ЗАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно-комунікаційних технологій

_____ Олександр КОРЧЕНКО
"08" травня 2026 року
(МП)

ВИТЯГ
з протоколу №10 міжкафедрального наукового семінару кафедри інженерії програмного забезпечення Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій від «04» травня 2026 року

ПРИСУТНІ:
15 осіб із 18 науково-педагогічних працівників кафедри:
завідувач кафедри доктор технічних наук, професор Замрій Ірина Вікторівна, професор кафедри, кандидат фізико-математичних наук, доцент Садовенко Володимир Сергійович, доцент кафедри, кандидат технічних наук Задонцев Юрій Вікторович, доцент кафедри, кандидат технічних наук Довженко Тимур Павлович, доцент кафедри, кандидат технічних наук, доцент Золотухіна Оксана Анатоліївна, доцент кафедри, кандидат технічних наук, доцент Яскевич Владислав Олександрович, доцент кафедри, доктор філософії (PhD) Залива Віталій Вікторович, доцент кафедри, доктор філософії (PhD) Худік Богдан Олександрович, старший викладач кафедри, доктор філософії (PhD) Коваленко Данило Сергійович, старший викладач кафедри Гаманюк Ігор Михайлович, викладач кафедри Шахматов Іван Олександрович, викладач кафедри Цапро Ігор Вікторович, асистент кафедри Колодюк Андрій Васильович, асистент кафедри Ярошевський Олександр Вікторович, асистент кафедри Аброскін Юрій Юрійович.

На науковому семінарі присутні аспіранти Шахматов Іван Олександрович, Колодюк Андрій Васильович, Цапро Ігор Вікторович, Корецький Олександр Валерійович, Миколаєнко Владислав Олександрович.

На науковий семінар запрошені директор навчально-наукового інституту інформаційних технологій, доктор технічних наук, професор Нестеренко Катерина Сергіївна, доцент кафедри технологій цифрового розвитку, кандидат технічних наук, доцент Сватко Віталій Володимирович, доцент кафедри технологій цифрового розвитку, кандидат технічних наук, Аронов Андрій Олексійович, доцент кафедри технологій цифрового розвитку, кандидат технічних наук, Ананченко Олексій Євгенович, доцент кафедри технологій цифрового розвитку доктор філософії (PhD) Герцюк Микола Модестович, завідувач кафедри інформаційних систем та технологій, доктор технічних

наук, професор Сторчак Каміла Павлівна, доцент кафедри інформаційних систем та технологій Полоневич Ольга Володимирівна, завідувач кафедри комп'ютерної інженерії, кандидат технічних наук, доцент Лащевська Наталія Олександрівна, доцент кафедри комп'ютерної інженерії, кандидат технічних наук, старший науковий співробітник Торошанко Ярослав Іванович, професор кафедри штучного інтелекту, доктор технічних наук, професор Чичкарьов Євген Анатолійович, доцент кафедри комп'ютерних наук, кандидат технічних наук, доцент Гніденко Микола Петрович, професор кафедри управління кібербезпекою та захистом інформації доктор технічних наук, професор Савченко Віталій Анатолійович, завідувач кафедри технічних систем кіберзахисту, доктор технічних наук, професор Туровський Олександр Леонідович, професор кафедри технічних систем кіберзахисту, кандидат технічних наук, доцент Пепа Юрій Володимирович.

Всього присутніх – 31 особа, серед присутніх 5 докторів технічних наук, 6 кандидатів технічних наук за профілем представленої дисертації.
Головуючий на науковому семінарі – директор Навчально-наукового інституту інформаційних технологій, доктор технічних наук, професор Нестеренко Катерина Сергіївна.

ПОРЯДОК ДЕННИЙ:
Обговорення публічної презентації наукових результатів дисертаційної роботи здобувача третього рівня вищої освіти кафедри інженерії програмного забезпечення Державного університету інформаційно-комунікаційних технологій Шахматова Івана Олександровича на тему: «Моделі та методи забезпечення довіри й цілісності у вебсистемах», поданої на здобуття ступеня доктора філософії за спеціальністю 121 – Інженерія програмного забезпечення, галузі знань 12 – Інформаційні технології.
Тему дисертації затверджено «27» листопада 2023 року на засіданні Вченої Ради Державного університету інформаційно-комунікаційних технологій, **протокол №5.** Уточнення теми дисертаційної роботи затверджено «18» листопада 2025 року на засіданні Вченої Ради Державного університету інформаційно-комунікаційних технологій, протокол №13.
Робота виконана на кафедрі інженерії програмного забезпечення Державного університету інформаційно-комунікаційних технологій.
Науковий керівник завідувач кафедри інженерії програмного забезпечення доктор технічних наук, професор, Замрій Ірина Вікторівна.

