ЗАТВЕРДЖЕНО
Наказ Міністерства освіти і науки України
24 квітня 2024 року № 578

# Рішення
# разової спеціалізованої вченої ради
# про присудження ступеня доктора філософії

Здобувач (ка) ступеня доктора філософії **Іван ШАХМАТОВ**,
(власне ім'я, прізвище здобувача (ки))
1984 року народження, громадянин України,
(назва держави, громадянином якої є здобувач (ка))
освіта вища: закінчив у 2007 році Національний авіаційний університет
(найменування закладу вищої освіти)
за спеціальністю «Автоматизовані системи управління»
(за дипломом)
працює викладач в Державному університеті інформаційно-комунікаційних технологій, Київ,
(посада) (місце основної роботи, підпорядкування, місто)
Здійснював підготовку в аспірантурі Державного університету інформаційно-комунікаційних технологій (2023-2026 рр.), виконав акредитовану освітньо-наукову програму «Інженерія програмного забезпечення» зі спеціальності 121 «Інженерія програмного забезпечення», галузі знань 12 «Інформаційні технології».
Разова спеціалізована вчена рада, утворена наказом Державного університету інформаційно-комунікаційних технологій, Міністерства освіти і науки України, м. Київ
(повне найменування закладу вищої освіти (наукової установи), підпорядкування (у родовому відмінку), місто)
від «22» травня 2026 року № 229, у складі:

**Голови разової спеціалізованої вченої ради** – **Віталія САВЧЕНКО**, доктора технічних наук, професора, професора кафедри управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

**Рецензентів** – **Андрія АРОНОВА**, кандидата технічних наук, доцента кафедри технологій цифрового розвитку Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

**Наталії ЛАЩЕВСЬКОЇ**, кандидата технічних наук, доцента, завідувача кафедри комп'ютерної інженерії Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

**Офіційних опонентів** – **Ярослава КОРНАГИ**, доктора технічних наук, професора, декана факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

**Світлани РЗАЄВОЇ**, кандидата технічних наук, доцента, доцента кафедри комп'ютерних наук Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

На засіданні «30» червня 2026 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології

(галузь знань)

Івану ШАХМАТОВУ

(власне ім'я, прізвище здобувача (ки) у давальному відмінку)

на підставі публічного захисту дисертації «Моделі та методи забезпечення довіри й цілісності у вебсистемах»

(назва дисертації)

за спеціальністю (спеціальностями) 121 «Інженерія програмного забезпечення»

(код і найменування спеціальності (спеціальностей)відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Дисертацію виконано у (в) Державному університеті інформаційно-комунікаційних технологій, Міністерства освіти і науки України, м. Київ

(найменування закладу вищої освіти (наукової установи), підпорядкування, місто)

Науковий керівник:

Ірина ЗАМРІЙ, доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій,

(власне ім'я, прізвище, науковий ступінь, вчене звання, місце роботи, посада)

Дисертацію виконано державною мовою, структура та правила оформлення дисертації відповідають вимогам, затвердженим наказом МОН України від 12.01.2017 №40, подано у вигляді спеціально підготовленого рукопису, який є завершеним науковим дослідженням, що здійснює вагомий внесок у розвиток теоретичних і практичних аспектів забезпечення довіри, цілісності, доказовості та функціональної стійкості вебсистем. Запропоновані автором науково-практичні підходи сприяють удосконаленню механізмів контролю критичних подій, незмінного журналювання, виявлення підозрілої активності, захисту вебформ, SQL-операцій і транзакційних процесів у вебзастосунках.

Результати дисертаційного дослідження мають наукову новизну та практичне значення, спрямовані на розв'язання актуального наукового завдання – розробці та обґрунтуванні моделей і методів забезпечення довіри, цілісності та надійності вебсистем на рівні архітектури вебзастосунків шляхом поєднання незмінного журналювання критичних подій із застосуванням методів машинного навчання для автоматизованого виявлення вебспаму та аномалій вебтрафіку, що сприяє підвищенню цілісності, безпеки, керованості, доказовості й стійкості вебсервісів до комбінованих загроз.

