ЗАТВЕРДЖУЮ
Перший проректор Державного університету інформаційно-комунікаційних технологій
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України в галузі науки і техніки,
Заслужений діяч науки і техніки України
_____ Олександр КОРЧЕНКО
"30" 04 2026 року

ВИСНОВОК

міжкафедрального семінару кафедри систем та технологій кібербезпеки інформації Державного університету інформаційно-комунікаційних технологій про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Гамзи Дмитра Євгенійовича на тему: "Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації", поданої на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Витяг
з протоколу № 8/2 засідання кафедри систем та технологій кібербезпеки
від "30" квітня 2026 року

Присутні: Головуючий на засіданні – директор Навчально-наукового інституту кібербезпеки та захисту інформації, д.т.н., професор Іванченко Євгенія Вікторівна.

- з кафедри Систем та технологій кібербезпеки:

завідувач кафедри – д.т.н., професор Гайдур Галина Іванівна;

професор кафедри – д.т.н., професор Зибін Сергій Вікторович;

професор кафедри – д.т.н., професор Казмірчук Світлана Володимирівна;

доцент кафедри – к.військ.н., доцент Гахов Сергій Олександрович;

доцент кафедри – к.т.н., доцент Борсуковський Юрій Володимирович;

доцент кафедри – к.т.н., доцент Власенко Вадим Олександрович;

доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації, доцент Марченко Віталій Вікторович;

доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Собчук Андрій Валентинович;

доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Педченко Євген Максимович;

старший викладач кафедри – Бойко Анна Олександрівна;
асистент кафедри – Шулімова Дар'я Денисівна

Запрошені:

з кафедри Управління кібербезпекою та захистом інформації:
завідувач кафедри – д.е.н., професор Легомінова Світлана Володимирівна;
професор кафедри – д.т.н., професор Савченко Віталій Анатолійович;
доцент кафедри – к.т.н., доцент Щавінський Юрій Віталійович;
доцент кафедри – доктор філософії за спеціальністю 125 Кібербезпека та захист інформації Запорожченко Михайло Михайлович

- *з кафедри Технічних систем кіберзахисту:*
завідувач кафедри – д.т.н., професор Туровський Олександр Леонідович;
- *з кафедри Інформаційних систем та технологій:*
завідувач кафедри – д.т.н., професор Сторчак Каміла Павлівна.

Всього присутніх – 18 осіб. Серед присутніх 8 докторів технічних наук та 8 кандидатів технічних наук.

ПОРЯДОК ДЕННИЙ:

Обговорення дисертаційної роботи аспіранта кафедри Систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій Гамзи Дмитра Євгенійовича на тему: "Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації", поданої на здобуття ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Дисертація виконана на кафедрі Систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій. Тема дисертаційної роботи затверджена в новій редакції та призначено наукового керівника доктора технічних наук, професора, професора кафедри систем та технологій кібербезпеки Зибіна Сергія Вікторовича на засіданні Вченої ради Державного університету інформаційно-комунікаційних технологій (протокол № 4 від 21.04.2026 року).

СЛУХАЛИ: доповідь про дисертаційну роботу Гамзи Дмитра Євгенійовича на тему "Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації", подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

Шановні Голово, члени міжкафедрального семінару, присутні! Вашій увазі представляється дисертаційна робота на тему «Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної

класифікації», виконана на здобуття наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека.

Науковий керівник – доктор технічних наук, професор Зибін Сергій Вікторович.

Дозвольте перейти до доповіді.

Сучасні організації щоденно стикаються зі зростанням складності та обсягів кіберзагроз. За даними звіту ENISA Threat Landscape за 2025 рік, в Європейському Союзі зафіксовано близько 4 900 верифікованих кіберінцидентів, при цьому 60% вторгнень починаються з фішингу, а понад 80% атак соціальної інженерії згенеровані з використанням штучного інтелекту.

Згідно з IBM Cost of a Data Breach Report 2024, середній час виявлення та стримування витоку даних становить 241 день – це критичний показник, який засвідчує неспроможність традиційних засобів захисту реагувати на сучасні загрози в реальному часі.

Існуючі підходи мають суттєві обмеження: сигнатурні методи неефективні проти атак нульового дня; аномальні методи генерують надмірну кількість хибних спрацювань; а моно-класифікатори машинного навчання мають обмежену узагальнюючу здатність.

Саме тому актуальною є розробка методу виявлення шкідливої активності на основі гібридної класифікації.

Аналіз стану досліджень показав результати робіт провідних світових та українських дослідників. Серед закордонних авторів варто відзначити Khraisat та співавторів з фундаментальним оглядом систем виявлення вторгнень, а також Karatas, Demir, Sahingoz з дослідженням ML-IDS на дисбалансованих датасетах – це безпосередньо перекликається з тематикою роботи. Фундаментальний теоретичний базис формують класичні роботи: Чавли, Джоліффа, Уолперта про SMOTE, PCA, стекінг-ансамблі. Серед українських науковців – Корченко О.Г. (робота про побудову систем захисту інформації на нечітких множинах); Савченка В.А., Гайдур Г.І., Гахова С.О., Марченко В.В. (цикл праць з кібербезпеки інформаційних систем організацій та виявлення шкідливих процесів).

