

ЗАТВЕРДЖУЮ



Президент Національного університету
«Київський авіаційний інститут»

Ксенія СЕМЕНОВА

24 » травня 2026 року

ВИСНОВОК

**Національного університету «Київський авіаційний інститут» (далі – КАІ)
про наукову новизну, теоретичне та практичне значення результатів
дисертації Юдіної Діани Олексіївни на тему «Методи та моделі оцінювання
стану кіберзахисту об'єктів критичної інформаційної інфраструктури»,
поданої на здобуття ступеня доктора філософії за спеціальністю
122 «Комп'ютерні науки»**

Витяг

із протоколу № 4 розширеного засідання
кафедри комп'ютерних інформаційних технологій КАІ
від 27 травня 2026 року

**Присутні на засіданні науково-педагогічні працівники кафедри
комп'ютерних інформаційних технологій:**

Головуючий на засіданні – Савченко Аліна Станіславівна, д.т.н, проф.,
завідувач кафедри;

Віноградов Микола Анатолійович, д.т.н., проф., професор кафедри;

Воронін Альбер Миколайович, д.т.н., проф., професор кафедри;

Райчев Ігор Едуардович, к.т.н., доц., доцент кафедри;

Климова Асія Сабірівна, к.т.н., доц., доцент кафедри;

Чуба Ірина Вікторівна, к.т.н., доц., доцент кафедри;

Колісник Олена Василівна, к.т.н., доц., доцент кафедри;

Зудов Олег Миколайович, к.т.н., доцент кафедри;

Прокопенко Костянтин Ігорович, к.т.н., доц., доцент кафедри;

Толстікова Олена Володимирівна, к.т.н., доц., доцент кафедри;

Сидоренко Вікторія Миколаївна, к.т.н., доц., доцент кафедри;

Положенцев Артем Анатолійович, PhD, доцент кафедри.

Присутні на засіданні науково-педагогічні працівники КАІ:

Нечипорук Олена Петрівна, д.т.н., проф., завідувач кафедри
інтелектуальних кібернетичних систем;

Гнатюк Сергій Олександрович, д.т.н., проф., проректор з наукових досліджень та трансферу технологій;

Ахрамович Володимир Миколайович, д.т.н., проф., професор кафедри кібербезпеки КАІ.

Ільєнко Анна Вадимівна, к.т.н., доц., завідувач кафедри кібербезпеки КАІ.

Одарченко Роман Сергійович, д.т.н., проф., декан факультету аеронавігації, електроніки та телекомунікацій КАІ;

Охріменко Тетяна Олександрівна, к.т.н., ст. дослідник, заступник декана Факультету комп'ютерних наук та технологій;

Фесенко Андрій Олексійович, к.т.н., доцент, декан Факультету комп'ютерних наук та технологій.

Порядок денний:

Обговорення дисертаційного дослідження аспірантки кафедри комп'ютерних інформаційних технологій КАІ Юдіної Діани Олексіївни на тему «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп'ютерні науки».

Науковий керівник – д.т.н., професор, проректор з наукових досліджень та трансферу технологій КАІ Гнатюк Сергій Олександрович.

Дисертація виконувалася на кафедрі комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ. Тема дисертації затверджена на засіданні Вченої ради Факультету кібербезпеки, комп'ютерної та програмної інженерії КАІ (протокол № 9 від 28 листопада 2022 року).

Виступили:

Здобувачка Юдіна Діана Олексіївна представила результати свого дослідження, обґрунтувавши актуальність обраної теми, мету, завдання, методи дослідження, охарактеризувавши об'єкт та предмет дисертаційного дослідження, виклала основні наукові положення та висновки, що виносяться на захист, вказала науково-практичну значимість роботи, зазначила про впровадження результатів дослідження.

Дисертаційна робота присвячена дослідженню моделей та методів оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури, а саме моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури, математичної моделі нечіткої інтерпретації стану кіберзахисту об'єктів критичної інформаційної інфраструктури, методу оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури.

Актуальність дослідження зумовлена необхідністю підвищення об'єктивності, точності та оперативності оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури (ОКІІ) в умовах динамічних змін ландшафту загроз та оновлення нормативно-правової бази України. Здобувачем запропоновано комплексний підхід до оцінювання стану кіберзахисту, який поєднує моделювання структурно-функціональних

характеристик об'єкта, удосконалений метод агрегування показників та модель нечіткої інтерпретації результатів.

Представлено математичну модель оцінювання стану кіберзахисту ОКІІ, яка базується на ієрархічній системі показників, декомпонованих за 7 функціональними системами критеріїв, що відображає взаємозв'язок між технічними заходами захисту, організаційними процесами та галузевою специфікою об'єкта.

У межах дослідження удосконалено метод розрахунку інтегрального показника стану кіберзахисту ОКІІ, що дозволяє адаптивно визначати вагові коефіцієнти критеріїв залежно від категорії критичності об'єкта. Запропоновані рішення сприяють усуненню «ефекту компенсації» слабких ланок захисту та забезпечують розширення теоретичної бази моделі на 85,8% для всіх 24 секторів критичної інфраструктури через впровадження коефіцієнта структурного розширення.

Розроблено математичну модель нечіткої інтерпретації результатів оцінювання, яка забезпечує інтелектуальну трансформацію числового показника у якісну лінгвістичну оцінку. Модель орієнтована на підвищення достовірності висновків у «сірих зонах» на межах рівнів захищеності та подолання суб'єктивізму експертних суджень. Оперативність та точність оцінювання забезпечуються використанням апарату нечітких чисел LR-типу трапецієподібної форми, що дозволяє розраховувати індекс впевненості та ідентифікувати перехідні стани системи. Для забезпечення динамічної інтерпретації застосовано процедури формування асоціативних правил, які дозволяють у реальному часі знаходити найбільш імовірні відповідності еталонним рівням захищеності.

Для перевірки ефективності запропонованого підходу була проведена апробація розробленого авторського програмного комплексу безпосередньо на базі реального функціонуючого ОКІІ паливно-енергетичного сектору. Це дозволило підтвердити адекватність розроблених моделей та методу в умовах реальної експлуатації, враховуючи фактичну конфігурацію систем захисту, актуальні кіберзагрози та реальну зрілість управлінських процесів підприємства.

