ЗАТВЕРДЖУЮ
Ректор Національного університету
«Одеська юридична академія»

_____ Олег ТОДОЩАК

«12» 03 2026 року

ВИСНОВОК

Національного університету «Одеська юридична академія» про наукову новизну, теоретичне та практичне значення результатів дисертації Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», поданої на здобуття ступеня доктора філософії в галузі знань 07 «Управління та адміністрування» за спеціальністю 073 «Менеджмент», затвердженої Вченою радою Національного університету «Одеська юридична академія» № 2 від 14 листопада 2023 року (уточнено Вченою радою Національного університету «Одеська юридична академія» № 1 від 28 серпня 2025 року)

ВИТЯГ

з протоколу міжкафедрального семінару кафедри кібербезпеки, кафедри економіки та менеджменту та кафедри штучного інтелекту та математичного моделювання Національного університету «Одеська юридична академія» від 26 березня 2026 року

Присутні:

Головуюча: професор кафедри економіки та менеджменту, д.е.н., професор Слободянюк О. В.

кафедра кібербезпеки: в.о. завідувача кафедри, д.т.н., професор Соколов А.В., доцент кафедри, к.т.н., доцент Бойко В.Д.

кафедра економіки та менеджменту: завідувач кафедри, д.е.н., професор Кібік О.М., доцент кафедри, к.е.н., доцент Примаченко І.Ф., доцент кафедри, к.е.н., доцент Котлубай В.О., доцент кафедри, к.е.н., доцент Редіна Є.В., доцент кафедри, к.е.н., доцент Візіренко С.В., доцент кафедри, к.е.н. Капустян І.В.

кафедра штучного інтелекту та математичного моделювання: в.о. завідувача кафедри, д.е.н., професор Горбаченко С.А. (*науковий керівник*), доцент кафедри, к.е.н., доцент Куклінова Т.В., доцент кафедри, к.ф.-м.н., доцент Черевко Є.В. асистент кафедри Разінкін Н.С., асистент кафедри Овчинников М.Ю.

аспіранти: Скідан В.С., Сіянко П.В., Крейтор С.Ю., Кірович А.Ф.

Були присутні 4 доктори наук та 8 кандидатів наук за профілем поданої на розгляд дисертації.

Порядок денний:

Обговорення дисертаційного дослідження Саврацького Олександра Олександровича на тему: «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», поданого на здобуття ступеня вищої освіти доктора філософії за спеціальністю 073 «Менеджмент» щодо рекомендації до разового публічного захисту дисертації у спеціалізованій вченій раді.

Слухали:

Доповідь здобувача ступеня вищої освіти доктора філософії Саврацького О. О. на тему: «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», поданої на здобуття вищої освіти доктора філософії за спеціальністю 073 «Менеджмент».

Доповідач обґрунтував актуальність обраної теми, визначив мету, завдання, методологію дисертаційного дослідження, охарактеризував його об'єкт та предмет, виклав науково-практичну значимість роботи, надав відомості щодо впровадження результатів дослідження.

Обґрунтовуючи вибір напряму дисертаційного дослідження, здобувач зазначає, що актуальність обраної теми зумовлена необхідністю управлінського втручання у вирішення проблеми забезпечення ефективного захисту об'єктів критичної інфраструктури від зростаючих загроз в умовах стрімкого впровадження цифрових технологій. Адже, з одного боку, функціонування ключових сфер життєдіяльності суспільства (енергетики, транспорту, зв'язку, фінансів тощо) дедалі більше залежить від інформаційної складової. З іншого боку, традиційні формалізовані технічні та нормативно-правові заходи кіберзахисту виявляються недостатніми для забезпечення належного рівня цифрової стійкості, що викликає необхідність переходу до комплексних управлінських рішень.

В умовах повномасштабного вторгнення прийшло загальне розуміння того, що протидія кіберзагрозам, особливо коли мова йде про критичну інфраструктуру, виходить за межі суто технічної проблематики і переходить на рівень стратегічного управління. Більш того, навіть успішна локальна модель управління кіберзахистом не завжди встигає за постійною трансформацією загроз, адже безпекові рішення швидко втрачають свою актуальність. Відтак, постійний пошук нестандартних рішень, розробка та впровадження управлінських інновацій виступають вже не просто як елемент зміцнення конкурентоспроможності, це – об'єктивна необхідність в сучасних реаліях.

Теоретичними, методологічними, методичними та прикладними аспектами впровадження управлінських інновацій при вирішенні питань безпеки та протидії загрозам, в тому числі кіберзагрозам критичній інфраструктурі, переймалися такі вітчизняні вчені, як Р. Августин, О. Божанова, Т. Васильців, А. Гайдученко, С. Горбаченко, В. Гречанінов, М. Домарацький, Д. Дячков, О. Зачко, В. Зянько, М. Караїм, О. Кібік, Д. Кобилкін, А. Ковальов, М. Копитко, Д. Котелевець, В. Котлубай, Я. Котляревський, Т. Куклінова, В. Лойко, С. Мельник,

Ю. Ольвінська, А. Осокіна, І. Павук, В. Панченко, С. Прохорчук, Є. Рединa, В. Франчук, В. Храпкіна, О. Чепурна, Н. Чухрай, А. Штангрет та інші.

Водночас, проблема інтеграції управлінських інновацій у систему кіберзахисту критичної інфраструктури ще недостатньо висвітлена в наукових дослідженнях. Адже в переважній більшості наукових праць або оглядово розглядається весь комплекс управлінських питань безпеки критичної інфраструктури, або висвітлюються підходи до забезпечення кібербезпеки в технічному або нормативно-правовому аспектах або досліджуються тренди інноваційного управління, але без фокусування на завданнях запобігання кіберзагрозам. Вказана ситуація дозволяє стверджувати про наукові перспективи формування окремої гілки досліджень у якій першочергова увага приділятиметься впровадженню управлінських інновацій в безпекові процеси.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота виконана відповідно до планів науково-дослідної роботи Національного університету «Одеська юридична академія» за темою: «Правове і соціальне життя сучасної України у людиноцентристському вимірі в цифрову еру» (державний реєстраційний номер 0122U000266) та кафедри кібербезпеки - за темою «Безпека інформації та її складових в інформаційно-комунікаційних системах». У межах кафедральної теми автор проводив дослідження управлінських аспектів забезпечення безпеки інформації та її складових, на прикладі об'єктів критичної інфраструктури. Тему дисертації затверджено рішенням вченої ради Національного університету «Одеська юридична академія» від 14 листопада 2023 року, протокол № 2 (уточнено 28 серпня 2025 року, протокол № 1).

Мета і завдання дослідження. Метою дисертаційної роботи є обґрунтування наукових засад та розробка практичного інструментарію впровадження управлінських інновацій у сфері кіберзахисту критичної інфраструктури.