СЛУХАЛИ:
1. Доповідь здобувача Шахматова Івана Олександровича щодо основних наукових результатів дисертаційного дослідження на тему: «Моделі та методи забезпечення довіри й цілісності у вебсистемах», подану на здобуття ступеня доктора філософії за спеціальністю 121 – Інженерія програмного забезпечення.
2. Запитання до здобувача.

По доповіді було задано 11 запитань, на які здобувач надав вичерпні та аргументовані відповіді.

Питання задавали:

завідувач кафедри інформаційних систем та технологій, доктор технічних наук, професор Сторчак Каміла Павлівна, завідувач кафедри інженерії програмного забезпечення, доктор технічних наук, професор Замрій Ірина Вікторівна, професор кафедри інженерії програмного забезпечення, кандидат фізико-математичних наук, доцент Садовенко Володимир Сергійович, доцент кафедри інженерії програмного забезпечення, кандидат технічних наук Задонцев Юрій Вікторович, доцент кафедри інженерії програмного забезпечення, кандидат технічних наук Довженко Тимур Павлович, доцент кафедри інформаційних систем та технологій Полоневич Ольга Володимирівна, завідувач кафедри комп'ютерної інженерії, кандидат технічних наук, доцент Лащевська Наталія Олександрівна, доцент кафедри технологій цифрового розвитку, кандидат технічних наук, Аронов Андрій Олексійович, професор кафедри штучного інтелекту, доктор технічних наук, професор Чичкарьов Євген Анатолійович, професор кафедри управління кібербезпекою та захистом інформації доктор технічних наук, професор Савченко Віталій Анатолійович.

3. Виступи присутніх.

З оцінкою дисертації Шахматова Івана Олександровича виступили рецензенти: завідувач кафедри комп'ютерної інженерії, кандидат технічних наук, доцент Лащевська Наталія Олександрівна, доцент кафедри технологій цифрового розвитку, кандидат технічних наук, Аронов Андрій Олексійович, які зазначили актуальність теми дослідження, високий рівень наукової новизни отриманих результатів, їх відповідність сучасним світовим тенденціям розвитку програмного, а також значну практичну цінність щодо забезпечення цілісності і безпеки вебсистем.

Серед зауважень було відзначено доцільність деталізації питання вибору та налаштування окремих параметрів моделі, оскільки це дало б змогу глибше простежити вплив цих параметрів на точність прийняття рішень у вебсистемі, розширення експериментальної бази, оскільки доцільно було б детальніше проаналізувати питання масштабованості запропонованого підходу для розподілених вебсистем із високоінтенсивними потоками критичних подій.

В обговоренні взяли участь присутні: директор навчально-наукового інституту інформаційних технологій, доктор технічних наук, професор Нестеренко Катерина Сергіївна, доцент кафедри інженерії програмного забезпечення, доктор філософії (PhD) Залива Віталій Вікторович, доцент кафедри інженерії програмного забезпечення, доктор філософії (PhD) Худік Богдан Олександрович, старший викладач кафедри інженерії програмного забезпечення, доктор філософії (PhD) Коваленко Данило Сергійович, завідувач кафедри інформаційних систем та технологій, доктор технічних наук, професор Сторчак Каміла Павлівна, доцент кафедри комп'ютерної

інженерії, кандидат технічних наук, старший науковий співробітник Торошанко Ярослав Іванович, доцент кафедри технологій цифрового розвитку, кандидат технічних наук Ананченко Олексій Євгенович, доцент кафедри комп'ютерних наук, кандидат технічних наук, доцент Гніденко Микола Петрович, професор кафедри управління кібербезпекою та захистом інформації доктор технічних наук, професор Савченко Віталій Анатолійович, які у своїх виступах відзначили актуальність дослідження у контексті сучасних вимог до забезпечення безпеки, довіри, цілісності та надійності вебсистем, а отримані результати мають високий практичний потенціал для побудови та модернізації захищених вебсистем, що підтверджується результатами експериментальної перевірки й впровадження у практичну діяльність підприємств.

У процесі обговорення відзначено актуальність теми, наукову новизну і практичне значення основних результатів дисертації, особистий внесок здобувача у вирішенні поставленої наукової задачі, а також можливість практичного застосування отриманих наукових результатів у сфері оптимізації вебсистем.