Практичні та теоретичні результати дисертації, а також результати експериментальних досліджень впроваджені і використовуються у науково-дослідній діяльності НДІЛ протидії кіберзагрозам в авіаційній галузі Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» (акт впровадження від 25.03.2026), у діяльності групи реагування на інциденти комп'ютерної безпеки Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації (акт впровадження від 16.03.2026), а також у діяльності Адміністрації Державної служби спеціального зв'язку та захисту інформації України (акт впровадження від 12.03.2026).

У процесі моделювання враховувались такі параметри: кількість та склад базових і галузевих показників; вагомість систем критеріїв; показники узгодженості експертних думок; параметри еталонних функцій належності.

Застосування розроблених методу та моделей дозволяє забезпечити високу точність оцінювання (інтегральний показник на рівні 0,558 для досліджуваного об'єкта), усунути методологічні прогалини універсальних стандартів, а також збільшити оперативність прийняття рішень щодо кіберзахисту ОКІІ в середньому на 42,2% завдяки впровадженню алгоритмізованих процедур методу аналізу ієрархій та нечіткої логіки.

Після закінчення презентації Юдіною Д.О. присутніми на захисті фахівцями були поставлені наступні запитання:

Запитання до здобувачки:

1. **ОХРІМЕНКО Т.О.**, к.т.н., ст. дослідник, заступник декана Факультету комп'ютерних наук та технологій КАІ.

Запитання: У чому полягає відмінність між Вашим «методом оцінювання» та «моделлю структурно-функціональних характеристик»?

Відповідь: Дякую за запитання. Модель – це математична структура, що описує об'єкт через ієрархію 111 показників та їхні взаємозв'язки. Метод – це алгоритмічна послідовність дій, яка визначає, як саме ці дані збираються, агрегуються за допомогою методу аналізу ієрархій та передаються до іншої моделі для інтерпретації. Тобто модель – це «що» ми оцінюємо, а метод — «як» функціонує вся система оцінювання.

2. **АХРАМОВИЧ В.М.**, д.т.н., проф., професор кафедри кібербезпеки КАІ.

Запитання: Як саме було удосконалено математичну модель нечіткої інтерпретації?

Відповідь: Дякую за запитання. Удосконалення полягає у переході від детермінованих інтервалів до трапецієподібних нечітких чисел LR-типу. Це дозволило формалізувати модальні значення (ядра) та зони перетину станів. Введено новий параметр – індекс впевненості (ЕСІ), який дозволяє кількісно оцінити ступінь належності об'єкта до суміжних рівнів у «сірих зонах», чого не дозволяли класичні моделі лінгвістичного оцінювання.

3. **ФЕСЕНКО А.О.**, к.т.н., доцент, декан Факультету комп'ютерних наук та технологій КАІ.

Запитання: Розкажіть докладніше про процедуру формування якісних висновків. Де вона реалізована?

Відповідь: Дякую за запитання. Дана процедура є частиною практичної цінності роботи та реалізована у програмному комплексі. Вона базується на векторі ступенів належності: алгоритм аналізує розраховані значення ЕСІ та, згідно з розробленими асоціативними правилами, автоматично генерує лінгвістичний висновок. Якщо об'єкт потрапляє в зону перетину, процедура ідентифікує стан як «нестабільний» і вказує вектор трансформації.

Запитання: Як Ви обґрунтували вибір 7 систем критеріїв? Чи є ця структура повною з точки зору теорії систем?

Відповідь: Дякую за запитання. Вибір базується на функціональній повноті фреймворку NIST CSF 2.0 (Govern, Identify, Protect, Detect, Respond, Recover). Ці 6 функцій та 7-ма додаткова «Секторальна складова» покривають

повний життєвий цикл управління кібербезпекою, що відповідає принципам системного підходу.

5. СИДОРЕНКО В.М., к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Ви згадували методику у практичній цінності. Чим вона відрізняється від методу?

Відповідь: Дякую за запитання. Метод – це наукове обґрунтування послідовності обробки інформації. Методика – це вже прикладний інженерний алгоритм, покрокова інструкція для персоналу ОКІІ. Вона описує конкретні етапи: від використання мого програмного забезпечення до отримання фінального звіту згідно з вимогами законодавства.

6. ІЛЬЄНКО А.В., к.т.н., доц., завідувач кафедри кібербезпеки КАІ.

Запитання: Як використання нечіткої логіки дозволило усунути «ефект компенсації» у результатах оцінювання?

Відповідь: Дякую за запитання. Замість простого додавання балів, де високий показник однієї системи приховує провал іншої, нечітка модель аналізує ступені належності. Це дозволяє ідентифікувати слабкі ланки як критичні фактори, що переводять загальний стан у зону «нестабільності», навіть при високих середніх значеннях.

7. ОХРІМЕНКО Т.О., к.т.н., ст. дослідник, заступник декана Факультету комп'ютерних наук та технологій.

Запитання: З точки зору архітектури ПЗ, як Ваша система обробляє виняткові ситуації, наприклад, при введенні суперечливих даних експертом?

Відповідь: Дякую за запитання. В архітектуру ПЗ впроваджено валідатор вхідних даних у реальному часі. Якщо введений масив парних порівнянь призводить до порушення транзитивності, система блокує розрахунок і підсвічує «конфліктну зону». Це реалізовано через перевірку власного значення матриці, що дозволяє уникнути логічних помилок на ранніх етапах обробки даних.

Запитання: Яке призначення коефіцієнта структурного розширення у Вашій першій моделі?

Відповідь: Дякую за запитання. Коефіцієнт – це розроблений математичний інструмент для адаптації універсальної моделі до галузевих особливостей. Він дозволяє кількісно оцінити, наскільки додавання специфічних галузевих критеріїв підвищує аналітичну здатність моделі. Для 24 секторів критичної інфраструктури це забезпечило розширення теоретичної бази на 85,8%.

8. САВЧЕНКО А.С., д.т.н., проф., завідувач кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Поясніть логічну повноту Вашої системи нечіткого виводу. Чи існують значення показника x , для яких неможливо сформулювати висновок?

Відповідь: Дякую за запитання. Логічна повнота забезпечується через повне покриття універсальної множини $[0,1]$ функціями належності 5 еталонних станів. Я використала коефіцієнт зближеності, щоб суміжні функції перетиналися на рівні не менше 0.25. Це гарантує, що для будь-якого вхідного x

сума ступенів належності не дорівнює нулю, отже, система завжди видасть хоча б один лінгвістичний висновок.

