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

Рішення
разової спеціалізованої вченої ради PhD14279
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії **Дмитро ГАМЗА**,
(власне ім'я, прізвище здобувача (ки))
1994 року народження, громадянин України,
(назва держави, громадянином якої є здобувач (ка))
освіта вища: закінчив (ла) у 2017 р. Національний технічний університет Київський політехнічний інститут імені Ігоря Сікорського
(найменування закладу вищої освіти)
за спеціальністю «Телекомунікаційні системи та мережі»,
(за дипломом)
Здійснював підготовку в аспірантурі Державного університету інформаційно-комунікаційних технологій (2022-2026 рр.), виконав акредитовану освітньо-наукову програму «Кібербезпека» зі спеціальності 125 «Кібербезпека», 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 № 228, у складі:

Голови разової спеціалізованої вченої ради	**Світлани КАЗМІРЧУК**, доктора технічних наук, професора, професора кафедри систем та технологій кібербезпеки, Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій. (власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Рецензентів –	**Євгенії ІВАНЧЕНКО**, доктора технічних наук, професора, директора Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій. (власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
	Світлани ЛЕГОМІНОВОЇ, доктора економічних наук, професора, завідувача 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)
Офіційних опонентів –	**Валентина СОБЧУКА**, доктора технічних наук, професора, професора кафедри інтегральних та диференціальних рівнянь механіко-математичного факультету Київського національного університету ім. Шевченка. (власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
	Максима ДЕЛЕМБОВСЬКОГО, кандидата технічних наук, доцента, завідувача Кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету архітектури та будівництва.

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

На засіданні **«03» липня 2026 року** прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології

(галузь знань)

Дмитру ГАМЗІ

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

на підставі публічного захисту дисертації «Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації»

(назва дисертації)

за спеціальністю (спеціальностями) 125 «Кібербезпека».

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

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

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

Науковий керівник:

Сергій ЗИБІН, доктор технічних наук, професор, професор кафедри систем та технологій кібербезпеки, Навчально-наукового інституту кібербезпеки та захисту інформації 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 положень, розробленню методичного забезпечення та практичних рекомендацій щодо виявлення шкідливої активності в інформаційних системах організацій на засадах гібридної класифікації та методів машинного навчання.

Результати дослідження включають розробку методів для протидії кіберзагрозам, таких як: гібридний метод на основі стекінг-архітектури; метод комплексної оптимізації вхідного набору даних (SMOTE, Min-Max нормалізація, PCA); метод багатокритеріального відбору оптимальних архітектур системи виявлення шкідливої активності в режимі реального часу. А також надані рекомендації щодо впровадження розроблених методів до виявлення мережевих аномалій, які об'єднують концепції машинного навчання, що дозволяє забезпечити надійний захист критично важливих інформаційних систем організацій.

Наукові результати, отримані в дисертаційній роботі:

- *Вперше* розроблено метод виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації, який базується на використанні гетерогенного набору базових класифікаторів та мета-класифікаторі на основі XGBoost для дворівневої стекінг-архітектури, що дає можливість застосовувати різнорідні ансамблеві методи машинного навчання у системах виявлення шкідливої активності в режимі реального часу з можливістю динамічного переналаштування класифікаторів.

- *Удосконалено* метод комплексної оптимізації вхідного набору даних методу виявлення шкідливої активності в інформаційній системі, який, на відміну від існуючих, поєднує балансування класів (SMOTE), нормалізацію (Min-Max) та зниження розмірності (PCA), що дозволило зменшити обчислювальне навантаження та підвищити точність методу гібридної класифікації.

- *Набув подальшого розвитку* метод багатокритеріального вибору оптимальної архітектури системи виявлення шкідливої активності у режимі реального часу, в якому, за рахунок використання послідовного застосування стратегії фільтрації за середніми значеннями та побудови фронту Парето забезпечується баланс між максимальною точністю виявлення шкідливої активності та мінімальними витратами обчислювальних ресурсів.

Авторський внесок полягає в розробці методу гібридної класифікації у системах виявлення шкідливої активності з можливістю динамічного переналаштування класифікаторів, методу комплексної оптимізації вхідних наборів даних та методу багатокритеріального вибору оптимальної архітектури системи виявлення шкідливої активності, що дозволило підвищити точність виявлення шкідливої активності в режимі реального часу.

Отримані наукові результати показали, що застосування методів виявлення шкідливої активності на основі гібридної класифікації, які засновані на комплексній стратегії попередньої обробки даних (SMOTE, Min-Max нормалізація, PCA), дозволяють досягти приросту точності на 3,87% та інтегральної метрики якості на 5,11%. Експериментально доведено, що найкраща конфігурація ансамблю XGBoost + CatBoost + LightGBM з мета-класифікатором XGBoost досягає Accuracy 98,07% та F1-score 96,57% при часі прогнозування 7,16 мс, що відповідає вимогам до систем виявлення вторгнень в режимі реального часу. Водночас встановлено, що середній час прогнозування скорочується на 76% – з 29,37 до 7,28 мс – завдяки PCA-редукції простору ознак з 80 до 18 компонент, що є вирішальним фактором для практичного розгортання системи в умовах інтенсивного корпоративного трафіку.