Аналіз показав, що попри значний обсяг досліджень, невирішеним залишається питання гібридизації різнорідних методів для виявлення шкідливої активності в реальному часі. Саме це й визначило напрямок роботи.

Метою дисертаційного дослідження є підвищення точності виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації.

Об’єктом дослідження є процес виявлення шкідливої активності в інформаційних системах організацій.

Предметом дослідження є методи виявлення шкідливої активності в інформаційних системах організацій.

Аналіз наявних підходів дозволив виявити два протиріччя. Зовнішнє протиріччя – між необхідністю виявлення нових типів атак, таких як Zero-day у режимі реального часу, та статичною природою існуючих засобів захисту.

Внутрішнє протиріччя – між точністю детектування, яка вимагає складних ансамблевих моделей, та швидкістю прийняття рішень, що вимагає спрощення обчислень. Інтеграція цих протиріч формує наукове протиріччя – між зростаючою складністю шкідливої активності та обмеженими можливостями існуючих методів виявлення.

На основі цього сформульовано наукове завдання – розробка методів виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації.

Робота побудована за чіткою логікою: від проблематики – через мету – до методів – і до результатів. Проблематика – обмежена ефективність існуючих ML-IDS, зростання обсягу кіберзагроз, високий рівень хибних спрацювань. Мета – створити метод виявлення шкідливої активності на основі гібридної класифікації. Методи – стекінг-ансамблі, комплексна оптимізація даних, багатокритеріальний відбір. Результати – три наукові результати, які буде розглянуто далі.

Перед розробкою власного методу проведено системний аналіз існуючих підходів. Сигнатурні методи мають високі хибні спрацювання для нових атак. Аномальні ML-детектори генерують багато хибних спрацювань. Моно-методи машинного навчання (SVM, k-NN, Random Forest) мають низьку узагальнюючу здатність.

Серед ансамблевих підходів порівняно три ключові: Bagging забезпечує зниження дисперсії, але працює з однотипними моделями; Boosting дає високу точність, але чутливий до аномалій; Stacking об’єднує різнорідні моделі через мета-класифікатор. Саме стекінг-архітектуру обрано як найбільш перспективну для подальшого дослідження.

Відповідно до наукового завдання формалізовано математичне представлення завдання. Дано: навчальну вибірку D, де кожен зразок – це вектор ознак мережевого потоку та клас активності з K можливих класів. Базові класифікатори формують ймовірнісні передбачення; простір мета-ознак формується як конкатенація їхніх ймовірностей; мета-класифікатор обчислює фінальний розподіл через Softmax, а вирішальне правило обирає клас з максимальною ймовірністю.

Критеріями оптимізації є три показники одночасно: F1-міра → max як гармонічне середнє між Precision та Recall; Accuracy → max для загальної точності; та час прогнозу → min для роботи в реальному часі.

Принципова різниця між стандартним та гібридним методом класифікації полягає в наступному. Стандартний метод використовує один класифікатор, який обробляє вхідні дані та формує прогноз. Її обмеження – мала узагальнююча здатність на складних розподілах. Гібридний метод має дворівневу структуру: на першому рівні працюють кілька різнорідних базових класифікаторів; на другому рівні мета-класифікатор навчається на їхніх прогнозах і динамічно коригує помилки. Така архітектура забезпечує синергетичний ефект – кожен базовий алгоритм компенсує слабкі сторони інших.

Для верифікації методу проведено експериментальне дослідження. Тестовий набір даних – канадський датасет CSE-CIC-IDS2018, що містить 80 ознак та 7 класів атак: Benign, DoS, DDoS, Brute Force, Web Attack, Botnet, Infiltration. Поділ – 70% навчальна вибірка, 15% валідаційна, 15% тестова.

Узагальнені результати експериментального дослідження містять порівняння поодиноких класифікаторів та найкращих стекінг-ансамблів на оптимізованому датасеті. Гібридна модель XGBoost+CatBoost+LightGBM з мета-XGBoost досягла: Accuracy 98,07%; F1-score 96,57%; Час прогнозування 7,16 мс – це менше 10 мілісекунд, що відповідає вимогам реального часу. Перевага над моно-моделями (порівнюючи з їх середніми значеннями): +12,4% Accuracy, +4,88% F1-score, мінус 16% часу прогнозування.

Переходимо до другого наукового результату – удосконаленого методу комплексної оптимізації набору даних. Метод послідовно застосовує три компоненти. Перший – SMOTE – синтетичний оверсемплінг міноритарних класів, що усуває дисбаланс між класами атак (приблизно 85% безпечного трафіку проти 15% атак у вихідному датасеті). Другий – Min-Max нормалізація – приводить усі ознаки до діапазону від нуля до одиниці, що критично для методів, чутливих до масштабу. Третій – метод головних компонент PCA – знижує розмірність з 80 до 18 ознак, зберігаючи 95% дисперсії.

