

*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

доктора технічних наук, професора, декана факультету інформатики та  
обчислювальної техніки Національного технічного університету України  
«Київського політехнічного інституту імені Ігоря Сікорського»

**Корнаги Ярослава Ігоровича**

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, все більше виконують роль ключових програмних платформ для обробки, передавання та зберігання даних у комерційних, корпоративних, фінансових, інформаційних і державних цифрових сервісах. Зі зростанням обсягів даних, кількості користувацьких взаємодій і складності архітектури вебзастосунків підвищуються вимоги не лише до їх функціональності, а й до довіри до результатів обробки інформації, цілісності критичних подій, контрольованості змін і можливості подальшої аудиторної перевірки. Особливої актуальності набувають задачі виявлення несанкціонованого доступу, прихованої модифікації даних, маніпуляцій із журналами подій, підозрілих SQL-операцій, атак на вебформи, вебспау та інших дій, що можуть порушувати стабільність і керованість вебсистем. Традиційні механізми захисту, журналювання та моніторингу здебільшого орієнтовані на фіксацію окремих подій або реагування на вже відомі шаблони



загроз. Водночас у багатокомпонентних вебархітектурах цього недостатньо для забезпечення повної доказовості виконаних дій, підтвердження незмінності критичних записів і відтворення логіки прийнятих рішень. Недостатня узгодженість між механізмами контролю доступу, аналізом поведінки користувачів, фіксацією SQL-операцій, обробкою вебформ і аудитом подій ускладнює своєчасне виявлення інцидентів та знижує рівень довіри до даних, що зберігаються і обробляються у вебсистемі.

У зв'язку з цим актуальним є розробка моделей і методів, які забезпечують не ізольований, а інтегрований підхід до контролю цілісності, фіксації критичних подій, перевірки їх незмінності та інтелектуального виявлення підозрілої активності. Поєднання криптографічного зв'язування записів, блокчейн-верифікованого журналювання, формалізованого подання подій, контролю доступу та графово-нейромережевого аналізу дає змогу підвищити обґрунтованість рішень системи безпеки, зменшити ризик прихованого втручання в дані та забезпечити можливість подальшої перевірки дій у межах аудиту.

Дисертаційна робота Шахматова Івана Олександровича є своєчасною та актуальною, оскільки спрямована на розв'язання важливої науково-прикладної проблеми забезпечення довіри й цілісності у вебсистемах. Запропонований у роботі підхід орієнтований на підвищення захищеності вебзастосунків, формування доказового середовища для аналізу критичних подій і покращення якості виявлення вебспаму та підозрілої активності, що має вагоме значення для розвитку сучасних захищених інформаційних систем.

**Загальна характеристика дослідження.** У вступі дисертаційної роботи окреслено загальну логіку дослідження, обґрунтовано вибір теми та показано її значення для сучасних вебсистем, що функціонують у середовищі постійних кіберзагроз і потребують надійного контролю даних. Автором визначено мету, завдання, об'єкт, предмет і методи дослідження, а також наведено зв'язок роботи з науково-дослідними темами. Вступ чітко задає науковий напрям роботи та підводить до необхідності розробки моделей і методів забезпечення довіри й цілісності у вебсистемах.



*Перший* розділ дисертаційної роботи присвячено дослідженню теоретичних і практичних передумов забезпечення довіри, цілісності та захищеності вебсистем. У розділі проаналізовано характерні загрози для вебзастосунків, серед яких несанкціонований доступ, порушення цілісності інформації, зміна журналів подій, атаки на вебформи, SQL-ін'єкції, DDoS-атаки, вебспам і підозріла активність користувачів. Автором розглянуто можливості традиційних засобів захисту, систем журналювання, аудиту та моніторингу, а також визначено їх обмеження в контексті доказовості й незмінності критичних подій. Окремо досліджено блокчейн-підходи до фіксації подій і методи машинного навчання для виявлення аномалій та атак. Проведений аналіз дозволив обґрунтувати потребу в комплексному підході, який поєднує криптографічну перевірку, аудит, контроль цілісності та інтелектуальний аналіз вебактивності.

*Другий* розділ дисертаційної роботи присвячено формуванню модельно-методичної основи забезпечення довіри й цілісності у вебсистемах. У цьому розділі автором розроблено модель інтегрованого контуру довіри й цілісності, у межах якої критичні події, їх контекст, результати аналізу, рішення системи та аудитні записи подаються як взаємопов'язані елементи єдиного формального середовища. Модель ІКДЦ базується на кортежно-графовому описі подій і криптографічній верифікації, що дає змогу забезпечити перевірку цілісності даних і відтворюваність прийнятих рішень. Також у розділі розроблено метод блокчейн-верифікованого журналювання критичних подій і контролю доступу, який використовує хешування, цифровий підпис і порогове правило прийняття рішення.