Запропоновані у дисертації методи і моделі є логічно обґрунтованими, мають прикладний характер і можуть бути використані у науковій, освітній та практичній діяльності. Дисертаційна робота Шахматова І.О. засвідчує належний рівень теоретичної підготовки здобувача, його здатність самостійно проводити наукові дослідження, формулювати обґрунтовані висновки та пропозиції, що підтверджує наукову зрілість, ґрунтовну підготовку та високу компетентність здобувача, а також завершеність і цілісність виконаної ним наукової роботи.

*Наукові результати, отримані в дисертаційній роботі:*

- *вперше* розроблено модель інтегрованого контуру довіри й цілісності у вебсистемі, яка за рахунок кортежно-графового подання критичних подій, 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, 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 інтегрованого контуру довіри й цілісності та теорії криптографічно зв'язаного ланцюга подій із хешуванням, цифровим підписом і пороговим правилом 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 грунтується на моделі інтегрованого контуру довіри й цілісності та багатопредставленому графовому описі подій через систему технічних, змістовних, часово-поведінкових і контекстних ознак, 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 грунтується на моделі інтегрованого контуру довіри й цілісності, 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 класи рішень, що забезпечує цілісність системи, простежуваність та точність прийняття рішень.

Авторський внесок полягає у формалізації задачі забезпечення довіри й цілісності у вебсистемах, побудові моделі інтегрованого контуру довіри й цілісності (ІКДЦ), створенні методу забезпечення довіри й цілісності критичних подій і даних, методу виявлення вебспаму та підозрілої активності у вебсистемах на основі ІКДЦ і методу інтегрованого забезпечення довіри й цілісності у вебсистемах, що грунтується на комбінації моделі ІКДЦ, блокчейн-верифікованого журналювання критичних подій і графово-нейромережевого аналізу підозрілої активності, а також у реалізації прототипу програмного рішення та проведенні експериментальної перевірки запропонованих рішень з аналізом отриманих результатів. Результати дисертаційної роботи реалізовано 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.

*Практичне значення наукових результатів полягає у наступному:*

1.Розроблені модель і методи дозволяють реалізувати в архітектурі вебзастосунку окрему підсистему довіри та контролю цілісності без повної перебудови існуючої прикладної інфраструктури. Це дозволяє інтегрувати незмінне журналювання критичних подій, контроль цілісності SQL-операцій, доказовий аудит рішень і засоби інтелектуального виявлення загроз у вже функціонуючі вебсервіси.

2.Практичне значення моделі ІКДЦ та розроблених на її основі методів полягає у поєднанні адаптивного виявлення загроз із доказовим журналюванням рішень, що забезпечує підвищення якості детекції, зниження навантаження на ручну модерацію та можливість незалежного ретроспективного аудиту рішень системи безпеки.

3.Програмні засоби, що реалізують метод виявлення вебспаму та підозрілої активності у вебсистемах, впроваджено у практичну діяльність ТОВ «ШЛІФАРБ», а програмні засоби, що реалізують метод забезпечення довіри й цілісності критичних подій і даних на основі блокчейн-орієнтованого контролю цілісності критичних подій і журналювання транзакційних операцій, - у практичну діяльність ТОВ «АРМА МОТОРС КИЇВ», що підтверджується відповідними актами впровадження. Результати дисертаційного дослідження, що стосуються моделі інтегрованого контуру довіри й цілісності у вебсистемі, методу блокчейн-верифікованого журналювання критичних подій і контролю доступу у вебсистемах, методу графово-нейромережевого виявлення вебспаму та підозрілої активності у вебсистемах і методу інтегрованого забезпечення довіри й цілісності у вебсистемах, також впроваджено в Інституті програмних систем Національної академії наук України при формуванні плану перспективних наукових досліджень, що підтверджується актом впровадження. За результатами впровадження у ТОВ «ШЛІФАРБ» узагальнений показник якості автоматичного розпізнавання повідомлень зріс з 78% до 92%, а частка помилкових спрацювань зменшилася з 2,6% до 0,9%. За результатами впровадження у ТОВ «АРМА МОТОРС КИЇВ» узагальнений показник якості виявлення ризикових ситуацій зріс з 74% до 90%, частка помилкових спрацювань зменшилася з 1,9% до 0,8%, а повнота виявлення атак

типу MITM на канали обміну транзакційними подіями склала 98%. Контрольне оцінювання результатів впровадження в Інституті програмних систем НАН України показало, що застосування методу інтегрованого забезпечення довіри й цілісності у вебсистемах дозволяє підвищити якість оцінювання критичних подій з 85% до 96%, а частку помилкових спрацювань зменшити з 3% до 0,8%, що підтверджує ефективність запропонованого підходу для задач забезпечення довіри й цілісності у вебсистемах. Окремі результати дисертаційного дослідження також використано в освітньому процесі Державного університету інформаційно-комунікаційних технологій.

