ЗАТВЕРДЖУЮ

Ректор Національного аерокосмічного університету «ХАІ»

Олексій ЛИТВИНОВ

«__» _____ 2026 р.

ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» для здобуття наукового ступеня доктора наук з державного управління зі спеціальності 25.00.02 – механізми державного управління

Науковий рівень дисертації Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» відповідає діючим вимогам до атестації здобувачів ступеня доктора наук, а саме «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого постановою КМУ від 17.11.2021 р. № 1197, а також науковому паспорту спеціальності 25.00.02 – механізми державного управління.

Дисертація Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» є кваліфікаційною науковою працею, виконаною особисто здобувачем, характеризується єдністю змісту, має встановлену вимогами структуру: анотацію, вступ, п'ять розділів, висновки, список використаних джерел, додатки, та містить наукові положення, що мають новизну і значущість у галузі державного управління, зокрема у напрямі теоретичного обґрунтування та науково-практичному аналізі механізмів реалізації інформаційної безпеки у системі публічного управління, визначенні їх стратегічних цілей і функціонального призначення,

а також у з'ясуванні особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період.

Актуальність теми дослідження. На сучасному етапі інформаційна безпека держави є фундаментальною складовою публічного управління, яка забезпечує захист її стратегічних інтересів як на внутрішньому національному, так і на міжнародному рівнях. У контексті публічного управління інформаційна безпека виступає як самостійний управлінський конструкт, що охоплює: захищеність, доступність, цілісність та конфіденційність інформаційних ресурсів, якими оперує держава; спрямування та координацію національного інформаційного простору з метою забезпечення його інформаційної гігієни.

Інформаційна безпека в системі публічно-управлінського забезпечення має чітко визначену структуру, модель, а також потребує ефективних механізмів реалізації та системної суб'єктності. Для цілей нашого дослідження є доцільним зосередити увагу на аналізі механізмів правового забезпечення та управлінської практики, застосовуючи порівняльний підхід на прикладі України та країн-партнерів (зокрема, ЄС та США).

Затребуваність тематики дослідження механізмів реалізації інформаційної безпеки у системі публічного управління особливо гостро проявилася в умовах повномасштабного вторгнення рф в Україну (з 24.02.2022 р.). Ця агресія спричинила безпрецедентні виклики для сфери інформаційної безпеки як ключового складника безпеки національної.

У зв'язку з цим, актуальним є огляд управлінської діяльності профільних органів, які відповідають за забезпечення інформаційної гігієни та безпеки держави в умовах воєнного стану: Міністерство культури України; Рада національної безпеки і оборони України (РНБО) та підпорядкований їй Центр протидії дезінформації; Кабінет Міністрів України (як головний суб'єкт управління).

Окремим завданням є дослідження нормативно-правового інструментарію, який використовується цими органами та інституціями для формування та підтримки безпечного інформаційного простору.

Аналіз наукових праць підтверджує, що проблематика механізмів реалізації інформаційної безпеки та її стратегічних цілей є об'єктом пильної уваги фахівців у галузях публічного управління та адміністрування, права, політології та філософії.

Теоретико-методологічні засади, структура правового механізму, міжнародна практика та аналіз загроз є предметом досліджень таких вітчизняних та іноземних вчених, як: Л. Кочубей, А. Войціховський, О. Олійник, П. Діхтієвський, З. Гбур, Н. Цибульник, В. Торічний, У. Ільницька, В. Панченко, І. Боднар, О. Архипов, В. Шемчук, І. Валюшко, Л. Мазуренко, І. Поліщук, І. Ломака, В. Шишко, В. Горовий, С. Петренко, Н. Назаренко, Є. Рогова, К. Захаренко, Т. Амро, Б. Кормич та інші; Б. Гудмен, Г.Г. Фостер, Т. Фітцджералд, М. Фазілда, Дж. Грамма, С. Кайпак, К. Кіфер, М. Камаріоту, Т. Лідтке, Д. Маркополу, В. Лонг, М. Мерков, Г. Паананен, Н. Ріпсмен, Н. Робертс, А. Сахід, М. Шумейкер, С. Штітцлейн та ін.