*Третій* розділ дисертаційної роботи присвячено розробленню методу графово-нейромережевого виявлення вебспаму та підозрілої активності. Автором визначено порядок підготовки даних для аналізу, що включає очищення, кодування, нормалізацію, масштабування та формування ознак подій. Значну увагу приділено врахуванню технічних, змістовних, часових, поведінкових, фінансових і контекстних характеристик. У розділі запропоновано багатопредставлений графовий опис подій вебсистеми, за якого окремі звернення



розглядаються як частина пов'язаного потоку взаємодій. Такий підхід дозволяє аналізувати не лише зміст повідомлення, а й зв'язки між користувачами, подіями, технічними параметрами та результатами оцінювання. Розділ підтверджує доцільність застосування графових нейромереж для підвищення якості розпізнавання вебспаму, зменшення хибних спрацювань і адаптації до змінних сценаріїв загроз.

*Четвертий* розділ дисертаційної роботи присвячено інтеграції запропонованих рішень у інтегрований метод забезпечення довіри й цілісності у вебсистемах, а також його програмній реалізації та експериментальному оцінюванню. У розділі показано, як модель ІКДЦ, метод блокчейн-верифікованого журналювання, контролю доступу та метод графово-нейромережевого виявлення підозрілої активності об'єднуються в єдиний контур обробки критичних подій. Автором описано послідовність проходження події від її фіксації та формування ознак до оцінювання ризику, класифікації, вибору політики реагування і створення доказового запису. Експериментальні результати для потоків SUBMIT і TX засвідчили підвищення F1-міри, зниження частки хибних спрацювань і прийнятний рівень накладних витрат, що підтверджує ефективність і практичну придатність запропонованого методу.

У *висновках* дисертаційної роботи узагальнено основні наукові та практичні результати, наведено підтвердження досягнення поставленої мети й виконання визначених завдань. Автором розкрито наукову новизну одержаних результатів, їх достовірність, практичне значення та можливість використання у вебсистемах із підвищеними вимогами до захищеності, аудиту й контролю цілісності.

У додатках наявні копії актів впровадження та псевдокод програмних модулів розроблених методів та моделей.

**Наукова новизна** особисто отриманих здобувачем результатів полягає в наступному:

- *вперше* розроблено модель інтегрованого контуру довіри й цілісності, у вебсистемі, що ґрунтується на кортежно-графовому поданні критичних подій і криптографічних принципах їх верифікації та за рахунок



поєднання незмінного журналювання критичних подій, формалізованого подання зв'язків між вебформами, SQL-операціями, рішеннями аналітичного модуля та політиками реагування забезпечує єдине інформаційне середовище для контролю цілісності даних, простежуваності подій, аудитної перевірки та відтворюваності рішень у вебсистемі;

- *вперше* розроблено метод блокчейн-верифікованого журналювання критичних подій і контролю доступу у вебсистемах, що ґрунтується на розробленій моделі ІКДЦ та теорії криптографічно зв'язаного ланцюга подій із хешуванням, цифровим підписом і пороговим правилом прийняття рішення щодо доступу, який дозволяє зменшити ризик прихованої модифікації інформації, підвищити доказовість журналів і контроль цілісності даних під час розслідування інцидентів;

- *вперше* розроблено метод графово-нейромережевого виявлення вебспау та підозрілої активності у вебсистемах, що ґрунтується на моделі ІКДЦ та багатопредставленому графовому описі подій, поданих через систему ознак технічного, змістовного, часово-поведінкового, контекстного характеру з урахуванням зв'язків між подіями й результатами аналітичного оцінювання, що забезпечує розрізнення легітимних, підозрілих і шкідливих звернень, підвищує точність виявлення вебспау та зменшує частку хибних спрацювань;

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

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

**Достовірність наукових положень.** Достовірність наукових положень дисертаційної роботи забезпечується обґрунтованим вибором теоретичних засад, послідовною формалізацією запропонованих моделей і методів, а також їх



перевіркою на рівні програмної реалізації та експериментальних результатів. Наукові висновки роботи спираються на використання апарату теорії графів, методів криптографічного захисту інформації, хешування, цифрового підпису, блокчейн-верифікації, контролю доступу, машинного навчання та графових нейронних мереж. Додаткову обґрунтованість результатам надає застосування методів математичної статистики, аналізу даних, оцінювання якості класифікації та експериментальної перевірки. Достовірність отриманих результатів підтверджується узгодженістю теоретичних положень із розробленим програмним прототипом, результатами тестування на потоках подій типу SUBMIT і TX, а також наявністю практичного впровадження результатів дисертаційного 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 розробці та апробації моделей, методів і програмного прототипу, призначених для підвищення довіри, цілісності та захищеності вебсистем, що обробляють критичні події, транзакційні дії, вебзвернення та прояви підозрілої активності. Розроблена 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 їх поєднання забезпечують практичну можливість фіксації критичних подій, контролю незмінності даних, виявлення загроз, зменшення хибних спрацювань і формування доказової основи для подальшого аудиту. Реалізований у межах дослідження програмний прототип може бути



використаний як додатковий контур безпекової обробки в наявних вебсистемах без необхідності повної перебудови їх архітектури. Запропоноване рішення забезпечує канонізацію подій, хешування, цифровий підпис, формування ознак, графове оцінювання ризику, класифікацію подій, вибір політики реагування та запис результатів у незмінний журнал. Це дає змогу застосовувати розроблені засоби у вебзастосунках електронної комерції, корпоративних інформаційних системах, платіжних контурах та інших програмних середовищах, де важливими є перевірка рішень, контроль цілісності, аудит критичних дій і зменшення ризику прихованої модифікації інформації.