Синергетичний ефект полягає в тому, що кожен компонент окремо не дає такого результату: SMOTE без PCA – повільно; PCA без SMOTE – низька повнота на рідкісних класах атак. Лише послідовне застосування забезпечує одночасне покращення якості, збалансованості, розмірності та швидкодії.

Підсумовуючи ефект оптимізації, маємо три ключові показники: Accuracy зросла з 94,41% до 98,07% – приріст 3,87%; F1-score зріс з 91,87% до 96,57% – приріст 5,11%; Час прогнозування скоротився з 28,6 мс до 7,16 мс – зниження на 75%. Це підтверджує синергетичний ефект методу оптимізації разом зі стекінг-архітектурою.

Переходимо до третього наукового результату – методу багатокритеріального відбору оптимальних архітектур. Метод складається з двох послідовних етапів. Етап перший – фронт Парето. Будується множина недомінованих архітектур – таких, де покращення одного критерію неможливе без погіршення іншого. Критерії: Accuracy → max, F1-score → max, Час прогнозу → min. Етап другий – стратегія above-average rule. Обчислюються середні значення по 10 комбінаціях: середній Accuracy 0,9775, середній F1-score 0,9621, середній час прогнозу 7,281 мс. Лише одна комбінація перевершує середнє за всіма трьома критеріями одночасно.

На основі розроблених методів спроектовано п’ятимодульну архітектуру програмного рішення виявлення шкідливої активності. Модуль 1 – Збір даних – захоплення трафіку. Модуль 2 – Інженерія ознак – формування 80 статистичних, темпоральних і поведінкових ознак. Модуль 3 – Попередня обробка – застосування комплексного методу SMOTE + Min-Max + PCA. Модуль 4 – Гібридна класифікація – стекінг-ансамбль з мета-класифікатором XGBoost. Модуль 5 – Реагування – формування сповіщень та інтеграція через CEF, LEEF, REST API із SIEM-системами.

Програмне рішення підтримує роботу в режимі реального часу із затримкою менше 7,16 мс на потік, контейнеризацію через Docker та Kubernetes.

Розроблено практичні рекомендації щодо впровадження в чотири етапи. Етап 1 – Підготовка: аудит мережі, інвентаризація активів, збір трафіку протягом 2-4 тижнів. Етап 2 – Розгортання: контейнеризація через Docker та Kubernetes, налаштування SPAN-портів, інтеграція з SIEM. Етап 3 – Калібрування: налаштування порогів класифікації 0,65-0,75, формування часового вікна 5-10 секунд, робота в shadow mode 2-4 тижні. Етап 4 – Підтримка: перенавчання моделі кожні 2-4 тижні, моніторинг концепт-дрейфу, щоквартальний аудит.

Дозвольте підсумувати наукову новизну.

1. 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.

2. 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.

3. 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.

Результати дисертаційного дослідження опубліковано у 9 наукових працях, з яких 1 – у виданні, що індексується в Scopus, 3 – у фахових виданнях України, 2 – в інших виданнях України, а також 3 тези доповідей на наукових конференціях.

Доповідь закінчено. Дякую за увагу!

По завершенню доповіді Гамзі Дмитру Євгенійовичу присутніми були поставлені такі запитання:

1. Чому був обраний саме стекинг як мета-класифікатор у порівнянні з іншими підходами?

2. За якими параметрами проходила оптимізація моделі класифікації ?

3. Ваш метод тестувався на датасеті CSE-CIC-IDS2018. Як ви оцінюєте здатність моделі до узагальнення на реальний трафік організацій, який суттєво

відрізняється від синтетичного? Чи проводилось крос-валідаційне тестування на інших датасетах (NSL-KDD, UNSW-NB15)?

4. Застосування SMOTE створює синтетичні приклади міноритарних класів. Чи не призводить це до того, що модель навчається розпізнавати «штучні» атаки, яких не існує в реальній мережі? Як ви боролися з ризиком artefact learning?

5. Чи використовували ви cross-validation для оцінки результатів, чи робили лише одне розбиття 70/15/15?

6. PCA знижує розмірність з 80 до 18 ознак, зберігаючи 95% дисперсії. Однак PCA – лінійний метод, а атаки часто мають нелінійні залежності між ознаками. Чи розглядалися альтернативи (Autoencoder, t-SNE, UMAP) і чому PCA виявився оптимальним?

7. Як ви обробляли пропущені значення (missing values) у датасеті CSE-CIC-IDS2018? Адже відомо, що в ньому є проблеми з NaN та Infinity у деяких ознаках flow-based трафіку.

8. Час прогнозування 7,16 мс на потік – як саме вимірювалась ця затримка? Чи враховано в ній витрати на інженерію ознак, попередню обробку та формування рішення, чи це лише час inference моделі?

9. Шкідлива активність постійно еволюціонує. Ви згадуєте перенавчання моделі кожні 2-4 тижні – на чому базується саме така періодичність? Як виявляється момент, коли модель потребує перенавчання, і які метрики його тригерять?