9. СИДОРЕНКО В.М., к.т.н., доцент, доцент кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Чому Ви обрали трапецієподібні функції належності, а не наприклад трикутні?

Відповідь: Дякую за запитання. Трикутні функції мають лише одну точку максимуму, що означає «ідеальний стан». Проте рівень захищеності зазвичай характеризується певним плато (ядро стану). Трапецієподібні функції LR-типу дозволяють формалізувати цей інтервал стабільності, що робить модель більш адекватною реальним процесам на ОКІІ.

Запитання: Чи можна застосувати Ваші результати поза сферою критичної інфраструктури, наприклад, для оцінювання ІТ-стартапів чи малого бізнесу?

Відповідь: Дякую за запитання. Так, це цілком можливо. Хоча модель оптимізована під ОКІІ через коефіцієнт розширення, її «функціональне ядро» (NIST CSF 2.0) є універсальним. Для малого бізнесу можна просто відключити секторальні критерії та використовувати метод нечіткої інтерпретації для отримання швидкого та зрозумілого звіту про стан захищеності.

10. ПОЛОЖЕНЦЕВ А.А., PhD, доцент кафедри комп'ютерних інформаційних технологій КАІ.

Запитання: Чому за основу взято саме NIST CSF 2.0, а не міжнародний стандарт ISO/IEC 27001?

Відповідь: Дякую за запитання. ISO 27001 є процесно-орієнтованим стандартом («так/ні»), тоді як NIST CSF 2.0 пропонує гнучку структуру функцій, що краще піддається кількісному вимірюванню та математичному моделюванню. Крім того, саме NIST зараз є базисом для оновлення нормативної бази України, що робить результати актуальнішими для впровадження.

Після відповідей на запитання виступили:

Науковий керівник – д.т.н., професор, проректор з наукових досліджень та трансферу технологій КАІ Гнатюк Сергій Олександрович.

Доброго дня, шановні колеги! Хочу подякувати за увагу до роботи Юдіної Діани Олексіївни. Представлена дисертація є результатом системної й послідовної роботи, що поєднала ґрунтовний теоретичний аналіз інформаційних процесів, складне математичне моделювання та практичну апробацію на реальних об'єктах.

Дисертація присвячена актуальній науково-прикладній проблемі – підвищенню об'єктивності та оперативності оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури (ОКІІ). Ця тема є надзвичайно критичною, оскільки сучасна система державного контролю у сфері кібербезпеки потребує переходу від суб'єктивного аудиту до точних обчислювальних методів, особливо в умовах воєнного стану та активної зміни ландшафту загроз.

У роботі розроблено та реалізовано: 1) математичну модель оцінювання структурно-функціональних характеристик ОКІІ, яка на базі 111 показників та коефіцієнта структурного розширення дозволяє адаптувати процес оцінювання до будь-якого із 24 секторів критичної інфраструктури; 2) математичну модель нечіткої інтерпретації результатів, яка за допомогою апарату нечітких чисел LR-типу та індексу впевненості забезпечує перехід від «сухих» цифр до багатоваріантного інтелектуального висновку щодо стану захищеності; 3) метод оцінювання стану кіберзахисту, що поєднує ці моделі в єдину інформаційну технологію, інтегровану з міжнародним фреймворком NIST CSF 2.0.

Хочу наголосити на високій дослідницькій культурі здобувачки: Діана Олексіївна продемонструвала відмінне знання сучасних наукових джерел, самостійність, вміння комплексно підходити до складних системних проблем і здатність довести теоретичне дослідження до рівня працюючого програмного продукту.

Здобувачка повністю виконала індивідуальний навчальний план та індивідуальний план наукової роботи. У процесі підготовки дисертації вона продемонструвала ґрунтовні знання у галузі комп'ютерних наук, методів прийняття рішень, володіння сучасним математичним апаратом, а також здатність до аналізу великих масивів нечітких даних. Отримані результати повністю відповідають освітньо-науковій програмі спеціальності 122 «Комп'ютерні науки».

Усі завдання дослідження реалізовані послідовно: від математичного обґрунтування моделей та методу до їх практичного впровадження. Запропоновані рішення дозволяють усунути «ефект компенсації» слабких ланок захисту та підвищити оперативність процедур оцінювання на 42,2%, що підтверджено реальними актами впровадження, зокрема в Адміністрації Держспецзв'язку.

Вважаю, що представлена дисертація цілком відповідає вимогам, які висуваються до кваліфікаційних робіт на здобуття наукового ступеня доктора філософії. Результати дослідження мають як фундаментальне значення для розвитку теорії інтелектуальних систем, так і широкі прикладні перспективи для зміцнення національної стійкості.

Дисертаційна робота є завершеною науковою працею, яка вирішує актуальну задачу в межах спеціальності 122 «Комп'ютерні науки», а її авторка, Юдіна Діана Олексіївна, заслуговує присудження ступеня доктора філософії на підставі Порядку, затвердженого постановою Кабінету Міністрів України № 44 від 12 січня 2022 року.

Рецензенти дисертаційної роботи, які наголосили на позитивних аспектах дослідження та висловили свої побажання та зауваження:

АХРАМОВИЧ В.М., д.т.н., проф., професор кафедри кібербезпеки КАІ.

Дисертаційна робота Юдіної Діани Олексіївни «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури» присвячена вирішенню актуальної науково-прикладної проблеми – підвищенню об'єктивності, точності та оперативності процесів оцінювання захищеності стратегічних об'єктів держави.

Позитивним аспектом роботи є комплексність дослідження: від системного аналізу методологічних прогалин чинної нормативної бази до створення гібридної ієрархічної моделі, математичного апарату нечіткої інтерпретації результатів та їх практичної перевірки за допомогою авторського програмного комплексу. Результати підтверджено експериментальними дослідженнями на об'єкті паливно-енергетичного сектору та впровадженням у діяльність Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, НДЛ протидії кіберзагрозам в авіаційній галузі Державного університету «Київський авіаційний інститут».

Авторкою розроблено метод багатокритеріального оцінювання та математичну модель нечіткої інтерпретації на основі чисел LR-типу трапецієподібної форми. Це забезпечує адаптивність процесу оцінювання до специфіки 24 галузей критичної інфраструктури, підвищує достовірність висновків у «сірих зонах» на межах рівнів захищеності, а також дозволяє нівелювати суб'єктивізм експертних суджень.