З характеристикою здобувача виступила науковий керівник – доктор технічних наук, професор Замрій Ірина Вікторівна, яка відзначила високий рівень наукової зрілості здобувача, його здатність до постановки та розв'язання складних задач, самостійність у проведенні наукових досліджень, а також уміння застосовувати сучасні методи та технології для побудови цілісного підходу, у межах якого поєднано криптографічну фіксацію подій, графове контекстне оцінювання ризику, кероване реагування та незмінне журналювання результатів. Отримані результати мають високий практичний потенціал для побудови та модернізації захищених вебсистем, що підтверджується результатами експериментальної перевірки й впровадження у практичну діяльність підприємств. У ході виконання дисертаційної роботи автором досягнуто мети дослідження шляхом побудови моделей і методів забезпечення довіри й цілісності в архітектурі вебзастосунків. Отримані результати мають важливе практичне значення, оскільки можуть бути використані для побудови або модернізації вебсистем із підвищеними вимогами до безпеки, простеження критичних подій, доказового аудиту та адаптивного виявлення підозрілої активності. Здобувач демонструє належний рівень наукової культури, відповідальне ставлення до досліджень, сформовані навички роботи з науковими джерелами та готовність до самостійної науково-дослідної діяльності, а проведене дисертаційне дослідження за рівнем наукової новизни, методологічною обґрунтованістю та прикладною значущістю відповідає вимогам, що висуваються до робіт на здобуття ступеня доктора філософії за спеціальністю 121 – Інженерія програмного забезпечення. Робота виконана державною мовою, з дотриманням норм та правил академічної доброчесності.

ВИСНОВОК
міжкафедрального наукового семінару про наукову новизну, теоретичне та практичне значення результатів дисертації
Шахматова Івана Олександровича на тему:
«Моделі та методи забезпечення довіри й цілісності у вебсистемах»
поданої на здобуття наукового ступеня доктора філософії
за спеціальністю 121 – Інженерія програмного забезпечення,
галузі знань 12 – Інформаційні технології

1. Актуальність теми дисертації та її зв'язок з державними програмами, науковими напрямами університету та кафедри

Актуальність дослідження зумовлена обмеженнями, притаманними традиційним підходам до забезпечення безпеки вебсистем, зокрема щодо їхньої здатності одночасно забезпечувати контроль цілісності даних, доказовість критичних подій, адаптивне виявлення підозрілої активності та підтримку функціональної стійкості вебзастосунків в умовах еволюції кіберзагроз. Багато існуючих рішень розв'язують ці завдання ізольовано: одні орієнтовані переважно на журналювання та аудит, інші — на виявлення атак і аномалій, однак не забезпечують їх узгодженого функціонування в межах єдиного архітектурного контуру. Це призводить до зниження ефективності захисту, ускладнення перевірки інцидентів і втрати довіри як до даних, так і до результатів їх обробки. Важливою науковою задачею є побудова моделей і методів, які одночасно враховують необхідність контролю цілісності критичних подій, незмінного журналювання, адаптивного виявлення вебспаму та підозрілої активності, а також обґрунтованого реагування на загрози у вебсередовищі. Це потребує поєднання криптографічних механізмів, зокрема блокчейн-верифікованого журналювання, з сучасними методами машинного навчання, насамперед графовими нейронними мережами, у межах єдиної моделі прийняття та фіксації рішень. Дане дослідження має на меті подолати обмеження традиційних підходів шляхом розроблення моделі інтегрованого контуру довіри й цілісності та методів, що забезпечують узгоджене поєднання доказового журналювання, контролю доступу, інтелектуального виявлення загроз і аудитно підтверджуваного реагування у вебсистемах. Таким чином, розроблення моделі інтегрованого контуру довіри й цілісності та відповідних методів блокчейн-верифікованого журналювання, графово-нейромережевого виявлення вебспаму й інтегрованого забезпечення довіри й цілісності у вебсистемах є актуальним у контексті зростання складності вебзагроз, цифровізації критичних сервісів і потреби у підвищенні безпеки, доказовості, надійності та функціональної стійкості сучасних вебзастосунків.

Дисертаційне дослідження пов'язане з науковими дослідженнями, які проводились у межах науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій на кафедрі інженерії програмного забезпечення: «Забезпечення функціональної стійкості інформаційних систем підприємства в умовах впливу дестабілізуючих факторів із застосуванням нейронних мереж» (держаний реєстраційний номер 0121U107501, термін виконання 2021-2025 роки) та «Методи побудови функціонально стійких

захищених інформаційних систем з централізованим управлінням» (держаний реєстраційний номер 0125U002823, термін виконання 2025-2027 роки).

