

*Голові разової спеціалізованої вченої
ради Державного університету
інформаційно-комунікаційних
технологій
доктору технічних наук, професору
Віталію САВЧЕНКУ
вул. Солом'янська, 7, м. Київ, 03110*

ВІДГУК

офіційного опонента

*кандидата технічних наук, доцента, доцента кафедри комп'ютерних наук
Київського столичного університету імені Бориса Грінченка*

РЗАЄВОЇ Світлани Леонідівни

на дисертаційну роботу

«Моделі та методи забезпечення довіри й цілісності у вебсистемах»

ШАХМАТОВА Івана Олександровича,

*подану на здобуття наукового ступеня доктора філософії за спеціальністю
121 Інженерія програмного забезпечення, галузі знань 12 Інформаційні технології*

Актуальність теми дослідження.

Вебсистеми сьогодні стали базовою інфраструктурою для електронної комерції, корпоративних сервісів, онлайн-оплат, інформаційних платформ і державних цифрових послуг. У таких умовах особливого значення набувають питання довіри до результатів обробки даних, збереження їх цілісності, аналіз критичних подій та захищеності вебзастосунків від динамічних кіберзагроз. Порушення цілісності інформації, приховане редагування журналів, несанкціонований доступ, SQL-ін'єкції, DDoS-атаки, MITM-атаки та масовий вебспам можуть призводити не лише до технічних збоїв, а й до фінансових втрат, репутаційних ризиків і зниження надійності функціонування вебсервісів.

Наявні засоби моніторингу, журналювання та виявлення загроз не завжди забезпечують належний рівень доказовості подій, архітектурно узгоджений контроль незмінності критичних операцій і своєчасне реагування на підозрілу активність у вебсередовищі. Тому актуальним є розробка таких моделей і методів, які поєднують механізми криптографічної верифікації, незмінного журналювання, контролю доступу та інтелектуального аналізу вебтрафіку. Саме така інтеграція дає змогу підвищити захищеність вебсистем, в тім числі забезпечити контроль цілісності даних, зменшити ризик прихованої модифікації інформації та покращити якість виявлення вебспама й підозрілої активності.

Дисертаційна робота Шахматова Івана Олександровича логічно вписується у сучасний науковий дискурс, пропонуючи ефективні рішення проблем забезпечення довіри й цілісності у вебсистемах, тому є актуальною і практично значущою для розвитку та впровадження захищених вебсистем.

Оцінка наукового рівня дисертації, представлених теоретичних та експериментальних результатів проведених здобувачем досліджень, їх наукової обґрунтованості, рівня виконання поставленого наукового завдання

Загальна характеристика дослідження.

У вступі дисертаційної роботи визначено вихідні положення дослідження, обґрунтовано актуальність теми в умовах зростання ролі вебсистем у сфері електронної комерції, корпоративних сервісів, онлайн-оплат і цифрових платформ. Автором сформульовано мету, завдання, об'єкт і предмет дослідження, визначено методологічну основу роботи та окреслено її зв'язок із науково-дослідними темами. Вступ формує логічне підґрунтя для подальшого розробки моделей і методів забезпечення довіри, цілісності та захищеності вебсистем.

Перший розділ дисертаційної роботи присвячено аналізу сучасного стану та проблематики забезпечення довіри й цілісності у вебсистемах. У розділі розглянуто основні загрози для вебзастосунків, зокрема порушення цілісності даних, несанкціонований доступ, приховану модифікацію журналів, SQL-ін'єкції, DDoS-атаки, вебспам та інші прояви підозрілої активності. Автором проаналізовано традиційні механізми захисту, журналювання та аудиту, а також підходи на основі блокчейну для фіксації критичних подій і перевірки цілісності записів. Окрему увагу приділено методам машинного навчання для виявлення атак, аномалій і вебспаму. Проведений аналіз дозволив обґрунтувати необхідність інтегрованого підходу, який поєднує криптографічну фіксацію подій, контроль цілісності, аудит змін і інтелектуальне виявлення підозрілої активності.