Ефективність запропонованих рішень кількісно оцінюється через скорочення часу проведення повного циклу оцінювання на 42,2% (з 13,5 до 7,8 люд.-год), що підтверджує досягнення поставленої мети щодо оптимізації операційних ресурсів під час оцінювання.

До зауважень можна віднести деяку стислу подачу порівняльного аналізу алгоритмічної складності розробленого ПЗ із комерційними аналогами та необхідність більш детального висвітлення питань автоматизованого збору даних у реальному часі. Ці моменти не знижують наукової цінності роботи, але можуть бути враховані в подальших дослідженнях.

На основі вищезазначеного вважаю, що дисертаційна робота Юдіної Діани Олексіївни є завершеним науковим дослідженням, відповідає спеціальності 122 «Комп'ютерні науки» та вимогам до дисертацій на здобуття ступеня доктора філософії, а її авторка заслуговує на присудження відповідного ступеня.

СИДОРЕНКО В.М., к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій КАІ.

Дисертаційна робота Юдіної Діани Олексіївни «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури» є ґрунтовним дослідженням, спрямованим на вирішення актуальної науково-прикладної задачі в межах спеціальності 122 «Комп'ютерні науки».

Авторці вдалося розв'язати складну науково-технічну задачу – алгоритмізувати процес оцінювання стану об'єктів критичної інформаційної інфраструктури в умовах високої ентропії та суб'єктивізму експертних даних.

Особливої наукової та технологічної уваги заслуговують програмна архітектура та реалізація дослідження. Важливим науковим результатом є впровадження каскадної обробки інформації. У роботі реалізовано оригінальний алгоритмічний підхід, де детерміновані дані, отримані в результаті перевірки показників, трансформуються в інтегральний показник через скалярний добуток векторів. Наступним етапом ці дані проходять через

шар нечіткої логіки для отримання обґрунтованого лінгвістичного висновку про стан об'єкта.

Технологічна довершеність системи підсилюється механізмом самодіагностики та перевірки узгодженості даних. Впроваджений алгоритм автоматизованого розрахунку відношення узгодженості дозволяє системі самостійно верифікувати якість вхідних експертних суджень. Експериментально доведено, що досягнутий у ході дослідження рівень $CR = 0,05$ гарантує високу математичну стійкість та достовірність отриманих результатів.

Окремо слід відзначити високу інтерпретованість результатів, що відповідає сучасній концепції Explainable AI (XAI). Завдяки використанню апарату асоціативних правил та розрахунку індексу впевненості, розроблена система не просто видає кінцеву цифру, а математично обґрунтовує ступінь довіри моделі до прийнятого рішення, що є критично важливим для об'єктів критичної інфраструктури.

Разом із загальним позитивним враженням від дослідження, слід висловити певні зауваження та побажання. У роботі розроблено теоретичний підхід та коефіцієнт розширення для 24 секторів критичної інфраструктури, проте детальна експериментальна апробація та верифікація результатів проведена переважно на прикладі одного – паливно-енергетичного сектору. Ширша апробація на об'єктах інших галузей (наприклад, банківської чи транспортної) дозволила б більш наочно продемонструвати універсальність запропонованого методу.

У другому розділі обґрунтовано вибір нечітких чисел LR-типу трапецієподібної форми. Проте в тексті дисертації бракує розгорнутого порівняльного аналізу обчислювальної складності цього підходу порівняно з іншими типами нечіткої логіки (наприклад, трикутними числами чи гаусовими функціями) саме в контексті продуктивності програмного комплексу на великих масивах даних.

Робота є завершеним науковим дослідженням. З огляду на викладене, вважаю, що дисертаційна робота Юдіної Діани Олексіївни відповідає вимогам спеціальності 122 «Комп'ютерні науки», а її авторка заслуговує на присудження ступеня доктора філософії.

В обговоренні дисертаційного дослідження взяли участь:

САВЧЕНКО А.С., д.т.н., проф., завідувачка кафедри комп'ютерних інформаційних технологій КАІ відзначила високий рівень наукової зрілості здобувачки та відповідність роботи спеціальності 122 «Комп'ютерні науки». Особливо було наголошено на вдалому поєднанні методів багатокритеріального аналізу з сучасними підходами до моделювання інформаційних процесів у сфері критичної інфраструктури. Це створює ґрунтовну базу для автоматизації процедур моніторингу та державного контролю та впровадження інтелектуальних систем підтримки прийняття рішень. Робота є завершеним науковим дослідженням, а її авторка заслуговує на присудження ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки».

ОХРІМЕНКО Т.О., к.т.н., ст. дослідник, заступник декана Факультету комп'ютерних наук та технологій, акцентувала увагу на науковій новизні дисертації, зокрема на розробленні математичної моделі нечіткої інтерпретації результатів оцінювання. Було зазначено, що використання нечітких чисел LR-типу та розрахунків індексу впевненості суттєво підвищує достовірність оцінювання у «сірих зонах» на межах рівнів захищеності. Зазначила, що дисертаційна робота Юдіної Діани відповідає спеціальності 122 «Комп'ютерні науки», є завершеним самостійним науковим дослідженням, а її авторка заслуговує на присудження ступеня доктора філософії.

ІЛЬЄНКО А.В., к.т.н., доцент, завідувачка кафедри кібербезпеки КАІ підкреслила, що робота вирізняється комплексністю та завершеністю: від глибокого математичного обґрунтування моделей та методу до їх практичної апробації на реальному об'єкті паливно-енергетичного сектору. Було відзначено суттєвий практичний ефект – скорочення часу оцінювання на 42,2%, що є важливим показником для спеціальності 122. Також було наголошено, що впровадження результатів дисертації в освітній процес та їх відповідність оновленим нормативним актам сприяє підвищенню якості підготовки майбутніх фахівців. Зазначила, що дисертаційна робота Юдіної Д. відповідає встановленим вимогам до завершених наукових досліджень за спеціальністю 122 «Комп'ютерні науки», у зв'язку з чим її авторка заслуговує на присудження ступеня доктора філософії.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Юдіної Діани Олексіївни на тему «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури», поданої на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології» за спеціальністю 122 «Комп'ютерні науки»

1. Обґрунтування вибору теми дослідження. Вибір теми дисертаційної роботи Юдіної Діани Олексіївни зумовлений сучасними викликами, що постають перед системою національної стійкості України в умовах інтенсифікації кіберзагроз та необхідності забезпечення надійного функціонування об'єктів критичної інформаційної інфраструктури (ОКІІ). Швидка цифровізація стратегічних галузей, складність архітектур інформаційних систем та динамічний характер кібератак у період воєнного стану створюють гостру потребу в об'єктивних моделях та методах оцінювання стану їхньої захищеності у реальному часі.