Для досягнення зазначеної мети у дисертації вирішувались такі завдання:

- дослідити науковий базис управління безпековими процесами на основі впровадження інновацій;
- охарактеризувати критичну інфраструктуру як об'єкт управління та систематизувати загрози її функціонуванню з позиції управлінського реагування;
- проаналізувати методичні підходи та міжнародні стандарти управління захистом критичної інфраструктури від кіберзагроз;
- визначити особливості процесу управління кіберзахистом критичної інфраструктури з урахуванням нормативно-правового базису та технологічних можливостей;
- оцінити доступність та управлінську доцільність використання наявних ринкових рішень для кіберзахисту об'єктів критичної інфраструктури;
- проаналізувати механізми управлінського впливу на забезпечення кіберзахисту критичної інфраструктури із застосуванням управлінських інновацій;

- розробити організаційні та інституційні підходи до реалізації інноваційних перетворень в управлінні кіберзахистом критичної інфраструктури;
- обґрунтувати інноваційний управлінський підхід до захисту критичної інфраструктури від кіберзагроз з використанням інструментів штучного інтелекту для підтримки управлінських рішень;
- розробити модель впливу управлінських інновацій на ефективність захисту об'єктів критичної інфраструктури.

Об'єктом дослідження є процес управління захистом критичної інфраструктури від кіберзагроз.

Предметом дослідження є комплекс теоретичних, організаційних, методичних і практичних основ управління кіберзахистом критичної інфраструктури з використанням управлінських інновацій.

Методи дослідження. В дисертаційній роботі використано методи: аналізу та синтезу – для узагальнення наукових джерел, систематизації понять безпеки, інновацій та кібербезпеки з огляду на їхнє використання в управлінських дослідженнях (підрозділи 1.1, 1.2); абстрагування – з метою виділення ключових складових елементів безпеки, таких як фізична, економічна, екологічна та кібербезпека (підрозділ 1.3); порівняльного аналізу – для дослідження кон'юнктури ринку продуктів та послуг кібербезпеки та його окремих сегментів (підрозділ 2.2), а також аналізу нормативно-правової бази та міжнародних стандартів (підрозділи 2.1, 2.2); графоаналітичного («Квадрат потенціалу») – для оцінки управлінської готовності підприємств енергетичної сфери до інтеграції штучного інтелекту, що передбачає ранжування об'єктів дослідження за технологічними, управлінськими, комунікаційними та фінансовими блоками з розрахунком сум місць та довжин векторів (підрозділ 3.2); графічного – для наочного і всебічного відображення результатів проведеного дослідження (розділи 2, 3); абстрактно-логічного – під час проведення теоретичних узагальнень і формування висновків дослідження (висновки до розділів). Застосовано економіко-математичне моделювання раціонального розподілу інвестицій у кіберзахист об'єктів критичної інфраструктури. Для інтерпретації комплементарності заходів запроваджено управлінський індикатор кіберстійкості (підрозділ 3.3).

Інформаційною базою дослідження є чинні нормативні документи (Верховної Ради України, Кабінету Міністрів України тощо), актуальна вітчизняна та зарубіжна наукова література, офіційні статистичні дані, аналітичні звіти, фінансова звітність і первинна документація суб'єктів підприємництва, що відносяться до критичної інфраструктури, результати опитування профільних фахівців, інформаційні ресурси мережі Інтернет, матеріали особистих досліджень автора.

Наукова новизна одержаних результатів полягає в тому, що дисертація є однією з перших у вітчизняній управлінській науці спроб комплексного дослідження теоретико-методичних та практичних засад забезпечення захисту критичної інфраструктури України від кіберзагроз на основі не тільки технічних

рішень та нормативно-правових обмежень, а й із застосуванням управлінських інновацій.

За результатами дисертаційного дослідження отримано наступні результати, що мають наукову новизну:

Вперше:

- розроблено інтегровану модель, яка формалізує взаємозв'язок між організаційною (управлінською), кадровою та технічною складовими системи кіберзахисту та враховує диференційований вплив управлінських інновацій на окремі категорії персоналу (управлінський, технічний, користувачі інформаційних систем) і галузеву специфіку секторів критичної інфраструктури (енергетика, телекомунікації, державне управління). На основі результатів оцінювання запропоновано управлінські рішення для підвищення кіберстійкості об'єктів критичної інфраструктури.

Вдосконалено:

- структуризацію об'єктів критичної інфраструктури, в якій, на відміну від існуючих варіантів, до нормативного показника критичності та рівня інформатизації окремих об'єктів додано управлінський показник організаційної схильності до інновацій, визначений на основі бального методу. В результаті розраховано інтегральний індекс інноваційної пріоритетності і визначено найбільш перспективні складові критичної інфраструктури для подальшого впровадження управлінських інновацій, спрямованих на протидію кіберзагрозам.

- модель оптимізації інвестицій у кібербезпеку на основі адаптації моделі Гордона–Льоба, яка, на відміну від базової версії, інтегрує функцію кіберстійкості об'єктів критичної інфраструктури, що дозволяє інтерпретувати кіберзахист як економічно обумовлений управлінський процес із властивими йому закономірностями зростання граничної ефективності інвестицій до визначеного порогового значення та її подальшого зниження. В результаті менеджмент об'єктів критичної інфраструктури може визначити економічно обґрунтований рівень інвестування у заходи кібербезпеки.

- механізм оцінки управлінських альтернатив при формуванні системи кіберзахисту, який, на відміну від існуючих, при виборі конкретних інструментів передбачає дослідження кон'юнктури ринку продуктів та послуг кібербезпеки із застосуванням методів найменших квадратів та експоненційного згладжування за алгоритмом ETS. Застосування зазначеного механізму дозволяє науково обґрунтовувати рівень доступності та управлінську доцільність придбання готових рішень для забезпечення кібербезпеки критичної інфраструктури.

Набуло подальшого розвитку:

- застосування кластерного підходу для збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів в сфері кібербезпеки. Запропоновано створення кластеру кібербезпеки, який, на відміну від існуючих, орієнтується не стільки на координацію учасників та інформаційно-комунікаційну підтримку, скільки на інституціоналізацію процесів апробації, впровадження та комерціалізації інноваційних безпекових

рішень. В результаті об'єкти критичної інфраструктури у межах новоствореного кластеру можуть виступати замовниками продуктів та послуг кібербезпеки, стейкхолдерами для закладів вищої освіти, інвесторами стартапів безпекового напряму, тестувальниками інноваційних рішень.

- методичний підхід до впровадження інструментів штучного інтелекту в управлінські процеси енергетичної критичної інфраструктури із застосуванням графоаналітичних розрахунків, який, на відміну від існуючих підходів, дозволяє кількісно оцінити рівень готовності управлінської структури до цифрової трансформації системи управління кібербезпекою.