Другий розділ дисертаційної роботи присвячено розробці моделі інтегрованого контуру довіри й цілісності та методу блокчейн-верифікованого журналювання критичних подій і контролю доступу у вебсистемах. У цьому розділі автор формалізує подання критичних подій, їх контексту, результатів оцінювання, рішень системи безпеки та аудитних записів у межах єдиного контуру. Запропонована модель ІКДЦ ґрунтується на кортежно-графовому поданні подій і криптографічних принципах їх верифікації, що дозволяє забезпечити контроль цілісності даних, фіксацію критичних подій та перевірку прийнятих рішень. Також розроблено метод блокчейн-верифікованого журналювання, який передбачає хешування, цифровий підпис і порогове правило прийняття рішень щодо доступу. Метод забезпечує фіксацію

критичних подій і рішень у незмінному журналі, зменшує ризик прихованої зміни інформації та підвищує доказовість аудиту у вебсистемі.

Третій розділ дисертаційної роботи присвячено методу графово-нейромережевого виявлення вебспаму та підозрілої активності у вебсистемах. Автором сформовано підхід до підготовки даних, їх очищення, кодування, нормалізації та масштабування, а також визначено ризикові компоненти, що враховують фінансові, географічні, часові та поведінкові характеристики подій. У розділі запропоновано багатопредставлений графовий опис подій, у якому вебзвернення розглядаються не ізольовано, а як елементи пов'язаного потоку дій користувачів, технічних параметрів і контекстних ознак. Такий підхід дозволяє враховувати не лише зміст окремого повідомлення, а й структурні та поведінкові закономірності між групами подій. Розділ демонструє доцільність використання графових моделей для підвищення точності виявлення вебспаму, зменшення кількості хибних спрацювань і адаптації до зміни шаблонів загроз.

Четвертий розділ дисертаційної роботи присвячено методу інтегрованого забезпечення довіри й цілісності у вебсистемах, його програмній реалізації та експериментальній перевірці. У розділі обґрунтовано поєднання моделі ІКДЦ, методу блокчейн-верифікованого журналювання критичних подій і методу графово-нейромережевого виявлення вебспаму та підозрілої активності в єдиний контур безпекової обробки. Автором описано послідовність перетворення критичної події у ризикову оцінку, рішення, дію реагування та доказовий запис. Створений програмний прототип забезпечує канонізацію подій, хешування, цифровий підпис, графове оцінювання, класифікацію, вибір політики реагування та незмінне журналювання. Експериментальна перевірка підтвердила ефективність запропонованого підходу, оскільки для подій SUBMIT і TX зафіксовано зростання F1-міри, зменшення частки хибних спрацювань і прийнятний рівень накладних витрат, що підтверджує практичну придатність методу.

У *висновках* наведено основні результати дисертаційного дослідження, розкрито їх наукову новизну, практичну цінність і достовірність. Автором показано, що поставлену мету досягнуто, а наукові завдання виконано повною мірою. Окремо підкреслено ефективність запропонованих моделей і методів за результатами експериментальної перевірки та практичного впровадження.

У додатках наявні копії актів впровадження та псевдокод розроблених алгоритмів та моделей.

Наукова новизна особисто отриманих здобувачем результатів полягає в наступному:

вперше розроблено модель інтегрованого контуру довіри й цілісності у вебсистемі, яка за рахунок коротко-графового подання критичних подій, використання криптографічних принципів їх верифікації, незмінного журналювання та формалізованого подання зв'язків між

вебформами, SQL-операціями, рішеннями аналітичного модуля і політиками реагування забезпечує єдине інформаційне середовище для контролю цілісності даних, простежуваності подій, аудиторної перевірки та відтворюваності рішень;

вперше розроблено метод блокчейн-верифікованого журналювання критичних подій і контролю доступу у вебсистемах, що ґрунтується на розробленій моделі інтегрованого контуру довіри й цілісності та теорії криптографічно зв'язаного ланцюга подій із використанням хешування, цифрового підпису й порогового правила прийняття рішення щодо доступу, що дозволяє зменшити ризик прихованої модифікації інформації, підвищити доказовість журналів і посилити контроль цілісності даних під час розслідування інцидентів;

вперше розроблено метод графово-нейромережевого виявлення вебспаму та підозрілої активності у вебсистемах, що ґрунтується на моделі інтегрованого контуру довіри й цілісності та багатопредставленому графовому описі подій через систему технічних, змістових, часово-поведінкових і контекстних ознак з урахуванням зв'язків між подіями та результатами аналітичного оцінювання, що забезпечує розрізнення легітимних, підозрілих і шкідливих звернень, підвищення точності виявлення вебспаму та зменшення частки хибних спрацювань;

вперше розроблено метод інтегрованого забезпечення довіри й цілісності у вебсистемах, що ґрунтується на моделі інтегрованого контуру довіри й цілісності, методі блокчейн-верифікованого журналювання критичних подій і контролю доступу, методі графово-нейромережевого виявлення вебспаму та підозрілої активності, а також на теорії композиції функціональних відображень критичних подій у клас рішень, що забезпечує цілісність системи, простежуваність подій та підвищення точності прийняття рішень.