Оцінювання стану кіберзахисту ОКІІ є одним із ключових напрямів, що дає змогу не лише констатувати рівень безпеки, а й гнучко керувати ризиками за рахунок ідентифікації «зон нестабільності» та перехідних станів системи. Існуючі підходи часто мають рамковий характер і базуються на суб'єктивних експертних оцінках, що в умовах спеціальності 122 потребує розроблення нових математичних моделей та алгоритмів для автоматизації цих процесів.

Актуальність теми посилюється прийняттям нової нормативно-правової бази у 2025–2026 роках, які висувають жорсткі вимоги до оперативності та точності оцінювання захищеності критичної інформаційної інфраструктури. Виявлення методологічних прогалин у класичних стандартах та необхідність урахування галузевої специфіки 24 секторів критичної інфраструктури роблять задачу розроблення інтелектуальних систем підтримки прийняття рішень надзвичайно важливою.

Обраний напрям дослідження має як фундаментальне наукове значення (розвиток апарату нечіткої логіки та багатокритеріального аналізу), так і високу практичну цінність. Розроблені моделі, метод та програмний комплекс забезпечують підвищення оперативності оцінювання на 42,2%, що має пряме прикладне значення для критичних секторів держави.

Таким чином, вибір теми дисертаційного дослідження є повністю обґрунтованим з точки зору сучасних потреб кіберзахисту України, наявних наукових проблем у сфері інтелектуальної обробки нечітких даних та актуальних завдань забезпечення стійкості об'єктів критичної інфраструктури в умовах постійних дестабілізуючих впливів.

2. Зв'язок роботи з науковими програмами, планами, темами, грантами. Теоретичні та практичні результати дисертаційного дослідження впроваджено у науково-дослідну діяльність Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Державного університету «Київський авіаційний інститут». Вони використовуються у межах теми «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (держ. реєстр №0125U000624).

Тема дисертації відповідає освітньої-науковій програмі «Комп'ютерні науки» за спеціальністю 122 «Комп'ютерні науки» галузі знань 12 «Інформаційні технології» в КАІ (зокрема, ОК 1.3.1, ОК 1.3.2, ОК 1.3.3 та ОК 1.3.4).

3. Мета і завдання дослідження. Мета дослідження полягає у досягненні високої точності та оперативності оцінювання показників кіберзахисту на основі розробленого комплексу моделей та методів.

Для досягнення поставленої мети були поставлені такі *завдання*:

- здійснити аналіз та класифікацію існуючих підходів до оцінювання кіберзахисту ОКІІ для виявлення методологічних прогалин та обґрунтування необхідності переходу від статичного аудиту до моделі керованої стійкості;
- розробити гібридну ієрархічну модель системи показників кіберзахисту ОКІІ, яка інтегрує критерії нормативної відповідності та процесної зрілості з урахуванням секторальної специфіки;
- розробити математичну модель нечіткої інтерпретації результатів оцінювання на основі чисел LR-типу для формалізації експертних суджень в умовах невизначеності;
- розробити метод оцінювання стану кіберзахисту ОКІІ на основі багатокритеріального аналізу та методу аналізу ієрархій для встановлення вагових коефіцієнтів систем захисту, що забезпечить оптимізацію розподілу інвестицій у найбільш критичні вразливості;

– здійснити програмну реалізацію та експериментальну перевірку розроблених рішень на об'єктах паливно-енергетичного сектору для підтвердження достовірності та оперативності розробленого інструментарію.

4. Об'єктом дослідження є процес оцінювання стану кіберзахисту ОКІІ.

5. Предметом дослідження є моделі та методи кількісного оцінювання та інтелектуальної інтерпретації показників кіберзахисту ОКІІ.

6. Методи дослідження. Для вирішення поставленого наукового завдання в дисертаційній роботі використані такі методи: системного аналізу – для вивчення архітектури систем кіберзахисту; теорії множин – для формалізації систем критеріїв; теорії нечітких множин – для моделювання невизначеності експертних оцінок; методу аналізу ієрархій – для визначення вагових коефіцієнтів впливу систем кіберзахисту на інтегральний показник.

7. Наукова новизна дослідження полягає у підвищенні об'єктивності, точності та оперативності процесів оцінювання стану кіберзахисту ОКІІ в умовах невизначеності експертних даних та динамічних дестабілізуючих впливів, де:

уперше:

– розроблено гібридну ієрархічну модель системи показників кіберзахисту ОКІІ, яка, на відміну від існуючих, базується на ієрархічній декомпозиції семи функціональних систем критеріїв (шість з яких гармонізовано з міжнародним фреймворком NIST CSF 2.0, а сьома – «Секторальна складова»), що дозволило вперше в межах єдиного оціночного циклу врахувати специфічні вимоги 24 галузей критичної інфраструктури України;

– обґрунтовано метод багатокритеріального оцінювання стану кіберзахисту, який відрізняється від відомих інтеграцією процедури перевірки нормативної відповідності з механізмом попарних порівнянь для пріоритезації захисних заходів, що забезпечило можливість формалізувати неоднаковий вплив різних систем захисту на інтегральний рівень безпеки об'єкта;

удосконалено:

– математичну модель нечіткої інтерпретації стану кіберзахисту, яка, на відміну від традиційних підходів, використовує нечіткі числа LR-типу трапецієподібної форми та розрахунок індексу впевненості, що дало змогу підвищити точність оцінювання у межових зонах між рівнями захищеності;

– процедуру формування якісних висновків щодо стану кіберзахисту шляхом впровадження апарату асоціативних правил до результатів фазифікації інтегрального показника, що дозволило констатувати поточний рівень захищеності та здійснювати прогнозування стійкості системи до дестабілізуючих впливів;

отримала подальший розвиток:

– класифікація рівнів зрілості процесів кіберзахисту, яка відрізняється врахуванням факторів воєнного стану та динамічної природи атак, що

дозволило диференціювати стан захищеності об'єктів за уточненою п'ятирівневою шкалою.