2. Особистий внесок здобувача в отриманні наукових результатів

Дисертаційна робота Шахматова Івана Олександровича «Моделі та методи забезпечення довіри й цілісності у вебсистемах» є самостійним науковим дослідженням, у межах якого автором здійснено розв'язання комплексної наукової задачі, що поєднує теоретичне обґрунтування, математичне моделювання, створення алгоритмів та їхню експериментальну перевірку.

Здобувачем сформульовано концепцію дослідження, обґрунтовано актуальність теми, розроблено модель інтегрованого контуру довіри й цілісності у вебсистемах, 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. Автором також реалізовано програмний прототип, проведено експериментальну перевірку запропонованих рішень та виконано аналіз отриманих результатів.

Усі основні наукові положення, висновки та результати дисертаційної роботи отримані здобувачем особисто.

3. Достовірність та обґрунтованість отриманих результатів та запропонованих автором рішень, висновків, рекомендацій

Наукова обґрунтованість і достовірність отриманих результатів підтверджується теоретичним обґрунтуванням базових положень дослідження, коректністю застосованого математичного та алгоритмічного апарату, а також результатами їх апробації. Достовірність результатів забезпечується узгодженістю теоретичних положень із результатами експериментальних досліджень.

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 аудитної 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.

У дисертації використано лише ті моделі, методи та програмні рішення, які є результатом власної наукової роботи здобувача. Усі наукові результати, представлені в роботі, відображають особистий внесок автора у формалізацію задачі забезпечення довіри й цілісності у вебсистемах, розроблення моделі інтегрованого контуру довіри й цілісності, відповідних методів контролю критичних подій і виявлення підозрілої активності, а також у реалізацію програмного прототипу та проведення його експериментальної перевірки.

Експериментальна перевірка запропонованих моделі та методів проводилась на основі розробленого програмного прототипу, призначеного для дослідження функціонування інтегрованого контуру довіри й цілісності у типових сценаріях використання вебсистем. Експериментальна база дослідження була орієнтована на оцінювання ефективності рішень щодо контролю критичних подій, виявлення вебспаму, фіксації підозрілої активності та забезпечення цілісності даних у процесах обробки, зберігання та передачі інформації. Для оцінювання результативності запропонованих рішень застосовувалися показники точності, повноти, F1-міри, частки хибних спрацьовувань, швидкодії та накладних витрат. За результатами експериментальних досліджень встановлено, що застосування розробленої моделі інтегрованого контуру довіри й цілісності та запропонованих методів дозволяє підвищити F1-міру виявлення підозрілої активності на 17,9% для класу SUBMIT і на 21,6% для домену TX, зменшити частку хибних спрацювань відповідно на 65,4% і 57,9%, а також підтвердити стабільність функціонування запропонованого контуру в умовах обробки різнорідних подій із збереженням контрольованої швидкодії та цілісності даних системи. Це підтверджує придатність розробленого підходу для використання у вебсистемах із підвищеними вимогами до безпеки, доказовості, простежуваності та функціональної стійкості.

4. Наукова новизна результатів дисертації

У дисертації отримано наукові результати, новизна яких полягає у наступному:

- *вперше розроблено* модель інтегрованого контуру довіри й цілісності (ІКДЦ), 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 вебспаму та підозрілої активності у вебсистемах, що ґрунтується на моделі ІКДЦ та багатопредставленому графовому описі подій, поданих через систему ознак технічного, змістовного, часово-поведінкового, контектного характеру з урахуванням зв'язків між подіями й результатами аналітичного оцінювання, що забезпечує розрізнення легітимних, підозрілих і шкідливих звернень, підвищує точність виявлення вебспаму 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 вебспаму й підозрілої активності, а також на теорії композиції функціональних відображень критичних подій у класі рішеннь, що забезпечує цілісність системи, простежуваність та точність прийняття рішень.

5. Теоретичне та практичне значення результатів дисертаційної роботи

Теоретичне значення результатів дисертаційної роботи полягає в розвитку науково-методичних положень забезпечення довіри й цілісності вебсистем на основі розроблення нової моделі інтегрованого контуру довіри й цілісності та методів, що формалізують критичні події, пов'язані з ними сутності, ознаки, рішення аналітичного модуля, політики реагування та процедури незмінного журналювання. Запропонована модель інтегрованого контуру довіри й цілісності і розроблені на її основі методи поглиблюють теоретичні положення програмної інженерії щодо побудови архітектур вебзастосунків, у яких контроль цілісності, аудитна перевірність, простежуваність подій і адаптивне виявлення підозрілої активності розглядаються як взаємопов'язані складові єдиного контуру довіри й цілісності.