10. Чи зберігається ефективність методу при роботі з потоковими даними на відміну від batch-режиму, в якому проводились ваші експерименти?

11. Стекінг-ансамбль із трьох градієнтних бустингів (XGBoost + CatBoost + LightGBM) – це по суті комбінація споріднених алгоритмів. Чи не суперечить це самій ідеї стекінгу, який передбачає об'єднання саме різнорідних моделей? Чи розглядалось додавання принципово інших алгоритмів (нейромережі, SVM)?

12. Розроблений метод орієнтований на класифікацію вже наявного трафіку. Як він поводиться з повністю невідомими атаками нульового дня, для яких не існує жодних прикладів у навчальній вибірці?

13. Як обиралась послідовність застосування SMOTE → Min-Max → PCA? Чому саме така послідовність, а не, наприклад, спочатку нормалізація, потім балансування?

14. Чи розглядалось використання глибокого навчання для виявлення шкідливої активності, і чому ви відмовилися від цього підходу на користь класичного ML?

На всі питання були дані вичерпні відповіді.

СЛУХАЛИ: відгук наукового керівника доктора технічних наук, професора, Зибіна Сергія Вікторовича про дисертаційну роботу аспіранта Гамзи Дмитра Євгенійовича на тему: “Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації”, подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

ЗИБІН С.В.: Дисертаційна робота Гамзи Дмитра Євгенійовича “Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації” виконана у межах плану науково-дослідних робіт Державного університету інформаційно-комунікаційних технологій МОН України за темами: “Методологія виявлення шкідливих процесів в інформаційних системах” (№ держ. реєстрації 0121U113613, ДУІКТ, м. Київ); “Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації” (ТОВ “АЛЬФА-МЕТАЛ”, м. Київ), в яких автором розроблено метод обробки даних для виявлення шкідливих процесів в інформаційній системі організації, обґрунтовано архітектуру гібридного класифікатора на основі стекінг-ансамблю різнорідних алгоритмів машинного навчання, а також сформульовано рекомендації щодо створення програмної реалізації системи виявлення шкідливих процесів та її інтеграції із сучасними засобами моніторингу інформаційної безпеки.

У процесі підготовки дисертації Дмитро Гамза проявив себе як самостійний, наполегливий, відповідальний і високоерудований науковець, здатний формулювати та ефективно вирішувати складні наукові завдання. Він володіє сучасними методами наукових досліджень, аналітичними підходами, а також комунікаційними та іншими професійними компетентностями, що дозволяють йому логічно і послідовно представляти результати власних досліджень, публікувати їх у вітчизняних та міжнародних наукових виданнях, брати участь у наукових дискусіях, демонструючи вміння аргументовано обґрунтовувати та відстоювати власні наукові досягнення.

Автором дослідження коректно визначено мету, завдання, об’єкт і предмет дослідження. У процесі виконання дисертаційної роботи ефективно застосовано методи машинного навчання та ансамблевого навчання (стекінг-архітектура з мета-класифікатором XGBoost), методи попередньої обробки даних (SMOTE, Min-Max нормалізація, метод головних компонент PCA), методи багатокритеріальної оптимізації (фронт Парето, стратегія above-average rule), а також методи статистичного аналізу та експериментального дослідження для досягнення поставленого наукового завдання. Такий підхід забезпечив не лише формулювання та теоретичне обґрунтування наукової новизни отриманих результатів, а й їх практичну реалізацію, що визначило значущість дослідження для розв’язання проблеми виявлення шкідливої активності в корпоративних інформаційних системах у режимі реального часу.

У ході виконання дисертаційної роботи автором досягнуто мети роботи – підвищення точності виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації. Експериментально підтверджено, що запропонований метод дозволяє підвищити точність виявлення шкідливої активності до 98,07%, F1-міру до 96,57%, скоротити час прогнозування до 7,16 мс на потік, а також знизити рівень хибнопозитивних спрацювань на 20–35% і скоротити середній час виявлення інцидентів (MTTD) на 40–60%. Отримані результати мають важливе практичне значення для фахівців у сфері кібербезпеки, побудови корпоративних SOC-центрів, систем виявлення

вторгнень (IDS/IPS) та їх інтеграції з SIEM-рішеннями, а також можуть бути використані в навчальних програмах підготовки фахівців із кібербезпеки.

За результатами дисертаційних досліджень опубліковано 9 наукових праць. Основні наукові результати викладені в 6 наукових статтях, серед яких 1 опублікована у наукових виданнях, які індексуються в міжнародних наукометричних базах Scopus та Web of Science, 3 опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України, 2 опубліковані в інших виданнях. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 3 збірниках тез доповідей.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. З наукових праць, які опубліковані у співавторстві, використано лише ті положення, ідеї та висновки, які є результатом власного дослідження здобувача, зокрема: метод виявлення шкідливої активності на основі гібридної класифікації; метод комплексної оптимізації набору даних, що поєднує SMOTE, Min-Max нормалізацію та PCA; метод багатокритеріального відбору оптимальних архітектур ансамблевого навчання на основі фронту Парето та стратегії above-average rule; програмне рішення з п’ятимодульною архітектурою для конвеєрної обробки мережевого трафіку; практичні рекомендації щодо впровадження розробленого рішення в існуючу інфраструктуру організації.