- визначення категорії «менеджмент кібербезпеки» як цілеспрямованого процесу планування, розробки, впровадження та управління комплексом організаційних, технічних і правових заходів, спрямованих на забезпечення сталого та безпечного функціонування життєво важливих об'єктів, а також їхній захист від актуальних і потенційних кіберзагроз, яке, на відміну від існуючих, конкретизує управлінський пріоритет на захисті «життєво важливих об'єктів», тобто, критичної інфраструктури.

- управлінську модель застосування командного підходу для вирішення завдань протидії кіберзагрозам, яка, на відміну від існуючих, передбачає наявність окремої посади менеджера з кібербезпеки, який приймає участь у стратегічному плануванні, відповідає за інтеграцію управлінських і технічних рішень, а також здійснює координацію діяльності команди з аналітика, фахівця з комунікацій та дослідження ринку, фахівців технічного блоку. В результаті сформована команда може швидше адаптуватися до нових безпекових викликів, генерувати інноваційні рішення та ефективно розподіляти ресурси.

- теоретичний підхід до застосування циклу PDCA для управління кіберзахистом критичної інфраструктури, який, на відміну від традиційних підходів, інтегрує принципи проактивності, комплексності та адаптивності. В результаті поєднання безперервного процесного управління із сучасними аналітичними моделями попередження загроз створюються умови для ефективного впровадження інноваційних управлінських рішень.

Після завершення доповіді Саврацького О.О. присутніми поставлені такі запитання:

Завідувач кафедри економіки та менеджменту, д.е.н., професор Кібік О.М. запитала, які методологічні підходи покладено в основу розробки моделі взаємозв'язку організаційної, кадрової та технічної складових системи кіберзахисту, і чому саме вони були обрані?

Саврацький О. О. відповів, що методологічною основою моделі стали системний, процесний та міждисциплінарний підходи. При цьому системний підхід дозволив розглядати кіберзахист як комплекс взаємопов'язаних елементів управління, кадрового забезпечення та технічної інфраструктури. Процесний підхід забезпечив можливість інтеграції управлінських інновацій у безперервний цикл функціонування системи безпеки. Міждисциплінарність була необхідною з

огляду на поєднання управлінських, економічних та інформаційно-технологічних аспектів кібербезпеки.

Доцент кафедри економіки та менеджменту, к.е.н., доцент Редіна Є.В. поставила питання щодо ризиків, які можуть виникнути при впровадженні командної моделі управління кіберзахистом із залученням CISO. В чому саме вони проявляються?

Саврацький О. О. відповів, що основними ризиками є можливі конфлікти повноважень між керівництвом об'єктів критичної інфраструктури та менеджером з кібербезпеки, а також недостатня інтеграція технічних та управлінських рішень. Для їх мінімізації необхідно чітко визначити функціональні обов'язки CISO, забезпечити його участь у стратегічному плануванні та створити ефективні механізми комунікації між усіма членами команди. Крім того кадровий резерв при формуванні управлінської команди майже завжди є обмеженим (адже проблема забезпечення кіберзахисту потребує специфічних компетенцій від менеджерів), успішність кожного менеджера у межах однієї команди не гарантує такий самий результат при переході в іншу, а самі кіберзагрози постійно еволюціонують, отже ефективність команди може погіршуватися із часом.

В.о. завідувача кафедри кібербезпеки, д.т.н., професор Соколов А.В. поцікавився, з якою метою в управлінському дослідженні використовувалися класичні технічні моделі, наприклад, «Діамант» та «MITRE ATT&CK?

Саврацький О. О. відповів, що, дійсно, в дисертаційному дослідженні доведено доцільність застосування вказаних моделей саме в управлінських процесах. Наприклад, як управлінська інновація, модель «Діамант» може застосовуватися менеджментом об'єктів критичної інфраструктури для зосередження зусиль на стратегічному аналізі вразливостей інформаційних систем і формуванні відповідних управлінських рішень. За її допомогою визначаються пріоритетні активи, що потребують найбільшого захисту. У свою чергу, модель «MITRE ATT&CK» є фундаментом для формування управлінських рішень під час переходу від реактивного до проактивного захисту. Адже у такій ситуації менеджменту доцільно застосовувати принцип Парето, щоб зосередитися на найпоширеніших тактиках атак, і розробляти плани для їхньої нейтралізації ще до фактичного виникнення.

Доцент кафедри економіки та менеджменту, к.е.н., доцент Котлубай В.О. запитав, яке практичне значення має запропонований кластерний підхід до організації кібербезпеки критичної інфраструктури?

Саврацький О. О. відповів, що практичне значення кластерного підходу полягає у створенні системної взаємодії між державою, бізнесом і науковими установами за моделлю «влада – бізнес – наука». При формуванні пропозиції використовувався, насамперед, іноземний досвід функціонування кластерів кібербезпеки, таких як кластер SFBA (США) та «Cyber Nation» (Ізраїль). Крім

того і в Україні вже функціонують «Національний Кластер Кібербезпеки» та «Український Кластер Кібербезпеки». Однак їхній функціонал є обмеженим: перший це координаційна платформа, спрямована на сталий розвиток сектору національної кібербезпеки України та організацію регулярних подій (зустрічей, форумів, самітів, освітніх конференцій), другий це Громадська спілка, яка займається правовими, процедурними та технічними питаннями комплексного захисту та безпеки інформаційних активів даних, а її основним завданням виступає просвітницька діяльність. Водночас, запропонований в дисертації кластер крім традиційної функції платформи кооперації бізнесу, держави та науки виступатиме також ініціатором інноваційних проєктів в сфері кібербезпеки, а також надаватиме комплекс послуг, орієнтованих на практичні потреби. Серед них консультаційні послуги з оцінки ризиків, семінари для менеджменту з персоналізованими рекомендаціями, модульні курси для персоналу з отриманням сертифікатів, спільний моніторинг та реагування на інциденти, комерціалізація розробок в сфері кібербезпеки тощо.

Доцент кафедри штучного інтелекту та математичного моделювання, к.ф.-м.н., доцент Черевко Є.В. запитав, який підхід використовувався для моделювання розподілу ресурсів на кіберзахист?

Саврацький О. О. відповів, що вирішення поставлених управлінських завдань спиралося, насамперед, на модель Гордона-Льоба. У цій моделі сукупні очікувані витрати розраховуються як сума самих інвестицій у захист та очікуваних втрат, які є добутком імовірності реалізації кіберінциденту на величину потенційних збитків. Однак класичний висновок цієї моделі, згідно з яким витрати на безпеку не можуть перевищувати певної математично визначеної частки від можливих збитків (відомий як правило «однієї третини»), орієнтований лише на один технічний напрям інвестування. Однак, сучасна практика вимагає від менеджменту враховувати спільний ефект не лише технічних інструментів, але й організаційних інвестицій, таких як навчання персоналу та розвиток культури інформаційної безпеки, що зумовлює потребу в складніших підходах до багатовекторного моделювання.