Отримані результати розширюють теоретичні засади забезпечення довіри й цілісності вебсистем шляхом обґрунтування єдиного підходу до формалізованого подання, аналізу, фіксації та перевірки критичних подій у вебсередовищі. На відміну від підходів, у яких контроль цілісності, аудит подій і виявлення загроз розглядаються окремо, у роботі ці складові узгоджено в межах інтегрованого контуру довіри й цілісності, що поглиблює теоретичне розуміння архітектури вебзастосунку як цілісного середовища фіксації, аналізу, перевірки та відтворення рішень щодо критичних подій.

Запропоновані наукові положення забезпечують теоретичне обґрунтування побудови інтегрованого контуру довіри й цілісності у вебсистемах, у межах якого незмінне журналювання критичних подій, криптографічна перевірка цілісності, графово-нейромережеве виявлення підозрілої активності та політики реагування узгоджуються в єдину систему прийняття й перевірки рішень. У теоретичному аспекті це розширює уявлення про довіру, цілісність, доказовість, простежуваність, відтворюваність і контрольованість як взаємопов'язані характеристики функціонування вебсистем.

Практичне значення наукових результатів полягає у наступному:

1. Завдяки застосуванню розробленої моделі інтегрованого контуру довіри й цілісності у вебсистемах можливо без повної перебудови наявної прикладної інфраструктури реалізувати окрему підсистему контролю критичних подій, цілісності даних та аудитної перевірності. Модель дозволяє інтегрувати у функціонуючі вебсервіси незмінне журналювання подій, контроль цілісності SQL-операцій, засоби доказового аудиту та механізми інтелектуального виявлення загроз.

2. Практично корисною властивістю програмного прототипу, побудованого на основі розроблених моделі та методів, є його здатність поєднувати адаптивне виявлення підозрілої активності з доказовим журналюванням рішень у межах єдиного захисного контуру. Це забезпечує підвищення якості детекції, зниження навантаження на ручну модерацію та створює можливість незалежного ретроспективного аудиту рішень системи безпеки.

3. Програмне забезпечення, що реалізує розроблені методи забезпечення довіри й цілісності критичних подій, виявлення вебспаму та інтегрованого захисту вебсистем, має потенціал до універсального застосування, зокрема у задачах захисту вебформ, контролю критичних SQL-операцій, виявлення підозрілої активності у вебтрафіку, аналізу інцидентів та побудови захищених модулів для систем електронної комерції, корпоративних вебзастосунків, інформаційних сервісів і вебплатформ, що працюють із критичними даними.

4. Результати дисертаційної роботи реалізовані у вигляді моделі підсистеми довіри й цілісності у вебсистемах, методів забезпечення цілісності критичних подій, виявлення вебспаму та інтегрованого забезпечення довіри й цілісності, а також програмного прототипу для їх експериментальної перевірки. Основні положення та результати дослідження впроваджено у ТОВ «ШЛІФАРБ», ТОВ «АРМА МОТОРС КИЇВ» та Інституті програмних систем НАН України, а окремі результати дисертаційної роботи використані у навчальному процесі Державного університету інформаційно-комунікаційних технологій.

5. У результаті експериментальних досліджень встановлено, що застосування розробленої моделі інтегрованого контуру довіри й цілісності та запропонованих методів дозволяє підвищити F1-міру виявлення підозрілої активності на 17,9% для подій надсилання вебформ і на 21,6% для

транзакційних подій, зменшити частку хибних спрацювань відповідно на 65,4% і 57,9%, а також забезпечити повноту виявлення MITM-атак на рівні 98% при керованих накладних витратах близько 23% за часом обробки 95% подій, що свідчить про прикладну доцільність і ефективність запропонованих рішень.

Наявність результатів апробації та можливість їх практичного впровадження підтверджує значущість виконаної роботи для розвитку як наукового напряму, так і прикладних аспектів сучасних вебсистем.

6. Оцінка структури та обсягу дисертації, її мови та стилю

Дисертаційна робота має чітку, логічно вибудувану та внутрішньо узгоджену структуру, що повністю відповідає поставленій меті, завданням і логіці проведеного дослідження. Виклад матеріалу є послідовним, системним і аргументованим, що забезпечує цілісне сприйняття отриманих результатів та їх наукову обґрунтованість.