Практична ефективність запропонованого підходу підтверджується результатами експериментальної перевірки. Для подій типу SUBMIT значення F1-міри зросло з 0,78 у базовій правилівій конфігурації до 0,92 для повного 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%. Підвищення індексу довіри до рішення, показує, що для подій SUBMIT - з 0,760 до 0,912, що відповідає приросту на 20,0%, а для подій TX - з 0,726 до 0,893, що відповідає приросту на 23,0%. Це свідчить, що практичний ефект полягає не лише у підвищенні якості виявлення загроз, а й у зростанні обґрунтованості рішень системи та зменшенні ризику помилкової реакції адміністратора на легітимні події.

Результати практичного використання підтверджені актами впровадження у Інституті програмних систем НАН України, ТОВ «ШЛІФАРБ», ТОВ «АРМА МОТОРС КИЇВ», освітньому процесі Державного університету інформаційно-комунікаційних технологій під час викладання дисципліни «Безпека програм та даних».

Стиль викладення дисертації є зрозумілими, послідовними та достатніми для розкриття суті запропонованих наукових положень, моделей, методів і 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 опубліковано у фахових наукових виданнях України категорії Б, а також здійснено апробацію результатів дослідження на міжнародних та всеукраїнських науково-технічних і науково-практичних конференціях.

### **Недоліки та зауваження.**

1. У дисертаційній роботі доцільно було б детальніше обґрунтувати введення похідного індексу довіри до рішення, який використовується для узагальнення впливу F1-міри та частки хибних спрацювань на рівень довіри до результату. Зокрема, бажано ширше пояснити межі застосування цього показника, його інтерпретацію для різних типів подій та можливість використання в інших конфігураціях вебсистем. Додаткове обґрунтування дозволило б чіткіше показати, що підвищення довіри оцінюється не лише як наслідок покращення метрик класифікації, а як комплексний результат зменшення помилкових реакцій і підвищення обґрунтованості рішень системи.

2. У частині експериментальної перевірки доцільно було б розширити пояснення щодо вибору порогових значень реагування  $t_1$  і  $t_2$ , які використовуються для прийняття рішень у контурі безпекової обробки. Зокрема, варто було б детальніше показати, як зміна цих порогів може впливати на співвідношення між дозволеними подіями, контрольованою перевіркою та блокуванням. Таке уточнення посилило б практичну інтерпретацію отриманих результатів і дало б змогу краще оцінити гнучкість запропонованого підходу для вебсистем із різними вимогами до ризику, швидкодії та допустимого рівня хибних спрацювань.

3. У розділі, присвяченому програмній реалізації інтегрованого контуру ІКДЦ, бажано було б більш наочно подати відповідність між теоретичними складовими методу та конкретними програмними модулями прототипу. Зокрема, доцільним було б додати узагальнену схему або таблицю, у якій показано, які компоненти відповідають за канонізацію подій, хешування, цифровий підпис, графове оцінювання ризику, класифікацію, вибір політики реагування та незмінне журналювання. Це зробило б опис програмної реалізації більш зручним



для сприйняття та полегшило б розуміння можливостей подальшої інтеграції запропонованого рішення в реальні вебсистеми.

Вказані недоліки мають рекомендаційний характер, не знижують наукової цінності та практичного значення отриманих результатів і не впливають на загальну позитивну оцінку дисертаційної роботи.

### **Висновок.**

На підставі аналізу дисертаційної роботи та наукових публікацій здобувача, виконаних за темою дослідження, можна зробити висновок, що дисертація Шахматова І.О. є завершеною кваліфікаційною науковою працею, яка відповідає освітньо-науковій програмі за спеціальністю 121 Інженерія програмного забезпечення. У роботі отримано нові науково обґрунтовані результати, що спрямовані на розв'язання актуального наукового завдання підвищення довіри, цілісності та захищеності вебсистем. Зокрема, здобувачем розроблено 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 метод інтегрованого забезпечення довіри й цілісності у вебсистемах. Отримані результати мають наукове та практичне значення для побудови програмних засобів контролю цілісності даних, доказового журналювання, аудитної перевірки, простежуваності критичних подій і адаптивного реагування на підозрілу активність у вебсередовищі.

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), 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 опонент:**

декан факультету інформатики та обчислювальної техніки

Національного технічного університету України

«Київського політехнічного інституту

імені Ігоря Сікорського»

доктор технічних наук, професор