Доцент кафедри економіки та менеджменту, к.е.н. Капустян І.В. запитала, які конкретно методи, інструменти, показники використовувалися для оцінки ефективності управлінських інновацій?

Саврацький О. О. відповів, що з огляду на обрану в дослідженні проблематику методика оцінки ефективності управлінських інновацій базується, насамперед, на підході OCTAVE, який дозволяє менеджменту систематично ідентифікувати активи та оцінювати вразливості. Економічна доцільність інвестицій в управлінські інновації оцінювалася через розрахунок інтегрального індексу інноваційної пріоритетності, що включає бальний метод для управлінського показника організаційної схильності до інновацій, з урахуванням критичності об'єктів та рівня їхньої інформатизації. Економічна ефективність

управлінських інновацій за напрямом захисту від кіберзагроз оцінювалася за допомогою показника повернення інвестицій у безпеку (ROSI).

Доцент кафедри штучного інтелекту та математичного моделювання, к.е.н., доцент Куклінова Т.В. запитала, які переваги має використання графоаналітичного обчислення при оцінці готовності підприємств до цифрової трансформації систем управління кібербезпекою?

Саврацький О. О. відповів, що графоаналітичне обчислення дозволяє формалізувати складні взаємозв'язки між елементами управлінської системи та кількісно оцінювати ступінь готовності підприємства до цифрової трансформації. Такий підхід забезпечує наочність результатів, можливість порівняння різних організацій та виявлення ключових напрямів розвитку системи кібербезпеки.

Професор кафедри економіки та менеджменту, д.е.н., професор Слободянюк О.В. запитала яким чином удосконалена дисертантом структуризація об'єктів критичної інфраструктури сприяє більш ефективному впровадженню управлінських інновацій?

Саврацький О. О. відповів, що удосконалення полягає у доповненні існуючих критеріїв структуризації об'єктів критичної інфраструктури новим управлінським показником — рівнем організаційної схильності до інновацій. Він визначається на основі бального методу і враховується разом із нормативним показником критичності та рівнем інформатизації об'єктів. У результаті в дисертації розраховано інтегральний індекс інноваційної пріоритетності та визначено ті складові критичної інфраструктури, де впровадження управлінських інновацій у сфері кіберзахисту є найбільш доцільним та потенційно ефективним.

Після відповідей на запитання виступив науковий керівник – в.о. завідувача кафедри штучного інтелекту та математичного моделювання, д.е.н., професор Горбаченко Станіслав Анатолійович.

Науковий керівник зазначив, що автору вдалося виконати поставлені завдання та досягти поставленої мети. Для цього було використано сукупність загальнонаукових та спеціальних методів, зокрема: методи аналізу та синтезу, абстрагування, порівняльного аналізу, графоаналітичний метод, а також економіко-математичне моделювання.

Дисертація має виражену наукову новизну, в ній наведено теоретичне узагальнення і нове вирішення наукового завдання, поставленого перед здобувачем наукового ступеня. Зокрема автором розроблено модель, яка відображає взаємозв'язок між організаційною (управлінською), кадровою та технічною складовими системи кіберзахисту і дозволяє оцінити ефективність управлінських інновацій з урахуванням спрямування на окремі категорії

персоналу та особливостей різних секторів критичної інфраструктури. На основі результатів проведеного оцінювання запропоновано перелік управлінських рішень, спрямованих на підвищення стійкості об'єктів критичної інфраструктури до кіберзагроз.

У дисертації вдосконалено структуризацію об'єктів критичної інфраструктури, розраховано інтегральний індекс інноваційної пріоритетності і визначено найбільш перспективні складові критичної інфраструктури для подальшого впровадження управлінських інновацій, спрямованих на протидію кіберзагрозам. Трансформовано модель Гордона-Льоба та функцію кіберстійкості для оптимізації інвестицій у кібербезпеку, що надає можливість інтерпретувати кіберзахист як цілісний управлінський процес із притаманними йому економічними закономірностями. У результаті можна визначити межу виправданого інвестування, щоб забезпечити необхідний кіберзахист без надмірного фінансового навантаження. Вдосконалено механізм оцінки управлінських альтернатив при формуванні системи кіберзахисту, який, на відміну від існуючих, при виборі конкретних інструментів передбачає дослідження кон'юнктури ринку продуктів та послуг кібербезпеки із застосуванням методів найменших квадратів та експоненційного згладжування за алгоритмом ETS. Застосування зазначеного механізму дозволяє науково обґрунтовувати рівень доступності та управлінську доцільність придбання готових рішень для забезпечення кібербезпеки критичної інфраструктури.

Набули подальшого розвитку методичні засади впровадження інструментів штучного інтелекту в управлінські процеси енергетичної критичної інфраструктури із застосуванням графоаналітичного обчислення; застосування кластерного підходу для збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів у сфері кібербезпеки у межах трикутника «влада-бізнес-наука»; управлінська модель організації кіберзахисту на основі командного підходу, з інтеграцією посади менеджера з кібербезпеки (CISO); теоретичний підхід до застосування циклу управління PDCA для захисту критичної інфраструктури від кіберзагроз, який ґрунтується на інтеграції принципів проактивності, комплексності та адаптивності; сформовано авторське визначення категорії «менеджмент кібербезпеки», яке, на відміну від існуючих, конкретизує управлінський пріоритет на захисті «життєво важливих об'єктів», тобто, критичної інфраструктури.

Основні результати дисертаційного дослідження Саврацького О. О. пройшли належну апробацію шляхом публікації положень дисертацій у фахових виданнях та виступах, обговорень на науково-практичних конференціях.

Зміст дисертації свідчить, що дослідження Саврацького О. О. виконано на високому науковому рівні, проаналізований значний обсяг теоретичного та аналітичного матеріалу, робота містить ряд цікавих нових висновків та пропозицій. Дослідження ґрунтується на виваженій самостійній роботі над темою дисертації.

У процесі підготовки дисертації Саврацький О. О. плідно співпрацював з науковим керівником протягом усього терміну навчання в аспірантурі,

результатом чого є написання дисертаційного дослідження. Здобувач виконав індивідуальний план наукової роботи та індивідуальний навчальний план у повному обсязі. Всі заплановані види робіт були виконані своєчасно та на високому рівні.

Щодо загальної оцінки роботи Саврацького О. О. у процесі підготовки дисертації та виконання індивідуального плану наукової роботи та індивідуального навчального плану, вона оцінюється на відмінно.

Викладене дозволяє зробити висновок про те, що дисертація Саврацького Олександра Олександровича на тему: «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз» є самостійним науковим дослідженням, яке відповідає всім встановленим вимогам, може бути рекомендована до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 073 «Менеджмент», галузі знань 07 «Управління та адміністрування» у разовій спеціалізованій вченій раді, а її автор заслуговує, на основі захисту, присвоєння наукового ступеня доктора філософії.