8. Теоретичне значення. Теоретичне значення дисертаційної роботи полягає у розвитку наукових уявлень про процеси моделювання та комплексного оцінювання стану кіберзахисту ОКІІ в умовах невизначеності експертних даних та динамічного ландшафту кіберзагроз. Сформовано гібридну ієрархічну модель системи показників кіберзахисту, яка базується на гармонізації міжнародних фреймворків та національних галузевих вимог, що дозволяє формалізувати структурно-функціональні особливості ОКІІ та описувати взаємозв'язок між технічними і організаційними заходами у реальних експлуатаційних умовах. Удосконалено математичний апарат нечіткої інтерпретації стану системи через застосування чисел LR-типу трапецієподібної форми та розрахунок індексу впевненості, що дало можливість теоретично обґрунтувати новий підхід до ідентифікації межових («сірих») зон захищеності та прогнозування стійкості систем до дестабілізуючих впливів. Отримані результати становлять основу для подальших досліджень у галузі інтелектуального аналізу даних, систем підтримки прийняття рішень та методів забезпечення кіберстійкості складних інформаційних систем.

9. Практичне значення та використання результатів дисертаційного дослідження. Практичні результати можна звести до наступних пунктів:

1. Сформовано систему критеріїв оцінювання, що включає 106 базових критеріїв та 91 галузевий критерій, що дозволяє суб'єктам критичної інфраструктури формувати індивідуальні оціночні профілі для проведення внутрішнього аудиту та забезпечення відповідності вимогам національного законодавства і європейської Директиви NIS 2.

2. Реалізовано програмний застосунок, який автоматизує розрахунок інтегрального показника захищеності та візуалізує результати у формі пелюсткових діаграм і звітів.

3. Реалізовано методику оцінювання стану кіберзахисту, адаптовану до вимог паливно-енергетичного сектору критичної інфраструктури.

4. Практичні, теоретичні та експериментальні результати дисертаційного дослідження впроваджено у науково-дослідну діяльність:

- НДІЛ протидії кіберзагрозам в авіаційній галузі Державного університету «Київський авіаційний інститут» (акт про впровадження від 25.03.2026);

- Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації у роботі групи реагування на інциденти комп'ютерної безпеки (акт про впровадження від 16.03.2026),

- Адміністрації Державної служби спеціального зв'язку та захисту інформації України під час розроблення наказів від 30.01.2026 № 75 та від 16.04.2026 № 285 (акт про впровадження від 12.03.2026).

10. Особистий внесок здобувача. Дисертація «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури», Юдіної Діани Олексіївни є самостійною науковою працею, в якій наведено

теоретичні положення і висновки, власні ідеї та розробки автора, які дають змогу вирішити поставлені завдання. Усі висновки та практичні рекомендації, винесені на захист, розроблені дисертантом особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

11. Апробація результатів дослідження. Наукові результати та основні положення дисертаційної роботи доповідались, обговорювались на таких міжнародних науково-технічних та науково-практичних конференціях: «Advanced Trends in Information Theory» (Львів, 2024), та галузевих семінарах з питань кібербезпеки КІ (2023-2025 рр.).

12. Публікації. Основні положення та результати дисертаційного дослідження викладено в 5,5 наукових публікаціях, серед них 5,5 публікацій у наукових фахових виданнях України категорії Б, 1 публікація у збірниках матеріалів конференцій.

Список опублікованих праць за темою дисертації

Статті у наукових фахових виданнях України:

1. Юдіна Д.О. Модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 4(28). 2025. с. 586-598. DOI: <https://doi.org/10.28925/2663-4023.2025.28.829>

2. Юдіна Д.О. Модифікація моделі розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 1(29). 2025. с. 18-836. DOI: <https://doi.org/10.28925/2663-4023.2025.29.943>

3. Юдіна Д.О. Метод розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2(30). 2025. с. 473-487. DOI: <https://doi.org/10.28925/2663-4023.2025.30.986>

4. Юдіна Д.О., Юдін Д.О. Методика розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 3(31). 2025. с. 833-859. DOI: <https://doi.org/10.28925/2663-4023.2025.31.1083>

Особистий внесок Юдіної Д.О.: розроблено методику розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури, проведено порівняльний аналіз розробленого програмного забезпечення із міжнародними аналогами.

Особистий внесок Юдіна Д.О.: здійснено огляд і групування існуючих світових методик розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури та визначено їх обмеження.

5. Потій О.В., Шульга В.П., Іванченко Є.В., Корченко О.Г., Бакалинський О.О., Мялковський Д.В., Верба Д.В., Зубков Д.А., Юдіна Д.О. Модель системи характеристик даних для оцінювання стану кіберзахисту в Україні. *Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України*, №4 (107), 2023.с. 313-329 (гриф обмеження доступу – для службового користування)

Особистий внесок Юдіної Д.О.: здійснено аналіз існуючих підходів до визначення показників стану кіберзахисту на державному рівні, сформовано перелік параметрів об'єктів оцінювання.

Особистий внесок Потія О.В.: загальне наукове керівництво проектом, визначення стратегічних цілей оцінювання відповідно до Стратегії кібербезпеки України та координація взаємодії між суб'єктами забезпечення кібербезпеки під час проведення огляду.

Особистий внесок Шульги В.П.: формування загальної концепції розбудови моделі систем характеристик, розробка ієрархічної структури параметрів оцінювання організаційних умов діяльності щодо кіберзахисту.

Особистий внесок Іванченко Є.В.: застосування теоретико-множинного підходу для формалізації процесу побудови моделі даних, розробка математичних виразів для інтеграції підмножин показників за категоріями.

Особистий внесок Корченка О.Г.: обґрунтування методології формування бази даних первинних параметрів, наукове консультування щодо використання кортежних моделей для нечітких оцінювальних систем.

Особистий внесок Бакалинського О.О.: дослідження нормативно-правової бази у сфері кібербезпеки та захисту інформації, аналіз положень Законів України та нормативних документів системи ТЗІ щодо їх відповідності реальним загрозам.

Особистий внесок Мялковського Д.В.: аналіз статистичних даних Держспецзв'язку та звітів секторальних органів захисту щодо реального стану виконання заходів кіберзахисту на об'єктах огляду.

Особистий внесок Верби Д.В.: дослідження специфіки оцінювання стану кіберзахисту в оборонній сфері та на об'єктах критичної інфраструктури військового призначення.