Обсяг дисертації є достатнім для повного розкриття теми дослідження, а її структура та науковий стиль викладу матеріалу відповідає сучасним вимогам до наукових робіт на здобуття ступеня доктора філософії, зокрема щодо повноти викладення теоретичних положень, моделей, методів та результатів експериментальних досліджень.

Дисертація виконана фаховою українською мовою, текстове подання матеріалу відповідає стилю науково-дослідної літератури і характеризується науковою коректністю, точністю використаної термінології та відповідністю вимогам академічного стилю. Виклад матеріалу є чітким, логічно вивіреним і доступним для сприйняття фахівцями у галузі інженерії програмного забезпечення.

Зміст, структура, оформлення дисертації та кількість публікацій відповідають вимогам п.6-9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 №44 (зі змінами), наказу Міністерства освіти і науки України від 12.07.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023. За своїм фаховим спрямуванням, науковою новизною і практичною значущістю дисертація Шахматова Івана Олександровича відповідає спеціальності 121 – Інженерія програмного забезпечення, галузі 12 – Інформаційні технології, що підтверджує належний рівень підготовки дисертації до подання у спеціалізовану вчену раду.

7. Результати перевірки роботи на академічний плагіат

Дисертаційна робота була перевірена автоматизованим сервісом пошуку плагіату StrikePlagiarism.com. Результати перевірки зафіксовано у звіті від «24» квітня 2026 р. З результатами звіту подібності, згенерованого системою виявлення збігів/ідентичності/схожості, ознайомлено.

Висновки щодо запозичень, виявлених у роботі, є коректними, запозичення мають належні посилання, не є плагіатом, а дисертаційна робота є самостійним науковим дослідженням і може бути рекомендована до захисту.

На підставі вивчення тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації, самоплагіату.

Усі використані здобувачем в тексті дисертації власні наукові праці без посилання на ці праці були попередньо опубліковані з метою висвітлення в них основних наукових результатів дослідження та вказані в анотації дисертаційної роботи.

Інші факти, встановлені рецензентами у процесі перевірки: відсутні.

Висновок: За результатами перевірки дисертація Шахматова Івана Олександровича визнана оригінальною роботою, яка не містить елементів академічного плагіату.

8. Перелік наукових праць, які відображають основні результати дисертації

Статті у наукових фахових виданнях України категорії Б:

1) Шахматов І.О. Технологія Blockchain як інструмент протидії неправомірному використанню доступу до веб-сайтів. Зв'язок, № 1, 2024. С.20-25. DOI: 10.31673/2412-9070.2024.012025.

Особистий внесок здобувача: ***Шахматовим І.О. запропоновано підхід до підвищення безпеки вебсайтів на основі інтеграції блокчейну, коефіцієнта Джині та кривої Лоренца, розроблено алгоритм і проведено його тестування.***

2) Шахматов І.О., Замрій І.В. Потенціал блокчейну у покращенні безпеки вебсайтів. Сучасний захист інформації, 2024, № 1(57). С.28-38. DOI: 10.31673/2409-7292.2024.010004.

Особистий внесок здобувача: ***Шахматовим І.О. проведено порівняльний аналіз блокчейн-технологій і традиційних методів безпеки вебсайтів, досліджено вплив кількості блоків та якості шифрування на точність рішень і швидкість обробки запитів, розроблено комплексну формулу оцінки надійності системи.***

3) Замрій І.В., Шахматов І.О. Підвищення безпеки веб-застосунків через інноваційні патерни інтеграції штучного інтелекту. Сучасний стан наукових досліджень та технологій в промисловості, № 1(27) (2024). С. 67–80 DOI: 10.30837/ITSSI.2024.27.067.

Особистий внесок здобувача: ***Шахматовим І.О. визначено критерії оцінювання ризикованості фінансових транзакцій, розроблено UML-схему класів програмної бібліотеки, алгоритм роботи моделі, псевдокод, методи генерації тестових даних і проведено тестування моделі на фінансових даних.***

4) Замрій І. В., Шахматов І. О. Інтегрована система безпеки для захисту синхронізації платежів від MITM-атак. Проблеми програмування. 2025. № 2. С. 28–39. DOI: 10.15407/pp2025.02.028.

Особистий внесок здобувача: ***Шахматовим І.О. досліджено сценарії MITM-атак у багатоканальних платіжних системах, розроблено багаторівневу архітектуру інтегрованої системи безпеки та обґрунтовано поєднання методів штучного інтелекту, цифрових підписів, часових міток і додаткової клієнтської верифікації.***

5) Замрій І. В., Шахматов І. О. Автоматизація оцінки безпеки вебзастосунків засобами Python. Зв'язок. 2025. № 4 (176). С. 58–66. DOI: 10.31673/2412-9070.2025.045866.