У **обговоренні** дисертаційного дослідження брали участь:

Доктор економічних наук, професор Кібік О.М. відзначила системність дослідження, належний рівень володіння здобувачем матеріалом, а також звернула увагу на загальну високу якість виконаної роботи. Підсумувала, що робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 073 «Менеджмент» відповідає встановленим вимогам, є завершеним та якісним дослідженням, що містить цілісні наукові положення та результати і може бути рекомендована до разового публічного захисту у спеціалізованій вченій раді.

Кандидат економічних наук, доцент Примаченко І.Ф. звернув увагу на актуальність наукових висновків та пропозицій, а також загальне практичне спрямування дисертації, що засвідчують довідки про впровадження її результатів. Вказав, що робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 073 «Менеджмент» є завершеним та якісним дослідженням, містить обґрунтовані наукові результати та може бути рекомендована до разового публічного захисту в спеціалізованій вченій раді.

Кандидат економічних наук, доцент кафедри Капустян І.В. підкреслила високу актуальність дисертаційного дослідження, його наукову значущість і комплексність. Було відзначено ґрунтовність виконаної роботи, логічність викладення матеріалу та ретельність проведеного аналізу. На її думку, дисертація Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент», є завершеним і якісним науковим дослідженням, що містить

обґрунтовані наукові результати, та може бути рекомендована до публічного захисту у спеціалізованій вченій раді.

Кандидат економічних наук, доцент Куклінова Т.В. звернула увагу на актуальність та змістовну наповненість дисертаційного дослідження, достатній рівень опрацювання матеріалу здобувачем, високий рівень застосування математичного апарату. Відзначила, що робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 073 «Менеджмент» є завершеним та якісним дослідженням, що містить положення та науково обґрунтовані результати у галузі менеджменту, та може бути рекомендована до разового публічного захисту у спеціалізованій вченій раді.

Кандидат економічних наук, доцент Редіна Є.В. наголосила на важливість обраної теми дисертації щодо вирішення питань протидії кіберзагрозам за допомогою управлінських інновацій, підкреслила її змістовність та високий рівень опрацювання наукових джерел. За її оцінкою, дисертаційна робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент», є завершеним науковим дослідженням, має теоретичне та практичне значення і може бути рекомендована до разового публічного захисту у спеціалізованій вченій раді.

Кандидат економічних наук, доцент Котлубай В.О. відзначив релевантність теми сучасним викликам та відмітив належну теоретичну підготовку здобувача. Порекомендував провести опитування серед керівництва об'єктів критичної інфраструктури щодо готовності запровадити штатну посаду менеджера з кібербезпеки. Зазначив, що робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент», відповідає встановленим вимогамі може бути рекомендована до разового публічного захисту у спеціалізованій вченій раді.

Кандидат економічних наук, доцент Візіренко С.В. звернула увагу на актуальність теми дисертаційного дослідження, його змістовність і наукову новизну, а також ґрунтовність проведеного аналізу та високий рівень володіння здобувачем теоретичним і практичним матеріалом. Було підкреслено, що дисертаційна робота Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня вищої освіти доктора філософії за спеціальністю 073 «Менеджмент», є завершеним і самостійним науковим дослідженням, яке містить науково обґрунтовані результати у сфері менеджменту та може бути рекомендоване до разового публічного захисту у спеціалізованій вченій раді.

Доктор економічних наук, професор Слободянюк О.В. констатувала доцільність та слушність пропозицій та рекомендацій, викладених у дисертаційному дослідженні і зазначила, що дисертація Саврацького Олександра Олександровича «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», подана на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент», відповідає встановленим вимогам і може бути рекомендована до разового публічного захисту у спеціалізованій вченій раді.

На основі результатів обговорення присутніх на міжкафедральному семінарі вирішили запропонувати наступний

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення дисертації Саврацького Олександра Олександровича на тему: «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», поданої на здобуття ступеня доктора філософії з галузі знань 07 «Управління та адміністрування» за спеціальністю 073 «Менеджмент»

Обґрунтування вибору теми дослідження. Актуальність обраної теми зумовлена необхідністю управлінського втручання у вирішення проблеми забезпечення ефективного захисту об'єктів критичної інфраструктури від зростаючих загроз в умовах стрімкого впровадження цифрових технологій. Адже, з одного боку, функціонування ключових сфер життєдіяльності суспільства (енергетики, транспорту, зв'язку, фінансів тощо) дедалі більше залежить від інформаційної складової. З іншого боку, традиційні формалізовані технічні та нормативно-правові заходи кіберзахисту виявляються недостатніми для забезпечення належного рівня цифрової стійкості, що викликає необхідність переходу до комплексних управлінських рішень.

В умовах повномасштабного вторгнення прийшло загальне розуміння того, що протидія кіберзагрозам, особливо коли мова йде про критичну інфраструктуру, виходить за межі суто технічної проблематики і переходить на рівень стратегічного управління. Більш того, навіть успішна локальна модель управління кіберзахистом не завжди відповідає темпам трансформації загроз, адже безпекові рішення швидко втрачають свою актуальність. Відтак, постійний пошук нестандартних рішень, розробка та впровадження управлінських інновацій виступають вже не просто як елемент зміцнення конкурентоспроможності, це – об'єктивна необхідність в сучасних реаліях.

Теоретичними, методологічними, методичними та прикладними аспектами впровадження управлінських інновацій при вирішенні питань безпеки та протидії загрозам, в тому числі кіберзагрозам критичній інфраструктурі, переймалися такі вітчизняні вчені, як Р. Августин, О. Божанова, Т. Васильців, А. Гайдученко, С. Горбаченко, В. Гречанінов, М. Домарацький, Д. Дячков, О. Зачко, В. Зянько, М. Караїм, О. Кібік, Д. Кобилкін, А. Ковальов, М. Копитко, Д.

Котелевець, В. Котлубай, Я. Котляревський, Т. Куклінова, В. Лойко, С. Мельник, Ю. Ольвінська, А. Осокіна, І. Павук, В. Панченко, С. Прохорчук, Є. Рединa, В. Франчук, В. Храпкіна, О. Чепурна, Н. Чухрай, А. Штангрет та інші.