Особистий внесок Зубкова Д.А.: розробка загальної структури узагальненої моделі даних, графічна візуалізація ієрархічних зв'язків між категоріями та показниками оцінювання.

6. Іванченко Є.В., Корченко О.Г., Бакалинський О.О., Мялковський Д.В., Верба Д.В., Зубков Д.А., Юдіна Д.О. Модель системи характеристик даних для оцінювання заходів кіберзахисту в Україні. *Збірник наукових праць Центрального науково-дослідного інституту Збройних Сил України* №4 (108). 2024. с. 180-196 (гриф обмеження доступу – для службового користування)

Особистий внесок Юдіної Д.О.: проведено аналіз узгодженості запропонованої системи характеристик із міжнародними стандартами у сфері оцінювання кібербезпеки. Сформовано перелік ознак (характеристик), що дозволяють ідентифікувати рівень впровадження окремих заходів кіберзахисту.

Особистий внесок Іванченко Є.В.: математичне моделювання процесів локалізації резервів поліпшення організаційно-технічних умов діяльності, формалізація шкал оцінювання показників у відсотковому відношенні.

Особистий внесок Корченка О.Г.: обґрунтування підходів до адаптації американського стандарту Risk Management Framework (NIST) та міжнародних стандартів серії ISO 27000 до нормативної бази України.

Особистий внесок Бакалинського О.О.: дослідження ефективності існуючої структури планування, звітування та моніторингу реалізації Стратегії

кібербезпеки України, розробка рекомендацій щодо впровадження індикаторів виконання запланованих заходів.

Особистий внесок Мялковського Д.В.: систематизація показників методики оцінювання, розподіл показників спроможності за п'ятьма базовими категоріями та розробка формату збору розгорнутих відповідей.

Особистий внесок Верби Д.В.: інтеграція вимог щодо кіберзахисту автоматизованих систем управління технологічними процесами (АСУ ТП) та специфічних військових стандартів у загальну модель характеристик даних.

Особистий внесок Зубкова Д.А.: алгоритмізація зведення та інтегрування оцінок, одержаних за кожною характеристикою в межах відповідного критерію по об'єктах огляду, підготовка графічного матеріалу статті.

7. Шульга В.П., Корченко О.Г., Іванченко Є.В., Бакалинський О.О., Мялковський Д.В., Зубков Д.А., Юдіна Д.О. Метод оцінювання стану кіберзахисту об'єкту огляду критичної інфраструктури держави. *Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем*. 2023. Вип. 25 (II). с. 40-57 (гриф обмеження доступу – для службового користування)

Особистий внесок Юдіної Д.О.: обґрунтовано вибір критичних параметрів, що підлягають обов'язковому огляду в межах об'єкта критичної інфраструктури.

Особистий внесок Шульги В.П.: загальне керівництво дослідженням, формування наукової концепції методу оцінювання стану кіберзахисту об'єктів критичної інфраструктури, координація роботи авторського колективу та фінальне затвердження тексту статті.

Особистий внесок Корченка О.Г.: наукове консультування з питань застосування теорії нечітких множин, розробка теоретичного підґрунтя для процедур фазифікації інтервалів і побудови еталонів для лінгвістичних змінних.

Особистий внесок Іванченко Є.В.: формалізація математичного апарату методу, розробка формул розрахунку поточних значень характеристик об'єктів огляду та розрахунку нечіткої суми складних систем.

Особистий внесок Бакалинського О.О.: аналіз сучасного стану нормативно-правового регулювання у сфері кібербезпеки об'єктів критичної інфраструктури в Україні, обґрунтування актуальності дослідження та його значення для забезпечення національної безпеки держави.

Особистий внесок Мялковського Д.В.: дослідження та критичний аналіз існуючих світових та вітчизняних підходів і методів оцінювання стану кіберзахисту, виявлення їхніх прогалин та недоліків в умовах динамічних кібератак.

Особистий внесок Зубкова Д.А.: розробка алгоритму первинного вимірювання на основі відстані Хемінга, розрахунок рівнів наближеності поточних значень до еталонних та розробка етапу візуалізації нечітких результатів.

Наукові праці, які додатково відображають наукові результати дисертації:

Yudina D., Yudin O. Model for Calculating the Level of Cybersecurity of Critical Infrastructure Facilities. *International Conference on Advanced Trends in Information Theory*, Lviv 21-23 Nov. 2024, pp. 325-329. DOI: <https://doi.org/10.1109/ATIT64324.2024.11222561>

13. Структура та обсяг дисертації. Дисертація складається з анотації, вступу, 4 розділів, висновків, списку використаних джерел та додатків. Повний обсяг дисертації становить 186 сторінок, із них – 143 основного тексту. Робота містить 20 рисунків, 13 таблиць, 4 додатки. Список використаних джерел налічує 103 найменування.

14. Характеристика особистості здобувача. Під час підготовки дисертаційної роботи Юдіна Діана Олексіївна проявила себе як ініціативний і наполегливий дослідник, здатний комплексно поєднувати глибокі теоретичні знання з комп'ютерних наук із практичним досвідом у сфері державного управління кіберзахистом. Здобувачка вільно володіє сучасними методами математичного моделювання, нечіткої логіки та алгоритмічного проектування, що дозволило їй отримати вагомні результати, які мають як наукову новизну, так і прикладну цінність для зміцнення кіберстійкості національної критичної інфраструктури. Поєднання наукової діяльності з роботою у Департаменті кіберзахисту Адміністрації Держспецзв'язку дало змогу Діані Олексіївні ефективно інтегрувати результати дослідження в реальну професійну практику та нормативну базу.

Під час роботи над дисертацією Діана Олексіївна виявила здатність ефективно планувати дослідницьку діяльність, дотримуватися термінів виконання етапів дослідження та інтегрувати отримані результати у практику.

15. Оцінка мови та стилю дисертації. Дисертація викладена науковим стилем сучасною українською мовою, із використанням усталеної термінології галузі «Комп'ютерні науки». Виклад матеріалу відзначається чіткістю, логічною послідовністю та аргументованістю.

Структура тексту відповідає вимогам Міністерства освіти і науки України щодо дисертаційних робіт, усі положення та результати подані в академічно коректній формі.

16. Відповідність принципам академічної доброчесності.