Робота є самостійно виконаним науковим дослідженням, що відповідає принципам академічної доброчесності та не містить некоректних запозичень. Вона повністю відповідає спеціальності 125 Кібербезпека, за якою подається до захисту.

Дисертаційна робота Гамзи Дмитра Євгенійовича є завершеним науковим дослідженням, яке здійснює вагомий внесок у розвиток теоретичних і прикладних аспектів інформаційної безпеки, зокрема у сфері виявлення шкідливої активності в корпоративних інформаційних системах із застосуванням методів машинного навчання та ансамблевих архітектур. Запропоновані автором науково-методичні підходи сприяють удосконаленню механізмів виявлення кіберзагроз у режимі реального часу, підвищенню точності класифікації шкідливих процесів та забезпеченню стійкості організацій до сучасних багатовекторних атак, у тому числі атак нульового дня. Дослідження виконане на високому науковому рівні, підтверджує наукову зрілість, ґрунтовну підготовку та високу компетентність здобувача в галузі кібербезпеки.

Вважаю, що дисертаційна робота повністю готова до захисту, а її автор заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Призначені рецензенти:

Д.т.н, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації Іванченко Євгенія Вікторівна та д.е.н., професор, завідувач кафедри управління кібербезпекою та захистом інформації Легомінова Світлана Володимирівна загалом позитивно оцінили дисертаційну роботу, відзначивши

її високу актуальність, теоретичну значущість та практичну цінність. Особливу увагу було приділено науковій новизні, обґрунтованості результатів і систематизованому підходу до вирішення поставленої проблеми.

Зокрема, **доктор економічних наук, професор, завідувач кафедри управління кібербезпекою та захистом інформації Легомінова Світлана Володимирівна** відзначила високий науковий рівень дисертаційної роботи Гамзи Дмитра Євгенійовича та її актуальність у контексті сучасних викликів кібербезпеки. Актуальність дослідження підтверджується проведеним аналізом сучасних кіберзагроз та обмежень існуючих систем виявлення шкідливої активності. У зв'язку з цим особливої актуальності набуває застосування гібридних методів машинного навчання, які поєднують переваги різних алгоритмів класифікації, поведінкового аналізу та інтелектуальної обробки даних. Використання таких підходів дозволяє підвищити точність виявлення аномалій, знизити рівень хибнопозитивних спрацювань та забезпечити адаптивність систем виявлення вторгнень до нових типів кіберзагроз.

Загальний аналіз дисертації дозволив зробити наступні висновки:

1. Ознайомлення зі змістом дисертаційної роботи підтверджує логічність її побудови, чіткість наукової аргументації, а також обґрунтованість висновків і рекомендацій, сформульованих автором самостійно.
2. Структура роботи відповідає визначеній меті та поставленому науковому завданню. Дисертація ґрунтується на положеннях теорії інформаційної безпеки, методів машинного навчання та ансамблевого навчання, теорії ймовірностей, методів багатокритеріальної оптимізації та математичного моделювання, що забезпечує її теоретичну глибину.
3. Автором сформульовано оригінальні наукові положення, що стосуються гібридної класифікації шкідливої активності на основі стекінг-архітектури, комплексної оптимізації набору даних для попередньої обробки та багатокритеріального відбору оптимальних архітектур ансамблевого навчання. Отримані результати мають значний практичний потенціал для підвищення кіберстійкості організацій та удосконалення корпоративних систем виявлення вторгнень.
4. Дисертаційна робота є самостійною науковою працею, що не містить некоректних запозичень. Опубліковані результати досліджень відображають основні положення наукової новизни та відповідають вимогам до дисертацій за спеціальністю 125 Кібербезпека.

Позитивно оцінюючи положення дисертаційного дослідження Гамзи Д.Є., Легомінова С.В. звернула увагу на певні аспекти, що можуть бути уточнені або розширені:

1. У роботі основну увагу приділено технічній реалізації методу гібридної класифікації на основі стекінг-архітектури, однак було б доцільно детальніше розглянути організаційно-управлінські аспекти впровадження запропонованого рішення в систему управління інформаційною безпекою організації, зокрема інтеграцію з процесами SIEM/SOC, а також узгодження з вимогами стандартів ISO/IEC 27001, NIST Cybersecurity Framework та національних нормативних актів у сфері кібербезпеки.

2. Дослідження проведено переважно на датасеті CSE-CIC-IDS2018, що є визнаним академічним стандартом, проте варто було б розширити експериментальну апробацію за рахунок реальних даних з інформаційних систем різних типів організацій (фінансовий сектор, державні установи, об'єкти критичної інфраструктури), оскільки специфіка мережевого трафіку та профілі загроз у них можуть суттєво відрізнятися від синтетичного датасету.