Водночас, проблема інтеграції управлінських інновацій у систему кіберзахисту критичної інфраструктури ще недостатньо висвітлена в наукових дослідженнях. Адже в переважній більшості наукових праць або оглядово розглядається весь комплекс управлінських питань безпеки критичної інфраструктури, або висвітлюються підходи до забезпечення кібербезпеки в технічному або нормативно-правовому аспектах або досліджуються тренди інноваційного управління але без фокусування на завданнях запобігання кіберзагрозам. Вказана ситуація дозволяє стверджувати про наукові перспективи формування окремої гілки досліджень у якій першочергова увага приділятиметься впровадженню управлінських інновацій в безпекові процеси.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційна робота виконана відповідно до планів науково-дослідної роботи Національного університету «Одеська юридична академія» за темою: «Правове і соціальне життя сучасної України у людиноцентристському вимірі в цифрову еру» (державний реєстраційний номер 0122U000266) та кафедри кібербезпеки - за темою «Безпека інформації та її складових в інформаційно-комунікаційних системах». У межах кафедральної теми автор проводив дослідження управлінських аспектів забезпечення безпеки інформації та її складових, на прикладі об'єктів критичної інфраструктури.

Мета і завдання дослідження. Метою дисертаційної роботи є обґрунтування наукових засад та розробка практичного інструментарію впровадження управлінських інновацій у сфері кіберзахисту критичної інфраструктури.

Для досягнення зазначеної мети у дисертації вирішувались такі завдання:

- дослідити науковий базис управління безпековими процесами на основі впровадження інновацій;
- охарактеризувати критичну інфраструктуру як об'єкт управління та систематизувати загрози її функціонуванню з позиції управлінського реагування;
- проаналізувати методичні підходи та міжнародні стандарти управління захистом критичної інфраструктури від кіберзагроз;
- визначити особливості процесу управління кіберзахистом критичної інфраструктури з урахуванням нормативно-правового базису та технологічних можливостей;
- оцінити доступність та управлінську доцільність використання наявних ринкових рішень для кіберзахисту об'єктів критичної інфраструктури;
- проаналізувати механізми управлінського впливу на забезпечення кіберзахисту критичної інфраструктури із застосуванням управлінських інновацій;
- розробити організаційні та інституційні підходи до реалізації інноваційних перетворень в управлінні кіберзахистом критичної інфраструктури;

- обґрунтувати інноваційний управлінський підхід до захисту критичної інфраструктури від кіберзагроз з використанням інструментів штучного інтелекту для підтримки управлінських рішень;
- розробити модель впливу управлінських інновацій на ефективність захисту об'єктів критичної інфраструктури.

Об'єктом дослідження є процес управління захистом критичної інфраструктури від кіберзагроз.

Предметом дослідження є комплекс теоретичних, організаційних, методичних і практичних основ управління кіберзахистом критичної інфраструктури з використанням управлінських інновацій.

Методи дослідження. В дисертаційній роботі використано методи: аналізу та синтезу – для узагальнення наукових джерел, систематизації понять безпеки, інновацій та кібербезпеки з огляду на їхнє використання в управлінських дослідженнях (підрозділи 1.1, 1.2); абстрагування – з метою виділення ключових складових елементів безпеки, таких як фізична, економічна, екологічна та кібербезпека (підрозділ 1.3); порівняльного аналізу – для дослідження кон'юнктури ринку продуктів та послуг кібербезпеки та його окремих сегментів (підрозділ 2.2), а також аналізу нормативно-правової бази та міжнародних стандартів (підрозділи 2.1, 2.2); графоаналітичного («Квадрат потенціалу») – для оцінки управлінської готовності підприємств енергетичної сфери до інтеграції штучного інтелекту, що передбачає ранжування об'єктів дослідження за технологічними, управлінськими, комунікаційними та фінансовими блоками з розрахунком сум місць та довжин векторів (підрозділ 3.2); графічного – для наочного і всебічного відображення результатів проведеного дослідження (розділи 2, 3); абстрактно-логічного – під час проведення теоретичних узагальнень і формування висновків дослідження (висновки до розділів). Застосовано економіко-математичне моделювання раціонального розподілу інвестицій у кіберзахист об'єктів критичної інфраструктури. Для інтерпретації комплементарності заходів запроваджено управлінський індикатор кіберстійкості (підрозділ 3.3).

Теоретичну основу дисертаційного дослідження становлять чинні нормативні документи (Верховної Ради України, Кабінету Міністрів України тощо), актуальна вітчизняна та зарубіжна наукова література, офіційні статистичні дані, аналітичні звіти, фінансова звітність і первинна документація суб'єктів підприємництва, що відносяться до критичної інфраструктури, результати опитування профільних фахівців, інформаційні ресурси мережі Інтернет, матеріали особистих досліджень автора.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших комплексних досліджень теоретико-методичних та практичних засад впровадження управлінських інновацій у сфері захисту критичної інфраструктури України від кіберзагроз у сучасних умовах.

За результатами дисертаційного дослідження отримано наступні результати, що мають наукову новизну:

Вперше:

- розроблено інтегровану модель, яка формалізує взаємозв'язок між організаційною (управлінською), кадровою та технічною складовими системи кіберзахисту та враховує диференційований вплив управлінських інновацій на окремі категорії персоналу (управлінський, технічний, користувачі інформаційних систем) і галузеву специфіку секторів критичної інфраструктури (енергетика, телекомунікації, державне управління). На основі результатів оцінювання запропоновано управлінські рішення для підвищення кіберстійкості об'єктів критичної інфраструктури.

Вдосконалено:

- структуризацію об'єктів критичної інфраструктури, в якій, на відміну від існуючих варіантів, до нормативного показника критичності та рівня інформатизації окремих об'єктів додано управлінський показник організаційної схильності до інновацій, визначений на основі бального методу. В результаті розраховано інтегральний індекс інноваційної пріоритетності і визначено найбільш перспективні складові критичної інфраструктури для подальшого впровадження управлінських інновацій, спрямованих на протидію кіберзагрозам.

- модель оптимізації інвестицій у кібербезпеку на основі адаптації моделі Гордона–Льоба, яка, на відміну від базової версії, інтегрує функцію кіберстійкості об'єктів критичної інфраструктури, що дозволяє інтерпретувати кіберзахист як економічно обумовлений управлінський процес із властивими йому закономірностями зростання граничної ефективності інвестицій до визначеного порогового значення та її подальшого зниження. В результаті менеджмент об'єктів критичної інфраструктури може визначити економічно обґрунтований рівень інвестування у заходи кібербезпеки.

- механізм оцінки управлінських альтернатив при формуванні системи кіберзахисту, який, на відміну від існуючих, при виборі конкретних інструментів передбачає дослідження кон'юнктури ринку продуктів та послуг кібербезпеки із застосуванням методів найменших квадратів та експоненційного згладжування за алгоритмом ETS. Застосування зазначеного механізму дозволяє науково обґрунтовувати рівень доступності та управлінську доцільність придбання готових рішень для забезпечення кібербезпеки критичної інфраструктури.