Особистий внесок здобувача: ***Шахматовим І.О. розроблено модель автоматизованої оцінки безпеки вебзастосунків, реалізовано зіставлення результатів сканування з еталонним набором вразливостей, класифікацію TP, FP, FN, TN, розрахунок метрик Precision, Recall і Accuracy та архітектуру Python-мультисканерної платформи.***

6) Шахматов І. О. Інтегрований контур довіри у вебзастосунках на основі графового оцінювання ризику та незмінного журналювання рішень. Зв'язок. 2026. № 2 (180). С.72-78. DOI: 10.31673/2412-9070.2026.024909.

Особистий внесок здобувача: ***Шахматовим І.О. розроблено інтегрований контур довіри у вебзастосунках на основі графового оцінювання ризику, незмінного журналювання рішень і перевірки цілісності критичних подій.***

Публікації в наукових фахових виданнях, що індексуються в міжнародних базах Scopus/WoS:

7) Zhurakovskyi, B., Averichev, I., and Shakhmatov, I. Using the Latest Methods of Cluster Analysis to Identify Similar Profiles in Leading Social Networks. CEUR Workshop Proceedings; 10th International Scientific Conference Information Technology and Implementation, IT and I-WS 2023; Volume 3646, 2023, Pages 116-126 (SCOPUS).

Особистий внесок здобувача: ***Шахматовим І.О. розроблено алгоритм роботи прототипу та проведено його тестування.***

8) Замрій І.В., Шахматов І.О., Яскевич В.О. Blockchainsqlsecure: Інтеграція блокчейн-технології для зміцнення захисту від SQL-ін'єкцій. Вісник Київського національного університету імені Тараса Шевченка. Фізико-математичні науки, № 1(78), 2024. С. 160-168. DOI: 10.17721/1812-5409.2024/1.29 (SCOPUS).

Особистий внесок здобувача: ***Шахматовим І.О. розроблено концепцію BlockchainSQLSecure, сформовано архітектуру блокчейн-журналу SQL-запитів, запропоновано механізм валідації SQL-запитів через smart-контракти та підхід до децентралізованого зберігання журналів.***

9) I. Zamrii, I. Shakhmatov, O. Yudin, Y. Diana, M. Tyshchenko and Y. Rudenko, Methods for Detecting DDoS Attacks in Web Traffic Using Autoencoders with an Adaptive Three-Level Approach. 2024 IEEE 5th International Conference

on Advanced Trends in Information Theory (ATIT), Lviv, Ukraine, 2024, pp. 1-5, DOI: 10.1109/ATIT64324.2024.11222524 (SCOPUS).

Особистий внесок здобувача: ***Шахматовим І.О. розроблено метод виявлення DDoS-атак у вебтрафіку на основі автоенкодерів, запропоновано трирівневу схему класифікації запитів і механізм донавчання моделі з урахуванням реальних даних та експертної оцінки.***

10) Zamrii I., Shakhmatov I. Multi-View Graph Model with Representation Alignment and Adaptive Fusion for Better Spam Detection. Proceedings of the Workshop on Cryptology and Data Security (WCDS 2025), co-located with SMICS 2025, Lviv, Ukraine, October 16–18, 2025. CEUR Workshop Proceedings. 2026. Vol. 4191. P. 99–106 (SCOPUS).

Особистий внесок здобувача: ***Шахматовим І.О. розроблено мультирепрезентаційну графову модель виявлення вебспаму, сформовано три подання подій, запропоновано механізми узгодження представлень, адаптивного злиття ознак і контрастивного навчання, проведено експериментальне оцінювання моделі.***

9. Апробація основних результатів дослідження на конференціях, симпозіумах, семінарах тощо

Основні результати дисертаційної роботи апробовано на наукових конференціях, симпозіумах та наукових семінарах, зокрема:

1) Шахматов І.О., Замрій І.В. Технологія блокчейн як інструмент протидії неправомірному використанню доступу до веб-сайтів. Матеріали V Міжнародної науково-практичної конференції молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології (Soft Tech-2023)», 19-21 грудня 2023 р., Київ. С. 360-364.

2) Замрій І.В., Шахматов І.А. Посилення безпеки веб-ідентифікації через технологію блокчейн. Всеукраїнська науково-технічна конференція «Застосування програмного забезпечення в інформаційно-комунікаційних технологіях», 24 квітня 2024 року, Київ ДУІКТ, 2024. С. 249-253.