Таким чином, поставлене в дисертаційному дослідженні наукове завдання виконане в повному обсязі.

Достовірність наукових положень.

Достовірність наукових положень дисертації підтверджується цілісною теоретико-методологічною базою дослідження, формальною побудовою запропонованої моделі інтегрованого контуру довіри й цілісності, методів блокчейн-верифікованого журналювання, контролю доступу та графово-нейромережевого виявлення підозрілої активності. Важливими елементами, що забезпечують наукову обґрунтованість, є використання положень теорії графів, теорії довіри до інформаційних систем, криптографічних методів хешування й цифрового підпису, підходів блокчейн-технологій, методів машинного навчання, зокрема графових нейронних мереж, а також методів математичної статистики, теорії ймовірностей і планування експерименту. Достовірність одержаних результатів також підтверджується узгодженістю теоретичних положень із програмною реалізацією, експериментальною перевіркою та практичним впровадженням результатів дослідження.

Наукове значення дисертаційної роботи полягає у розробці моделей і методів забезпечення довіри, цілісності та захищеності вебсистем шляхом поєднання незмінного журналювання критичних подій, криптографічної верифікації, графового подання подій і методів машинного навчання для адаптивного виявлення вебспаму, підозрілої активності та аномалій вебтрафіку. Запропонований підхід формує наукову основу для побудови архітектур вебсистем, у яких результати обробки критичних подій мають належне обґрунтування, підтверджуються даними журналювання та можуть бути використані для подальшого аудиту.

Практичне значення дисертаційної роботи полягає у створенні та впровадженні моделей, методів і програмних засобів для забезпечення довіри, цілісності та захищеності вебсистем, що функціонують в умовах обробки критичних подій, транзакційних дій, вебзвернень і підозрілої активності. Розроблені модель інтегрованого контуру довіри й цілісності, метод блокчейн-верифікованого журналювання критичних подій і контролю доступу, метод графово-нейромережевого виявлення вебспаму та підозрілої активності, а також інтегрований метод, що поєднує зазначені підходи в єдиний контур безпекової обробки, забезпечують можливість контролю цілісності даних, підвищення доказовості журналів, простежуваності рішень, виявлення підозрілої активності та зменшення ризику прихованої модифікації інформації.

Реалізований у межах дослідження програмний прототип може бути інтегрований у наявні вебсистеми як додатковий контур безпекової обробки без повної перебудови їхньої архітектури. Запропоноване рішення забезпечує канонізацію критичних подій, хешування, цифровий підпис, графове оцінювання ризику, класифікацію подій, вибір політики реагування та незмінне журналювання результатів. Такий підхід дозволяє використовувати розроблені засоби у вебзастосунках електронної комерції, корпоративних інформаційних системах, платіжних контурах та інших програмних середовищах, де важливими є аудит, контроль цілісності, надійність і перевірюваність прийнятих рішень.

Ефективність практичного застосування підтверджується результатами експериментальної перевірки та впровадження. Для подій типу SUBMIT значення F1-міри зросло з 0,78 у базовій конфігурації правил до 0,92 для повного інтегрованого контуру ІКДЦ, а частка хибних спрацювань зменшилася з 2,6% до 0,9%. Для подій типу TX значення F1-міри зросло з 0,74 до 0,90, а частка хибних спрацювань зменшилася з 1,9% до 0,8%. Практичні результати також підтверджені впровадженням у ТОВ «ШЛІФАРБ», ТОВ «АРМА МОТОРС КИЇВ», Інституті програмних систем НАН України та використанням окремих результатів в освітньому процесі Державного університету інформаційно-комунікаційних технологій.