Набуло подальшого розвитку:

- застосування кластерного підходу для збільшення ефективності протидії кіберзагрозам за допомогою реалізації інноваційних проєктів в сфері кібербезпеки. Запропоновано створення кластеру кібербезпеки, який, на відміну від існуючих, орієнтується не стільки на координацію учасників та інформаційно-комунікаційну підтримку, скільки на інституціоналізацію процесів апробації, впровадження та комерціалізації інноваційних безпекових рішень. В результаті об'єкти критичної інфраструктури у межах новоствореного кластеру можуть виступати замовниками продуктів та послуг кібербезпеки, стейкхолдерами для закладів вищої освіти, інвесторами стартапів безпекового напряму, тестувальниками інноваційних рішень.

- методичний підхід до впровадження інструментів штучного інтелекту в управлінські процеси енергетичної критичної інфраструктури із застосуванням графоаналітичних розрахунків, який, на відміну від існуючих підходів, дозволяє кількісно оцінити рівень готовності управлінської структури до цифрової трансформації системи управління кібербезпекою.

- визначення категорії «менеджмент кібербезпеки» як цілеспрямованого процесу планування, розробки, впровадження та управління комплексом організаційних, технічних і правових заходів, спрямованих на забезпечення сталого та безпечного функціонування життєво важливих об'єктів, а також їхній захист від актуальних і потенційних кіберзагроз, яке, на відміну від існуючих, конкретизує управлінський пріоритет на захисті «життєво важливих об'єктів», тобто, критичної інфраструктури.

- управлінську модель застосування командного підходу для вирішення завдань протидії кіберзагрозам, яка, на відміну від існуючих, передбачає наявність окремої посади менеджера з кібербезпеки, який приймає участь у стратегічному плануванні, відповідає за інтеграцію управлінських і технічних рішень, а також здійснює координацію діяльності команди з аналітика, фахівця з комунікацій та дослідження ринку, фахівців технічного блоку. В результаті сформована команда може швидше адаптуватися до нових безпекових викликів, генерувати інноваційні рішення та ефективно розподіляти ресурси.

- теоретичний підхід до застосування циклу PDCA для управління кіберзахистом критичної інфраструктури, який, на відміну від традиційних підходів, інтегрує принципи проактивності, комплексності та адаптивності. В результаті поєднання безперервного процесного управління із сучасними аналітичними моделями попередження загроз створюються умови для ефективного впровадження інноваційних управлінських рішень.

Практичне значення одержаних результатів полягає в тому, що на основі наукових та практичних матеріалів дослідження запропоновані рекомендації з впровадження управлінських інновацій в діяльність об'єктів критичної інфраструктури, спрямовану на протидію кіберзагрозам. Результати дослідження та пропозиції отримали позитивні відгуки та впроваджені в управлінську практику Державної служби спеціального зв'язку та захисту інформації України, ПАТ «ОДЕСКАБЕЛЬ», КП «Теплопостачання міста Одеси», ТОВ «КІПСОЛІД Україна» а також бізнес-структур, що є членами ГС «Odesa IT Family».

Окремі результати дисертаційної роботи впроваджено в освітній процес Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «Менеджмент та маркетинг інновацій», «Проєктний менеджмент», «Інноваційний менеджмент», «Управління та організаційне забезпечення кібербезпеки», «Цифрові технології в бізнесі».

Апробація результатів дисертації. Положення та висновки дисертаційного дослідження обговорювалися під час розширеного засідання кафедри кібербезпеки Національного університету «Одеська юридична академія». Основні результати дослідження були оприлюднені на: міжнародній

науково-практичній конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.), міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.), VII Міжнародній науково-практичній конференції «Конкурентоспроможна модель інноваційного розвитку економіки України» (м. Кропивницький, 7-8 листопада 2024 р.), міжнародній науково-практичній конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.); III міжнародній науково-практичній конференції «Achievements of Science and Applied Research» (м. Дублін, 21-23 липня 2025), міжнародній науково-практичній конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.).

Публікації. Основні положення дисертаційного дослідження відображено в дванадцяти наукових публікаціях, у тому числі в шести статтях, опублікованих у наукових фахових виданнях, перелік яких затверджено МОН України, одній статті, опублікованій у виданні, включеному до міжнародної наукометричної бази Scopus, а також п'яти тезах доповідей на науково-практичних конференціях.

Список публікацій здобувача за темою дисертації та відомості про апробацію матеріалів дисертації:

Публікації, в яких опубліковані основні наукові результати дисертації:

1. Саврацький О. О. Адаптація системи управління об'єктами критичної інфраструктури до сучасних безпекових викликів. *Трансформаційна економіка*. 2024. №1(06). С. 53–57.

2. Саврацький О. О. Аналіз кон'юнктури ринку продуктів та послуг кібербезпеки. *Науково-виробничий журнал «Бізнес-навігатор»*. 2025. №1. С. 443-449. DOI: https://doi.org/10.32782/business-navigator.78-74

3. Саврацький О.О. Перспективи застосування командного підходу в процесі управління проєктами в сфері кіберзахисту. *Актуальні питання економічних наук.* 2025 № 13. DOI: https://doi.org/10.5281/zenodo.16885042

4. Горбаченко С. А., Саврацький О. О. Transformation of the innovative component of management processes in the context of digitalization. *Приазовський економічний вісник.* 2025. № 3 (43). С. 62-67. DOI: https://doi.org/10.32782/2522-4263/2025-3-11

5. Саврацький О. О., Слатвінська В. М. Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень. *Наука і техніка сьогодні.* 2025. № 8 (49). С. 1704-1716. DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716

6. Саврацький О. О., Чепурна О. Є. Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних системах з урахуванням спадної віддачі інвестицій. *Успіхи і досягнення у науці*. 2026. № 1(23). С. 1305–1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317

7. Соколов А. В., Кілко В. В., Трофименко О. Г., Саврацький О. О. Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об'єктах критичної інфраструктури. *Вісті вищих учбових закладів. Радіоелектроніка.* 2026. DOI: https://doi.org/10.20535/S0021347025040028

Публікації, які засвідчують апробацію матеріалів дисертації та додатково відображають її наукові результати:

1. Саврацький О. О. Критична інфраструктура як об'єкт кіберзахисту. Матеріали Міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. С. 76-78.
2. Саврацький О. О. Особливості підготовки фахівців з кібербезпеки в умовах війни. Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів : матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квітня 2024 р.) / НУ "ОЮА" ; за заг. ред. С. В. Ківалова ; відп. за вип. М. Р. Аракелян. – Одеса : Фенікс, 2024. – С. 905-907.
3. Саврацький О. О. Нормативно-правовий фундамент управління кібербезпекою підприємства. Матеріали VII Міжнародної науково-практичної конференції «Конкурентоспроможна модель інноваційного розвитку економіки України» (м. Кропивницький, 7-8 листопада 2024 р.). Кропивницький, 2024. С. 116-118.
4. Саврацький О. О. Системний підхід при управління кіберризиками в умовах війни. Кібербезпека в сучасному світі: актуальні виклики: матеріали Міжнародної науково-практичної конференції (м. Одеса, 22 листопада 2024 р.). 2024. С. 274-277.
5. Саврацький О. О. Current trends in security management. Третя Міжнародна науково-практична конференція «Achievements of Science and Applied Research» (м. Дублін, Ірландія) 21-23 липня 2025. С. 70-75. DOI: 10.70286/EOSS-21.07.2025

Характеристика особистості здобувача. Саврацький Олександр Олександрович має вищу освіту. У 2010 році закінчив Національну академію Державної прикордонної служби України імені Богдана Хмельницького. В 2015 році закінчив Харківський регіональний інститут Державного управління Національної академії державного управління при Президентові України. Наразі проходить військову службу у Державній прикордонній службі України.

