднує модель ІКДЦ, блокчейн-верифіковане журналювання та графово-нейромережеве виявлення підозрілої активності. У розділі наведено програмну реалізацію, експериментальну перевірку та аналіз отриманих результатів. Отримані показники підтверджують ефективність запропонованих рішень для задач контролю цілісності, виявлення підозрілої активності та підтримки аудитної перевірки.

Висновки до розділів і загальні висновки дисертації відповідають поставленим завданням, узагальнюють основні результати дослідження та підтверджують досягнення мети роботи. Загалом зміст дисертації є послідовним, логічно структурованим і відповідає заявленій темі.

Логіка побудови дослідження є послідовною: від аналізу сучасних проблем забезпечення довіри й цілісності у вебсистемах - до розроблення моделі ІКДЦ, окремих методів журналювання та виявлення підозрілої активності, а також їх інтеграції в єдиний підхід. Запропоновані методи відповідають поставленим завданням і спрямовані на розв'язання визначеної у роботі науково-практичної проблеми.

Достовірність результатів підтверджується експериментальною перевіркою запропонованих рішень, використанням кількісних метрик

оцінювання, зокрема Precision, Recall, F1-міри, частки хибних спрацювань та часових характеристик обробки подій. Наведені у роботі результати демонструють підвищення якості виявлення підозрілої активності та зменшення частки хибних спрацювань для подій типу SUBMIT і TX.

Зауваження до проведеного дисертаційного дослідження.

Загальна оцінка дисертаційної роботи є позитивною. Разом із тим, на окремі положення доцільно звернути увагу:

1. У теоретичній частині роботи доцільно було б ширше показати відмінність запропонованого інтегрованого контуру довіри й цілісності від наявних підходів до журналювання, моніторингу та аудиту подій у вебсистемах. Це дозволило б ще чіткіше окреслити місце запропонованої моделі ІКДЦ серед суміжних архітектурних рішень.

2. У частині формалізації окремі параметри, що використовуються для оцінювання ризику, прийняття рішень і вибору порогових значень, могли б бути пояснені детальніше з погляду їх практичного налаштування в різних типах вебсистем. Це особливо важливо для випадків, коли запропонований підхід переноситься з експериментального середовища у промислову експлуатацію.

3. В експериментальній частині основну увагу зосереджено на потоках подій типу SUBMIT і TX. Було б доцільно в подальших дослідженнях розширити перелік сценаріїв перевірки, зокрема для інших типів критичних подій вебсистеми, щоб додатково підтвердити універсальність запропонованого підходу.

4. Практичне впровадження результатів роботи підтверджує прикладну цінність дослідження, однак у роботі можна було б детальніше описати типові вимоги до інтеграції запропонованого програмного прототипу в уже наявні вебсистеми, зокрема щодо продуктивності, керування ключами, зберігання журналів і масштабування.

5. У тексті дисертації трапляються окремі термінологічні та стилістичні неточності, зокрема щодо вживання близьких за змістом понять «довіра», «цілісність», «простежуваність», «перевірюваність» та «аудитна доказовість». Їх додаткове уніфікування сприяло б ще більшій чіткості викладу.

Зазначені зауваження мають рекомендаційний характер, не знижують загальної наукової новизни, теоретичної та практичної значущості отриманих результатів і не впливають на позитивну оцінку дисертаційної роботи.

Оцінка змісту дисертації, відповідність встановленим вимогам щодо оформлення та теоретико-методологічна база дослідження.

Дисертаційна робота Шахматова І.О. характеризується логічною послідовністю викладу, обґрунтованістю постановки задач і коректним застосуванням методів. Для розв'язання поставлених у дисертаційному дослідженні завдань було використано низку взаємопов'язаних теоретичних і методичних підходів. Основу теоретичного підґрунтя становлять положення

теорії графів, які використано для подання взаємозв'язків між подіями, об'єктами та рішеннями у вебсистемі, а також положення теорії довіри до інформаційних систем, що забезпечують формалізацію моделі довіри й цілісності у вебзастосунках. Методологічною основою дослідження є поєднання криптографічних підходів, засобів блокчейн-технології та методів машинного навчання, що дає змогу одночасно забезпечити контроль цілісності критичних подій, незмінність журналювання та адаптивне виявлення підозрілої активності у вебсередовищі. Для забезпечення контролю цілісності в роботі застосовано криптографічні методи хешування та цифрового підпису, а також підходи блокчейн-технології та незмінного журналювання для фіксації, перевірки та аудиторної інтерпретації критичних подій. Для виявлення вебспаму та аномальної активності використано методи машинного навчання, зокрема графові нейронні мережі, що дозволяють враховувати багатопредставленнєвий опис подій, поведінкові ознаки та зв'язки між об'єктами взаємодії у вебсистемі. Для оцінювання якості запропонованих рішень використано методи математичної статистики та теорії ймовірностей, а для організації й інтерпретації результатів експериментальних досліджень — методи теорії планування експерименту.

Представлені результати узгоджені з метою та завданнями дослідження, а сформульовані висновки є аргументованими.

Дисертація має логічну структуру і складається зі вступу, чотирьох розділів, висновків і списку використаних джерел. Загальний обсяг роботи становить 187 сторінок, з яких 135 сторінок основного тексту. Робота містить 25 рисунків, 7 таблиць, а список використаних джерел включає 151 найменування. Зміст дисертаційної роботи відповідає заявленій темі, поставленій меті та спеціальності 121 «Інженерія програмного забезпечення». Структура роботи є послідовною, а отримані результати свідчать про завершеність проведеного дослідження.

Оформлення дисертації загалом відповідає чинним вимогам до кваліфікаційних наукових праць на здобуття ступеня доктора філософії: структура витримана, науковий стиль дотримано, термінологія застосована коректно, наведені джерела є релевантними предметній області.

Загальний висновок про дисертаційну роботу.

Дисертаційна робота Шахматова І.О. «Моделі та методи забезпечення довіри й цілісності у вебсистемах» є завершеною кваліфікаційною науковою працею, у якій розв'язано актуальне науково-практичне завдання підвищення довіри, цілісності та захищеності вебсистем. Робота відповідає діючим вимогам, що висуваються до дисертацій на здобуття наукового ступеня доктора філософії, передбачених «Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти,

наукової установи про присудження ступеня доктора філософії», затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

У роботі отримано нові науково обґрунтовані результати, що мають теоретичне і практичне значення для розвитку моделей, методів і програмних засобів забезпечення довіри й цілісності у вебсистемах. Запропоновані результати є самостійними, достатньо обґрунтованими, апробованими та підтвердженими практичним впровадженням.

За актуальністю, науковою новизною, практичним значенням, повнотою викладення, обсягом виконаних досліджень, обґрунтованістю висновків та рівнем апробації дисертаційна робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії за спеціальністю 121 «Інженерія програмного забезпечення», а її автор, Шахматов Іван Олександрович, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 121 «Інженерія програмного забезпечення» галузі знань 12 «Інформаційні технології».

Офіційний рецензент:

доцент кафедри технологій цифрового розвитку

Державного університету інформаційно-

комунікаційних технологій

кандидат технічних наук



Андрій АРОНОВ

Підпис



ЗАСВІДЧУЮ

Учений секретар

Державного університету

інформаційно-комунікаційних технологій