Мова та стиль викладення дисертації дозволяють зрозуміти суть розроблених наукових положень, запропонованих моделей і методів, а також отриманих практичних результатів. Дисертація відповідає вимогам, які висуваються до її оформлення.

Оцінка рівня наукових публікацій здобувача та підтвердження повноти викладу в них основних результатів дисертації.

Основні результати за темою дисертаційного дослідження опубліковані у 19 наукових працях, серед яких 4 публікації індексуються у наукометричній базі Scopus, 6 статей надруковано у фахових наукових виданнях України категорії Б, а також 9 публікацій представлено у збірниках матеріалів і тез міжнародних та всеукраїнських науково-технічних і науково-практичних конференцій. Апробація результатів дослідження здійснювалася на конференціях різного рівня в період з 2023 по 2025 роки.

Недоліки та зауваження.

1. У дисертаційній роботі доцільно було б надати більш розгорнуте пояснення щодо вибору конкретних механізмів блокчейн-верифікованого журналювання критичних подій. Зокрема, бажано детальніше обґрунтувати вибір способу криптографічного зв'язування записів, використання хешування, цифрового підпису та порогового правила прийняття рішень щодо доступу в порівнянні з альтернативними підходами до забезпечення незмінності журналів. Додаткове пояснення дозволило б чіткіше показати переваги запропонованого методу саме для вебсистем із високими вимогами до доказовості, аудиту та контролю цілісності даних.

2. У розділі, присвяченому графово-нейромережевому виявленню вебспаму та підозрілої активності, бажано було б конкретизувати особливості вибору графового подання подій і параметрів моделі. Зокрема, доцільним є ширше пояснення того, як саме визначаються ваги окремих ознак, порогові значення ризику та співвідношення між технічними, змістовими, часово-поведінковими й контекстними характеристиками подій. Це дозволило б глибше розкрити механізм адаптації методу до зміни шаблонів загроз і краще продемонструвати переваги запропонованого підходу порівняно з традиційними правилами або класичними методами машинного навчання.

3. У частині практичної реалізації та експериментальної перевірки доцільно було б більш детально описати умови інтеграції програмного прототипу в реальні вебсистеми. Зокрема, варто конкретизувати, які саме компоненти інтегрованого контуру довіри й цілісності були впроваджені в тестових або виробничих середовищах, які вимоги висуваються до наявної архітектури вебзастосунку, а також які обмеження можуть виникати під час масштабування рішення. Додаткове подання таких аспектів дозволило б повніше оцінити практичну універсальність запропонованого підходу та його придатність до використання в різних типах вебсистем.

Вказані недоліки не знижують наукової цінності та практичного значення одержаних наукових результатів і не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

На основі детального вивчення дисертації та праць здобувача, опублікованих за темою дисертації, встановлено, що дисертація Шахматова І.О. є завершеною кваліфікаційною науковою працею, що відповідає вимогам освітньо-наукової програми за спеціальністю 121 Інженерія програмного забезпечення, містить нові науково обґрунтовані результати проведених здобувачем досліджень, які вирішують конкретне наукове завдання, пов'язане з підвищенням рівня довіри, цілісності та захищеності вебсистем шляхом розробки моделі інтегрованого контуру довіри й цілісності, методу блокчейн-верифікованого журналювання критичних подій і контролю доступу, методу графово-нейромережевого виявлення вебспау та методу інтегрованого забезпечення довіри й цілісності у вебсистемах. Дане наукове завдання має значення для створення та впровадження ефективних програмних засобів контролю цілісності даних, простежуваності критичних подій, доказового аудиту та адаптивного виявлення підозрілої активності у вебсистемах.

Дисертаційна робота Шахматова Івана Олександровича 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 (зі змінами від 03 травня 2024 р. № 507), та «Порядком підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах)», затвердженим постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (зі змінами від 19 травня 2023 р. № 502). Автор дисертації ШАХМАТОВ Іван Олександрович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 121 Інженерія програмного забезпечення, галузі знань 12 Інформаційні технології.

Офіційний опонент:

кандидат технічних наук, доцент,
доцент кафедри комп'ютерних наук
Факультету інформаційних технологій та математики
Київського столичного університету
імені Бориса Грінченка

С. Рзаєва

Світлана РЗАЄВА

Підпис Світлани Рзаєвої завіряю
Декан Факультету інформаційних технологій
та математики



Литвин

Оксана ЛИТВИН