Практичне значення отриманих результатів полягає у розробці програмного рішення, яке може бути інтегроване у сучасні системи моніторингу безпеки інформаційних систем організацій. За результатами моделювання таке програмне рішення щодо виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації дозволяє забезпечити приріст точності на 3,87 % та F1-score на 5,11 %, а також скоротити найменший час прогнозування на 76 %, порівняно з відповідними результатами на необробленому датасеті. При здійсненні багатокритеріального відбору оптимальних архітектур із використанням стратегії фільтрації за середніми значеннями та побудови фронту Парето програмне рішення забезпечує максимальну точність на рівні 0,9807 та мінімальну затримку на рівні 7,16 мс, що задовольняє вимогам до систем виявлення вторгнень в режимі реального часу.

(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 9 наукових публікацій за темою дисертації, з них: 1 публікація в іноземному періодичному індексованому в Scopus/WoS виданні; 5 публікацій у фахових наукових виданнях України категорії Б та 3 тези доповідей за матеріалами конференцій, які відповідають дотриманню 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»

(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)

Публікація в іноземному періодичному індексованому в Scopus/WoS виданні:

1. Haidur H., Gakhov S., Hamza D. Using support vectors to build a rule-based system for detecting malicious processes in an organisation's network traffic. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska.* 2024. Vol. 14, No. 4. P. 90–96. https://doi.org/10.35784/iapgos.6366

Статті у наукових фахових виданнях України:

1. Гайдур Г. І., Гахов С. О., Гамза Д. Є. Модель виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації. *Сучасний захист інформації.* 2024. № 4(60). С. 30–38. https://doi.org/10.31673/2409-7292.2024.040003.

2. Гайдур Г. І., Гамза Д. Є. Гібридний метод виявлення шкідливої активності на основі стекінг-ансамблю класифікаторів. *Сучасний захист інформації.* 2025. № 3(63). С. 20–26. https://doi.org/10.31673/2409-7292.2025.030315.

3. Гамза, Д. (2025). Вплив оптимізації датасету CSE–CIC–IDS2018 на ефективність гібридної стекінгової моделі виявлення мережевих вторгнень. Електронне фахове наукове видання «*Кібербезпека: освіта, наука, техніка*», 2(30), С. 766–777. https://doi.org/10.28925/2663-4023.2025.30.963.

4. Савченко В.А., Смолєв Є.С., Гамза Д.Є., Методика виявлення аномалій взаємодії користувачів з інформаційними ресурсами організацій. *Сучасний захист інформації.* 2023. № 4. С. 6–12.

5. Волошко Д. С., Гамза Д. Є., Смолєв Є. С. Технологія виявлення простих вірусів у програмному коді. *Сучасний захист інформації.* 2023. № 2(54). С. 41–49.

Публікації за матеріалами науково-практичних конференцій:

1. Haydur, H., & Hamza, D. Hybrid method for malicious activity detection in information systems. *In Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World.* 2025. november 4-5. pp. 39–41.

2. Смолєв, Є. С., & Гамза, Д. Є. Метод оптимізації даних для тренування моделі виявлення вторгнень на основі SVM. *Цифрова трансформація кібербезпеки:* матеріали наук.-практ. конф. 2024. 26 квітня. С. 220–223. РВЦ ДУІКТ. https://duikt.edu.ua/uploads/n_12581_11703414.pdf .

3. Haydur, H., & Hamza, D., Zybin S. Multi-criteria selection of optimal hybrid stacking ensemble model for intrusion detection systems: pareto front and above-average rule filtering. *Цифрова трансформація кібербезпеки*: матеріали наук.-практ. конф. 2026. 29 квітня. С. 27-30. РВЦ ДУІКТ. https://duikt.edu.ua/uploads/p_3086_30075970.pdf.

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

Рецензент – ІВАНЧЕНКО Євгенія Вікторівна, доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надала позитивну рецензію без зауважень.

Рецензент – ЛЕГОМІНОВА Світлана Володимирівна, доктор економічних наук, професор, завідувач кафедри Управління кібербезпекою та захистом інформації Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надала позитивну рецензію без зауважень.

Опонент – СОБЧУК Валентин Володимирович, доктор технічних наук, професор, професор кафедри Інтегральних та диференціальних рівнянь механіко-математичного факультету Київського національного університету імені Тараса Шевченка надав позитивний відгук без зауважень.

Опонент – ДЕЛЕМБОВСЬКИЙ Максим Михайлович, кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури надав позитивний відгук без зауважень.

Голова ради – КАЗМІРЧУК Світлана Володимирівна, доктор технічних наук, професор, професор кафедри Систем та технологій кібербезпеки Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій надала позитивний відгук 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 Дмитру ГАМЗІ

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

ступінь доктора філософії з галузі знань 12 «Інформаційні технології»

(галузь знань)

за спеціальністю 125 «Кібербезпека»

(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

М.П.

(підпис)

Світлана КАЗМІРЧУК

(власне ім`я та прізвище)