3. Дисертаційна робота має значний прикладний потенціал, проте було б корисно детальніше проаналізувати вартість впровадження розробленого програмного рішення та вимоги до апаратних ресурсів для організацій різного масштабу – від підприємств малого та середнього бізнесу до великих корпоративних мереж із високошвидкісним трафіком.

Наведені зауваження стосуються переважно питань подальшого розвитку дослідження та не впливають на його загальну наукову та практичну значущість. Робота є завершеним дослідженням, що робить вагомий внесок у розвиток методів виявлення шкідливої активності та підвищення рівня кібербезпеки корпоративних інформаційних систем. За рівнем наукової аргументації, методологічного підходу та практичної значущості висновків, дисертація відповідає вимогам, які висуваються до досліджень на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека. Робота виконана державною мовою, з дотриманням норм та правил академічної доброчесності.

Доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації Іванченко Євгенія Вікторівна охарактеризувала дисертаційну роботу як ґрунтовне наукове дослідження високого рівня, що відображає актуальні виклики у сфері кібербезпеки, зокрема проблему виявлення шкідливої активності в корпоративних інформаційних системах у режимі реального часу. Робота містить чітке теоретичне обґрунтування, новітні підходи до гібридизації методів машинного навчання та практичні рекомендації щодо їх впровадження. Наукові результати дослідження мають важливе значення для подальшого розвитку систем виявлення вторгнень (IDS/IPS) та практичного застосування в кіберзахисті організацій різного рівня.

Разом із позитивною оцінкою дисертації, рецензент висловив окремі зауваження та наголосив на деяких аспектах, що можуть бути предметом подальшого дослідження:

1. Запропонований метод гібридної класифікації демонструє високу точність на стандартних класах атак, представлених у датасеті CSE-CIC-IDS2018, однак доцільно було б додатково дослідити його стійкість до adversarial-атак, коли зловмисник цілеспрямовано модифікує параметри мережевого трафіку для обходу ML-детектора, а також розглянути потенційні ризики атак типу data poisoning на етапі перенавчання моделі.

2. У роботі передбачено періодичне перенавчання моделі (кожні 2-4 тижні) як механізм боротьби з концепт-дрейфом, проте варто було б глибше дослідити автоматичні механізми виявлення моменту, коли модель потребує

перенавчання, на основі моніторингу метрик якості, а також оцінити вплив частоти перенавчання на загальну продуктивність та стабільність системи.

3. Робота орієнтована на класифікацію мережевого трафіку за flow-based ознаками, отриманими з відкритих заголовків пакетів, проте недостатньо розкрито питання роботи методу в умовах зашифрованого трафіку (TLS 1.3, QUIC), частка якого в сучасних корпоративних мережах сягає 90% і більше. Доцільно було б розглянути можливості інтеграції методів аналізу зашифрованого трафіку без розшифровування (Encrypted Traffic Analysis) у запропоновану архітектуру.

Загалом, рецензована робота підготовлена на високому науковому рівні, вирізняється системністю, новизною та практичною цінністю отриманих результатів, виконана з дотриманням норм та правил академічної доброчесності. Це дає підстави оцінити її позитивно та рекомендувати до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензентами відзначено, що дисертаційна робота відповідає встановленим вимогам щодо наукової новизни, теоретичної та практичної значущості, а також може бути рекомендована до Вченої Ради Державного університету інформаційно-комунікаційних технологій щодо затвердження складу разової спеціалізованої вченої ради про присудження ступеня доктора філософі.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертаційної роботи Гамзи Дмитра Євгенійовича на тему “Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації”, поданої на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека

Актуальність теми дослідження. Сучасні інформаційні системи є ключовим елементом цифрової інфраструктури організацій, забезпечуючи управління даними, підтримку бізнес-процесів та захищену комунікацію. Водночас, зростаюча складність цифрових екосистем створює нові виклики у сфері кібербезпеки, серед яких цілеспрямована шкідлива мережева активність займає провідне місце. Сучасні кібератаки використовують передові технології обходу традиційних засобів захисту, що дозволяє зловмисникам отримувати несанкціонований доступ до критичної інформації та управлінських функцій організації.

Шкідлива активність (сканування, флуд-атаки, активність ботнетів, інсайдерські загрози, експлуатація вразливостей) має значний руйнівний потенціал, оскільки може призводити до тривалого порушення роботи сервісів, витоку даних, фінансових втрат, порушення цілісності інформації та репутаційних ризиків. У зв'язку з цим виникає потреба у розробці методів, що дозволяють з високою точністю класифікувати загрози в реальному часі, ідентифікувати аномалії на ранніх етапах та ефективно відфільтровувати легітимний трафік від шкідливого.

Незважаючи на зростаючу увагу наукової спільноти до проблематики виявлення вторгнень, існуючі моделі мають суттєві обмеження. Сигнатурні методи ефективно виявляють відомі атаки, проте є неефективними проти атак нульового дня та поліморфних загроз. Аномальні методи детектування генерують надмірну кількість хибнопозитивних спрацювань, що ускладнює роботу SOC-аналітиків. Моно-моделі машинного навчання мають обмежену узагальнюючу здатність та не забезпечують одночасно високу точність класифікації та необхідну швидкість обробки великих обсягів трафіку. Найбільш перспективними у вирішенні цієї проблеми є підходи на основі ансамблевого навчання та градієнтного бустингу, проте їх необхідно удосконалити шляхом гібридизації різнорідних алгоритмів та комплексної оптимізації ознакового простору для підвищення точності класифікації при одночасному зниженні кількості хибних спрацювань у динамічних умовах корпоративного середовища.