3) Шахматов І.О., Замрій І.В. Використання блокчейн-технології для підвищення безпеки від SQL ін'єкцій. XIII Міжнародна науково-технічна конференція "Безпека інформаційних технологій: ITSEC-2024", 9-11 травня 2024 р. Львів. С.98-101.

4) Шахматов І. О., Замрій І. В. Технології масштабування даних у боротьбі з DDOS-атаками. Науково-практична конференція «Штучний інтелект і безпека», 19-21 листопада 2024 р. Київ. С. 27-30.

5) Білодід Д. В., Шахматов І. О. Ефективність CSRF-токенів у запобіганні міжсайтовим запитам у фронтенд-додатках. Всеукраїнська науково-технічна конференція «Виклики та рішення в програмній інженерії», 26 листопада 2024 р. Київ. С. 92-96.

6) Шахматов І.О., Замрій І.В. Адаптивні нейромережі у боротьбі з веб-спамом. ITSec: Безпека інформаційних технологій: матеріали XIV Міжнар. наук.-техн. конф., м. Тернопіль, 22-24 трав. 2025 р. Тернопіль-Київ: ЗУНУ-ДУІКТ, 2025. С. 211-213.

7) Замрій І.В., Шахматов І.О. Мультирепрезентаційна GNN-модель з узгодженням і адаптивним злиттям для детекції спаму. SMICS: Безпека сучасних інформаційно-комунікаційних систем. м. Львів, 16-18 жовтня 2025 р. ЛНУ ім. І. Франка, 2025, с. 320-325.

8) Замрій І.В., Нестеренко К.С., Задонцев Ю.В., Глушкова О.І., Шахматов І.О. Методика підвищення функціональної стійкості інформаційної системи через виявлення вторгнень та реконфігурації мережі. Матеріали XIV Міжнародної науково-практичної конференції «Математика. Інформаційні технології. Освіта», Луцьк - Світязь, 13-15 червня 2025 р. С. 101-104.

9) Бовкун І.В., Шахматов І.О. Визначення вимог до веб-системи для управління безконтактними замовленнями у ресторані. II Всеукраїнська науково-технічна конференція «Виклики та рішення в програмній інженерії». Збірник тез. Київ: ДУІКТ, 2025. С. 432–434.

Основні положення та результати дисертаційної роботи доповідалися та обговорювалися на зазначених наукових заходах, що підтверджує їх апробацію, наукову значущість та зацікавленість наукової спільноти.

У ході обговорення дисертації до неї не було висунуто жодних зауважень щодо самої суті роботи.

УХВАЛИЛИ:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Шахматова Івана Олександровича на тему «Моделі та методи забезпечення довіри й цілісності у вебсистемах».

2. Констатувати, що за актуальністю, ступенем наукової новизни, обґрунтованістю, теоретичним та практичним значенням, науковою та практичною цінністю здобутих результатів дисертація Шахматова Івана Олександровича відповідає спеціальності 121 – Інженерія програмного забезпечення, галузі знань 12 – Інформаційні технології, та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261, пп. 6, 7, 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44.

У 10 (десятити) наукових публікаціях повністю відображені основні результати дисертації, з них 6 (шість) статей у наукових фахових виданнях України категорії Б, 1 (одна) стаття у виданні, яке входить до міжнародної науко метричної бази Scopus та 3 (три) матеріалів конференцій, що індексуються науко-метричною базою даних Scopus.

3. Рекомендувати дисертацію Шахматова Івана Олександровича на тему «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, для подання до захисту у разовій спеціалізованій вченій раді.

Результати голосування щодо затвердження Висновку та рекомендації до захисту дисертації:

«За» 15 (п'ятнадцять)
«Проти» немає –
«Утримались» немає –

Головуючий на міжкафедральному науковому семінарі
Директор Навчально-наукового інституту
інформаційних технологій,
д-р тех. наук, професор _____ Катерина НЕСТЕРЕНКО

Рецензенти:
Доцент кафедри
технологій цифрового розвитку,
канд. тех. наук _____ Андрій АРОНОВ

Завідувач кафедри
комп'ютерної інженерії,
канд. тех. наук, доцент _____ Наталія ЛАЩЕВСЬКА

Відповідальний секретар
Доцент кафедри
інженерії програмного забезпечення,
доктор філософії (PhD) _____ Богдан ХУДІК

«04» травня 2026 року