Дисертація відповідає чинним принципам академічної доброчесності. У роботі відсутні ознаки плагіату чи безпідставних запозичень. Усі використані наукові результати, підходи, методи та твердження супроводжуються відповідними бібліографічними посиланнями.

Авторка чітко відокремлює власні наукові здобутки від результатів попередніх досліджень інших учених. Представлені результати є достовірними та перевіреними, що підтверджено експериментальною перевіркою, апробацією на науковій конференції, публікаціями у фахових виданнях та впровадженням у практику.

17. Рецензенти рекомендують: відповідно до пп. 15, 16 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, *пропонується такий склад разової ради:*

Голова ради:

ОДАРЧЕНКО Роман Сергійович, д.т.н., проф., декан Факультету аеронавігації, електроніки та телекомунікацій КАІ.

Рецензенти:

АХРАМОВИЧ Володимир Миколайович, д.т.н., проф., професор кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

СИДОРЕНКО Вікторія Миколаївна, к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ.

Офіційні опоненти:

ГОНЧАР Сергій Феодосійович, д.т.н., ст. д-к, заступник директора з науково-технічної роботи Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

МИРУТЕНКО Лариса Вікторівна, к.т.н., доц., доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Усі члени разової спеціалізованої вченої ради не мають реальний чи потенційний конфлікт інтересів щодо здобувачки Юдіної Діани Олексіївни (зокрема, не є її близькою особою) та/або її наукового керівника.

У результаті попередньої експертизи дисертації Юдіної Діани Олексіївни повноти публікації основних результатів дослідження

УХВАЛЕНО:

1. Затвердити висновок про наукову новизну, теоретичне та практичне значення результатів дисертації Юдіної Діани Олексіївни на тему «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури».

2. Вважати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Юдіної Діани Олексіївни відповідає спеціальності 122 «Комп'ютерні науки» та вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), затвердженого постановою Кабінету Міністрів України від 23.03.2016. № 261 (зі змінами і доповненнями від 03 квітня 2019 року № 283), вимогам пп. 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 року № 44.

3. Рекомендувати дисертаційну роботу «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури», подану Юдіною Діаною Олексіївною на здобуття ступеня доктора філософії з галузі знань 12 «Інформаційні технології», за спеціальністю 122 «Комп'ютерні науки» до захисту у разовій спеціалізованій вченій раді.

4. Рекомендувати Вченій раді затвердити склад разової спеціалізованої вченої ради:

Головою спеціалізованої вченої ради:

ОДАРЧЕНКА Романа Сергійовича, д.т.н., проф., декана Факультету аеронавігації, електроніки та телекомунікацій КАІ.

Рецензентами:

АХРАМОВИЧА Володимира Миколайовича, д.т.н., проф., професора кафедри кібербезпеки Факультету комп'ютерних наук та технологій КАІ.

СИДОРЕНКО Вікторію Миколаївну, к.т.н., доц., доцента кафедри комп'ютерних інформаційних технологій Факультету комп'ютерних наук та технологій КАІ.

Офіційними опонентами:

ГОНЧАРА Сергія Феодосійовича, д.т.н., ст. дослідника, заступника директора з науково-технічної роботи Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

МИРУТЕНКО Ларису Вікторівну, к.т.н., доц., доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.

Результати голосування щодо рекомендації до захисту дисертації Юдіної Діани Олексіївни:

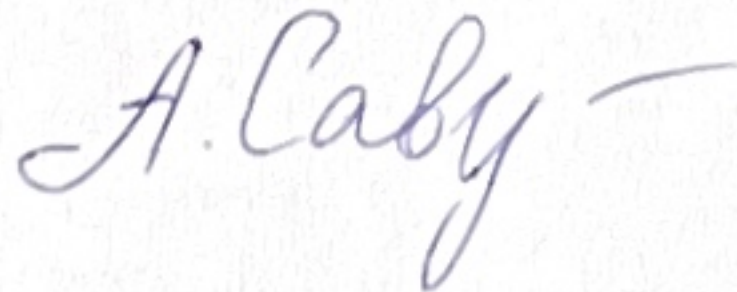
«за» – 10.

«проти» – немає.

«утримались» – немає.

Головуючий на засіданні:

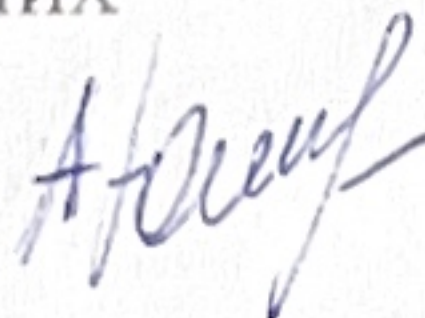
завідувачка кафедри комп'ютерних інформаційних технологій КАІ,
д.т.н., професор



Аліна САВЧЕНКО

Секретар засідання:

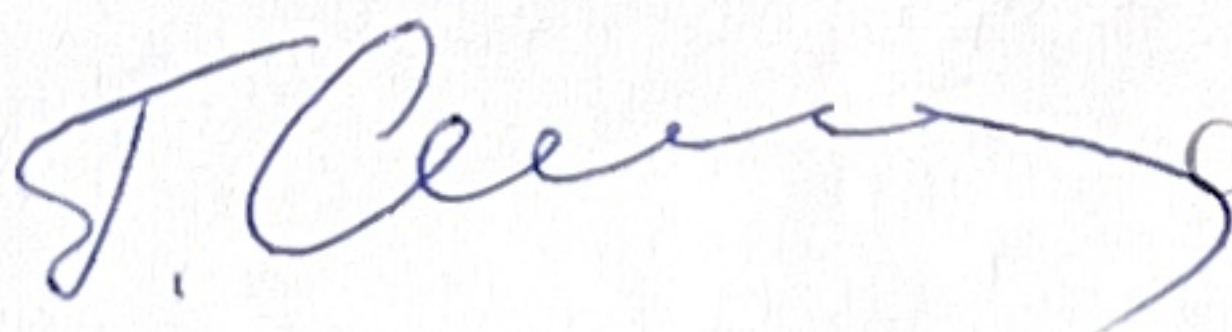
доцент кафедри комп'ютерних інформаційних технологій КАІ,
PhD



Артем ПОЛОЖЕНЦЕВ

ПОГОДЖЕНО:

проректор з наукових досліджень та трансферу технологій КАІ,
д.т.н., професор



Сергій ГНАТЮК