Враховуючи виявлені обмеження, у дисертаційній роботі вирішується актуальне наукове завдання, що полягає у розробці методів виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації. Запропонований підхід дозволяє підвищити точність виявлення шкідливої активності, знизити рівень хибнопозитивних спрацювань та забезпечити роботу системи в режимі реального часу, що сприяє підвищенню рівня кіберстійкості організацій.

Зв'язок роботи з науковими програмами, планами, темами, грантами.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Державного університету інформаційно-комунікаційних технологій в рамках науково-дослідних робіт «Методологія виявлення шкідливих процесів в інформаційних системах» (№ держ. реєстрації 0121U113613, ДУІКТ, м. Київ) та «Розробка науково-методичних рекомендацій виявлення шкідливих процесів в інформаційній системі організації» (ТОВ «АЛЬФА-МЕТАЛ», м. Київ). Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією Законів України «Про основні засади забезпечення кібербезпеки України» та «Про захист інформації в інформаційно-комунікаційних системах».

Мета і завдання дослідження.

Метою дослідження є підвищення точності виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації.

Для досягнення поставленої мети автором виконано наступні *окремі завдання дослідження*:

проаналізовано існуючі методи та підходи до виявлення шкідливої активності в інформаційній системі організації;

розроблено гібридний метод виявлення шкідливої активності, визначено його архітектуру, специфікацію компонентів та обґрунтовано вибір мета-класифікаторів.

розроблено метод попередньої обробки даних для виявлення шкідливої активності на основі гібридної класифікації в інформаційних системах організацій з метою зниження обчислювального навантаження та підвищення точності виявлення.

розроблено метод багатокритеріального відбору оптимальних архітектур ансамблевого навчання для виявлення шкідливих процесів у реальному часі.

проведено експериментальне дослідження розробленого методу виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації.

розроблено рекомендації щодо створення та впровадження програмного рішення на базі розробленого методу виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації**.**

Об'єкт дослідження – процес виявлення шкідливої активності в інформаційних системах організацій.

Предмет дослідження – методи виявлення шкідливої активності в інформаційних системах організацій.

Методи дослідження.

Дослідження проведено на основі системного підходу із застосуванням: методів машинного навчання та ансамблевого навчання (стекінг-архітектура); методів попередньої обробки даних (SMOTE, Min-Max нормалізація, метод головних компонент PCA); методів багатокритеріальної оптимізації (фронт

Парето, стратегія above-average rule); методів статистичного аналізу та експериментального дослідження.

Наукова новизна дослідження:

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 можливіст ю 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.

Практичне значення одержаних результатів. 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 здісненні 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 реального часу.

Результати наукових досліджень прийняті до впровадження в діяльність ТОВ «ЄВРОТЕЛЕКОМ» та ТОВ «АРВІОМ», а також реалізовані в освітньому процесі кафедри систем та технологій кібербезпеки Державного університету інформаційно-комунікаційних технологій.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлені власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

Основні наукові та прикладні результати дисертаційної роботи, що виносяться на захист, отримані автором особисто. У роботах, опублікованих у співавторстві, автором: розроблено метод гібридної класифікації на основі стекінг-архітектури, що інтегрує прогнози різнорідних алгоритмів машинного навчання через мета-класифікатор для підвищення точності виявлення шкідливої активності; розроблено комплексний метод оптимізації набору даних для гібридного класифікатора, який поєднує балансування класів (SMOTE), Min-Max нормалізацію та зниження розмірності методом PCA; удосконалено метод багатокритеріального відбору оптимальних архітектур ансамблевого навчання на основі послідовного застосування стратегії above-average rule та побудови фронту Парето; розроблено програмне рішення з п'ятимодульною архітектурою, яке може бути інтегровано у сучасні системи моніторингу безпеки; розроблено практичні рекомендації щодо впровадження рішення в існуючу інфраструктуру організації.

Апробація результатів дослідження.

Основні теоретичні та практичні результати були представлені та обговорені в ході низки наукових конференцій (міжнародних – 1, всеукраїнських – 2):

Всеукраїнська науково-практична конференція «Цифрова трансформація кібербезпеки» (26 квітня 2025 року);

The International Scientific and Practical Conference «Digital Transformation: Strengthening the Cybersecurity Capacities in the Modern World» (November 4–5, 2025);

Всеукраїнська науково-практична конференція «Цифрова трансформація кібербезпеки» (29 квітня 2026 року).