4.У результаті експериментальних досліджень встановлено, що застосування методу інтегрованого забезпечення довіри й цілісності у вебсистемах на основі моделі інтегрованого контуру довіри й цілісності дозволяє зменшити частку хибних спрацювань для класу подій SUBMIT на 65,4% порівняно з базовою конфігурацією на основі правил, що підтверджує практичну доцільність використання запропонованих методів у вебсистемах із підвищеними вимогами до точності виявлення підозрілої активності.

5.Розроблений прототип програмного забезпечення реалізує модель інтегрованого контуру довіри й цілісності та розроблені на її основі методи у вигляді окремого програмного компонента, який може бути інтегрований у наявне вебсередовище без повної зміни бізнес-логіки системи. Практична цінність прототипу полягає в тому, що він може застосовуватися у вебзастосунках як додатковий контур контролю довіри й цілісності без істотної перебудови їхньої архітектури та забезпечує збір і нормалізацію критичних подій, оцінювання їх ризику, кероване реагування й незмінне журналювання результатів. Такий підхід забезпечує практичну основу для побудови підсистем довіри, проведення аудиту, перевірки політик безпеки та подальшого розвитку захисного контуру у вебсистемах.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій у межах науково-дослідної роботи «Забезпечення функціональної стійкості інформаційних систем підприємства в умовах впливу дестабілізуючих факторів із застосуванням нейронних мереж» (робота виконувалася у 2021-2025 роках, облікова картка науково-дослідної роботи 0226U000249) та науково-дослідної роботи «Методи побудови функціонально стійких захищених інформаційних систем з централізованим управлінням» (державний реєстраційний номер 0125U002823).

(наводиться аналіз дисертації щодо дотримання вимог пункту 6 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 року № 44 (зі змінами))

Здобувач має 19 наукових публікації за темою дисертації, з них 6 статей у наукових фахових виданнях України категорії Б, 4 публікації в періодичних виданнях індексованих у міжнародній наукометричній базі Scopus та 9 тез доповідей за матеріалами конференцій. Авторський внесок у роботах, написаних у співавторстві, здобувачем розкрито у списку опублікованих праць за темою дисертації.

(наводиться аналіз наукових публікацій щодо дотримання вимог пунктів 8, 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії) (зазначити наукові публікації)

*Публікації у виданнях і матеріалах конференцій, що індексуються в міжнародній наукометричній базі Scopus:*

1. Zhurakovskyi B., Averichev I., 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*. Vol. 3646. 2023. P. 116–126. SCOPUS.
2. 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. 2024. № 1(78). С. 160–168. DOI: 10.17721/1812-5409.2024/1.29. SCOPUS.

3. Zamrii I., Shakhmatov I., Yudin O., Diana Y., Tyshchenko M., Rudenko Y. 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. P. 1–5. DOI: 10.1109/ATIT64324.2024.11222524. SCOPUS.
4. 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.

*Статті у фахових наукових виданнях України категорії Б:*

5. Шахматов І. О. Технологія Blockchain як інструмент протидії неправомірному використанню доступу до веб-сайтів. *Зв'язок*. 2024. № 1. С. 20–25. DOI: 10.31673/2412-9070.2024.012025.
6. 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.
7. Замрій І. В., Шахматов І. О. Підвищення безпеки веб-застосунків через інноваційні патерни інтеграції штучного інтелекту. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 1(27). С. 67–80. DOI: 10.30837/ITSSI.2024.27.067.
8. 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.
9. 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.
10. 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.