Особистий внесок здобувача. Дисертаційна робота є самостійним і завершеним науковим дослідженням. Усі наукові положення, розроблені рекомендації, пропозиції та висновки, викладені в дисертації, є результатом особистої роботи автора. У тих наукових публікаціях, що виконані у співавторстві та використані в роботі, автором використовуються виключно положення та ідеї, які є наслідком його власних досліджень і розробок.

У статті «Transformation of the innovative component of management processes in the context of digitalization» (пер. «Трансформація інноваційної складової

управлінських процесів в умовах цифровізації». Приазовський економічний вісник. 2025. № 3 (43). С. 62-67. DOI: https://doi.org/10.32782/2522-4263/2025-3-11 автор дослідив вплив цифрових технологій (зокрема, штучного інтелекту Big Data, Інтернету речей, блокчейн, хмарних обчислень) на управлінські процеси та виявив наявні резерви для їхньої оптимізації за рахунок інноваційних підходів, механізмів, інструментів. В подальшому це було деталізовано в самій дисертації, зокрема, в підрозділі 3.2 на прикладі впровадження інструментів штучного інтелекту в управлінські процеси.

У статті «Оптимізація кіберзахисту критичної інфраструктури на основі інноваційних управлінських рішень». Наука і техніка сьогодні. 2025. № 8 (49). С. 1704-1716.DOI: https://doi.org/10.52058/2786-6025-2025-8(49)-1704-1716 автор довів перспективність управлінського втручання в процеси організації кіберзахисту на об'єктах критичної інфраструктури та запропонував основні напрями застосування інноваційних управлінських рішень, які мають допомогти у вирішенні завдань протидії кіберзагрозам.

У статті «Математичне моделювання ефективності інноваційних управлінських рішень у соціально-економічних системах з урахуванням спадної віддачі інвестицій». Успіхи і досягнення у науці. 2026. № 1(23). С. 1305–1317. DOI: https://doi.org/10.52058/3041-1254-2026-1(23)-1305-1317 автор обґрунтував власне припущення, що ефективність кіберзахисту не зростає необмежено зі збільшенням інвестицій, а носить характер поступового насичення, що аналітично проявляється у зменшенні граничного приросту результативності за кожної додаткової одиниці інвестицій. Вказаний висновок знайшов відображення у підрозділах 2.3 та 3.3 дисертації.

У статті «Стеганографічний метод з кодовим управлінням та сліпим декодуванням для цифрових відео, що використовуються на об'єктах критичної інфраструктури». Вісті вищих учбових закладів. Радіоелектроніка. 2026. DOI: https://doi.org/10.20535/S0021347025040028 автор сформулював особливості критичної інфраструктури як середовища для впровадження технологічних інновацій, у подальшому основні з них були проаналізовано в підрозділі 2.1 дисертації.

Оцінка мови та стилю дисертації. Дисертація написана сучасною науковою мовою, стиль викладання відповідає прийнятному у науковій літературі й забезпечує легкість та доступність сприйняття наукових положень, висновків і рекомендацій дисертаційного дослідження.

Дисертація відповідає вимогам 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 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507).

Загальний висновок. Враховуючи викладену інформацію вважаємо, що за своєю актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Саврацького Олександра

Олександровича на тему «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», відповідає спеціальності 073 «Менеджмент», 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 (зі змінами від 08.04.2025, № 426), Вимогам до оформлення дисертації, затвердженими наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40 (зі змінами від 31.05.2019, № 759) та 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 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507) та **рекомендується до захисту на здобуття ступеня доктора філософії з галузі знань 07 «Управління та адміністрування» за спеціальністю 073 «Менеджмент».**

У результаті відкритого голосування усі учасники засідання подали голоси «за». Ніхто із учасників міжкафедрального семінару не проголосував «проти» рекомендації дисертаційної роботи Саврацького Олександра Олександровича до захисту в разовій спеціалізованій вченій раді. Науковий керівник Горбаченко С.А. участі в голосуванні не приймав.

УХВАЛИЛИ:

1. Затвердити висновок про дисертаційне дослідження Саврацького Олександра Олександровича на тему «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», представленої на здобуття ступеня доктора філософії за спеціальністю 073 «Менеджмент».

2. Констатувати, що за актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною цінністю здобутих результатів дисертація Саврацького Олександра Олександровича відповідає спеціальності 073 «Менеджмент» 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 (зі змінами від 08.04.2025, № 426), Вимогам до оформлення дисертації, затвердженими наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40 (зі змінами від 31.05.2019, № 759) та 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 12.01.2022 р. № 44 (зі змінами від 03.05.2024, № 507).

3. Рекомендувати дисертацію Саврацького Олександра Олександровича на тему «Впровадження управлінських інновацій у сфері захисту критичної інфраструктури від кіберзагроз», до захисту на здобуття ступеня доктора

філософії у разовій спеціалізованій вченій раді за спеціальністю 073 «Менеджмент».

4. Запропонувати Вченій раді наступний склад разової спеціалізованої вченої ради для проведення публічного захисту:

Голова: завідувач кафедри економіки та менеджменту, д.е.н, професор Кібік Ольга Миколаївна;

Опонент: завідувач кафедри менеджменту авіаційної діяльності Української державної льотної академії, д.е.н., професор Панченко Володимир Анатолійович.

Опонент: завідувач кафедри статистики та математичних методів в економіці Одеського національного економічного університету, к.е.н., доцент Ольвінська Юлія Олегівна;

Рецензент: доцент кафедри економіки та менеджменту Національного університету «Одеська юридична академія», к.е.н., доцент Котлубай Вячеслав Олексійович;

Рецензент: доцент кафедри штучного інтелекту та математичного моделювання Національного університету «Одеська юридична академія», к.е.н., доцент Куклінова Тетяна Вікторівна.

Результати голосування присутніх на засіданні докторів та кандидатів наук за профілем поданої на розгляд дисертації: за – 11; проти – немає; утримались – немає; науковий керівник участі у голосуванні не приймав.

Головуюча на засіданні,
професор кафедри економіки
та менеджменту
Національного університету
«Одеська юридична академія»,
доктор економічних наук, професор **Ольга СЛОБОДЯНЮК**