Публікації. За результатами дисертаційних досліджень опубліковано 9 наукових праць. Основні наукові результати викладені в 6 наукових статтях, серед яких 1 опублікована у наукових виданнях, які індексуються в міжнародних наукометричних базах Scopus та Web of Science, 3 опубліковані у спеціалізованих фахових виданнях, затверджених наказом МОН України, 2 опубліковані в інших виданнях. Матеріали виступів на наукових та науково-практичних конференціях опубліковано у 3 збірниках тез доповідей.

Список опублікованих праць за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

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. 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 .

3. 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.

4. 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), 766–777. https://doi.org/10.28925/2663-4023.2025.30.963.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

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

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

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

Наукові праці, які додатково відображають наукові результати дисертації:

1. Савченко В. А., Смолєв Є. С., Гамза Д. Є. Методика виявлення аномалій взаємодії користувачів з інформаційними ресурсами організації. *Сучасний захист інформації*. 2023. № 4. С. 6–12. https://doi.org/10.31673/2409-7292.2023.030101.

2. 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. https://doi.org/10.31673/2409-7292.2023.020006.

Структура та обсяг дисертації.

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел. Загальний обсяг роботи відповідає вимогам, які висуваються до дисертацій на здобуття ступеня доктора філософії.

Характеристика особистості здобувача.

Гамза Дмитро Євгенович у 2017 році закінчив Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського» та отримав диплом Спеціаліста за спеціальністю 172 «Телекомунікаційні системи та мережі». У 2022 році вступив до аспірантури Державного університету телекомунікацій за спеціальністю 125 Кібербезпека. 21 квітня 2026 року на засіданні Вченої Ради Державного університету інформаційно-комунікаційних

технологій було затверджено у новій редакції тему дисертаційної роботи Гамзи Д.Є. “ Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації ”.

Під час виконання дисертаційної роботи Гамза Д.Є. провів ґрунтовне дослідження, спрямоване на аналіз сучасного стану проблематики, заявленої у дисертації. Було чітко визначено об’єкт, предмет, мету та завдання дослідження, обґрунтовано актуальність теми та обрано відповідні методи для досягнення поставлених цілей. Здобувач Дмитро Гамза приймав безпосередню участь під час постановки наукових завдань, планування та виконання експериментів, а також обговорення отриманих результатів. Проявив себе як відповідальний, дисциплінований та ініціативний дослідник, здатний працювати як самостійно, так і в команді. Продемонстрував високий рівень теоретичної підготовки, володіє сучасними методами дослідження, аналітичними інструментами та практичними навичками. Системно підходить до вирішення наукових завдань, критично оцінює результати власної роботи, виявляє наполегливість у досягненні поставлених цілей. Постійно вдосконалює свої знання, прагнучи підвищити рівень наукової обґрунтованості та практичної значущості отриманих результатів.

Оцінка мови та стилю дисертації. Дисертація виконана фаховою українською мовою, текстове подання матеріалу відповідає стилю науково-дослідної літератури.

Рецензенти рекомендують: відповідно до **п.15** 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, ***пропонується такий склад разової ради:***

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.

Рецензенти:

Іванченко Євгенія Вікторівна, доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

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.

Офіційні опоненти:

Собчук Валентин Володимирович, доктор технічних наук, професор, професор кафедри Інтегральних та диференціальних рівнянь механіко-математичного факультету Київського національного університету імені Тараса Шевченка.

Делембовський Максим Михайлович, кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

У результаті попередньої експертизи дисертації **Гамзи Дмитра Євгенійовича** і повноти публікації основних результатів дослідження

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Гамзи Дмитра Євгенійовича на тему "Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації".

2. Констатувати, що за актуальністю, степенем наукової новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Гамзи Д.Є. відповідає спеціальності 125 Кібербезпека 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.

3. Рекомендувати дисертацію Гамзи Д.Є на тему " Методи виявлення шкідливої активності в інформаційній системі організації на основі гібридної класифікації" до захисту на здобуття ступеня доктора філософії у разовій спеціалізованій вченій раді за спеціальністю 125 Кібербезпека.

4. Рекомендувати вченій раді Державного університету інформаційно-комунікаційних технологій затвердити склад разової спеціалізованої вченої ради:

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.

Рецензенти:

Іванченко Євгенія Вікторівна, доктор технічних наук, професор, директор Навчально-наукового інституту кібербезпеки та захисту інформації Державного університету інформаційно-комунікаційних технологій.

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.

Офіційні опоненти:

Собчук Валентин Володимирович, доктор технічних наук, професор, професор кафедри Інтегральних та диференціальних рівнянь механіко-математичного факультету Київського національного університету імені Тараса Шевченка.

Делембовський Максим Михайлович, кандидат технічних наук, доцент, завідувач кафедри Кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва та архітектури.

Результати голосування щодо рекомендації до захисту дисертації Гамзи Дмитра Євгенійовича:

"За" – 18

"Проти" – немає

"Утримались" – немає

Додаток: Презентація Гамзи Дмитра Євгенійовича на 20 стор.

Головуючий на засіданні –
д.т.н., професор, директор
Навчально-наукового інституту
кібербезпеки та захисту інформації Євгенія ІВАНЧЕНКО

Секретар засідання Дар'я ШУЛІМОВА