У дисертації використано лише ті методи, моделі та програмні рішення, які є результатом власної наукової роботи здобувача. Усі наукові результати, представлені в роботі, відображають особистий внесок автора в розвиток моделей і методів забезпечення довіри й цілісності у вебсистемах. У роботах, опублікованих у співавторстві, особисто здобувачу належать: у [1] - запропоновано підхід до підвищення безпеки вебсайтів на основі інтеграції блокчейну, коефіцієнта Джині та кривої Лоренца, розроблено алгоритм і проведено його тестування; у [2] - 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; у [3] - 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; у [4] - 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; у [5] - 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; у [6] - розроблено інтегрований контур довіри у вебзастосунках на основі графового оцінювання ризику, незмінного журналювання рішень і перевірки цілісності критичних подій; у [7] - розроблено алгоритм роботи прототипу та проведено його тестування; у [8] - розроблено концепцію BlockchainSQLSecure, сформовано архітектуру блокчейн-журналу SQL-запитів, запропоновано механізм валідації

SQL-запитів через smart-контракти та підхід до децентралізованого зберігання журналів; у [9] - 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; у [10] - розроблено мультирепрезентаційну графову модель виявлення вебспаму, сформовано три подання подій, запропоновано механізми узгодження представлень, адаптивного злиття ознак і контрастивного навчання, проведено експериментальне оцінювання моделі.

*Публікації за матеріалами науково-практичних конференцій:*

1. Шахматов І. О., Замрій І. В. Технологія блокчейн як інструмент протидії неправомірному використанню доступу до веб-сайтів. *V Міжнародна науково-практична конференція молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології (Soft Tech-2023)»*, 19–21 грудня 2023 року, 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 року, 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 року, 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 року, Київ. С. 92–96.
6. Шахматов І. О., Замрій І. В. Адаптивні нейромережі у боротьбі з веб-спамом. *XIV Міжнародна науково-технічна конференція ITSec: Безпека інформаційних технологій*, м. Тернопіль, 22–24 травня 2025 року. 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 року. 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. *XIV Міжнародна науково-практична конференція «Математика. Інформаційні технології. Освіта»*, Луцьк – Світязь, 13–15 червня 2025 року. 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.

У дискусії взяли участь голова і члени спеціалізованої вченої ради та присутні на захисті фахівці:

Голова ради – САВЧЕНКО Віталій Анатолійович, доктор технічних наук, професор, професор кафедри управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надав позитивну оцінку без зауважень.

Рецензент – АРОНОВ Андрій Олексійович, кандидат технічних наук, доцент кафедри технологій цифрового розвитку Навчально-наукового інституту інформаційних технологій

Державного університету інформаційно-комунікаційних технологій надав позитивну оцінку без зауважень.

Опонент – КОРНАГА Ярослав Ігорович, доктор технічних наук, професор, декан факультету інформатики та обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» надав позитивну оцінку без зауважень.

Опонент – РЗАЄВА Світлана Леонідівна, кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Київського столичного університету імені Бориса Грінченка надала позитивну оцінку без зауважень.

Рецензент – ЛАЩЕВСЬКА Наталія Олександрівна, кандидат технічних наук, доцента завідувач кафедри комп'ютерної інженерії Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій надала позитивну оцінку із зауваженням:

1.Надано рекомендацію щодо більш повного висвітлення рекомендаційних аспектів експлуатаційних застосування запропонованого в дисертаційному дослідженні підходу.

Інші присутні:

Нестеренко Катерина Сергіївна, доктор технічних наук, професор, директор Навчально-наукового інституту інформаційних технологій Державного університету інформаційно-комунікаційних технологій. Оцінка позитивна без зауважень.

Результати відкритого голосування:

«За» 5 (п'ять) членів ради,

«Проти» немає,

«Утримались» немає.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує

Івану ШАХМАТОВУ

(власне ім'я, прізвище, здобувача (ки) у давальному відмінку)

ступінь доктора філософії з галузі знань 12 Інформаційні технології

(галузь знань)

за спеціальністю 121 «Інженерія програмного забезпечення»

(код і найменування спеціальності (спеціальностей) відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Відеозапис трансляції захисту дисертації додається.

Окрема думка члена разової ради додається (за наявності).

Голова разової спеціалізованої вченої ради

(підпис)

Віталій САВЧЕНКО

(власне ім'я та прізвище)

М.П.