Незважаючи на достатньо велику загальну кількість робіт з проблем механізмів реалізації інформаційної безпеки держави, потребують вирішення наукові питання щодо: комплексної розробки та обґрунтування інтегративної моделі механізмів реалізації інформаційної безпеки у системі публічного управління України, яка б поєднувала інституційно-правовий, комунікаційно-стратегічний та міжсекторальний аспекти в умовах гібридних загроз та викликів воєнного часу; формування цілісної концепції стратегічного управління інформаційною безпекою, що включає діагностику управлінських обмежень та розробку науково обґрунтованих напрямів удосконалення функціоналу ключових суб'єктів (РНБО, Центр протидії дезінформації; Кабінет Міністрів України) з урахуванням сучасного міжнародного досвіду.

Потреба у теоретичному, методологічному та практичному вирішенні окреслених завдань підтверджує актуальність дослідження, його наукову новизну та зумовлює мету, завдання, предмет і об'єкт роботи.

Мета дослідження полягає у теоретичному обґрунтуванні та науково-практичному аналізі механізмів реалізації інформаційної безпеки у системі публічного управління, визначенні їх стратегічних цілей і функціонального призначення, а також у з'ясуванні особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період.

Реалізація визначеної мети зумовила постановку й вирішення наступних завдань :

–обґрунтувати та розробити інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України;

–уточнити теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління;

–обґрунтувати підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління;

–систематизувати та концептуалізувати методологічні засади дослідження інформаційної безпеки у системі публічного управління;

–розкрити сутнісні характеристики механізму правового регулювання інформаційної безпеки;

–систематизувати та науково обґрунтувати методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії;

–розробити концептуальну модель переходу до адаптивної архітектури забезпечення інформаційної безпеки;

–розвинути теоретичні засади стратегічного управління інформаційною безпекою;

–узагальнити та систематизувати сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави;

–обґрунтувати теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки;

–розробити та науково обґрунтувати стратегію-модель національної цифрової стійкості України.

Об'єкт дослідження — інформаційна безпека держави як система суспільних відносин у сфері публічного управління.

Предмет дослідження — механізми реалізації інформаційної безпеки у системі публічного управління.

Методи дослідження. Методологічну основу проведеного дослідження становить сукупність взаємопов'язаних загальнонаукових і спеціалізованих підходів, серед яких застосовано системний, історико-ретроспективний, компаративний, структурно-функціональний методи, а також методи аналізу й синтезу, узагальнення та класифікації, індуктивного й дедуктивного мислення, принципи взаємозв'язку частини та цілого, проблемного і прогностичного аналізу. Застосування історико-ретроспективного методу дало змогу здійснити концептуалізацію термінологічного та категоріального апарату поняття «інформаційна безпека» в межах системи національної безпеки [параграф 1.1]. У свою чергу, через узагальнення й систематизацію вітчизняних наукових джерел було проаналізовано інформаційну безпеку як багатовимірну систему суспільних відносин і водночас — як об'єкт правової охорони [параграф 1.2], а також виокремлено ключові методологічні орієнтири для подальшого дослідження даного феномену [параграф 1.3].

Системний та структурно-функціональний підходи надали можливість розкрити сутність та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки, концептуалізувавши нормативні особливості такого процесу та систему суб'єктів забезпечення інформаційної безпеки [параграф 2.1; параграф 2.2; параграф 2.3]. Використання емпіричних методів, індукції й дедукції забезпечило розкриття сутності, мети та особливостей стратегічного управління забезпеченням інформаційної безпеки [параграф 3.1]. Метод моделювання дозволив сформувати концепцію

розвитку інформаційної безпеки держави та розробити відповідну Стратегію-модель національної цифрової стійкості [параграф 5.3]. Завдяки проблемному й прогностичному підходам проаналізовано глобальний характер інформаційної безпеки крізь призму інституційних можливостей та ризиків, а також комунікаційну стратегію як складову національного управління інформаційною безпекою та, на додаток, класифіковано загрози інформаційній безпеці України і систематизовано методичні підходи протидії загрозам інформаційній безпеці України.

Наукова новизна дисертаційної роботи й отриманих результатів полягає у комплексному теоретичному обґрунтуванні стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки (ІБ) у системі публічного управління як автономного, системно організованого феномену в контексті сучасних трансформаційних викликів. Найбільш вагомими науковими результатами дисертаційного дослідження є такі:

уперше

–обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури України); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства;

–обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії

гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам);

–розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення;

удосконалено

– підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб'єктів — Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) — виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку

функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб'єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція);

–концептуалізацію сутнісного призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванадцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри;

–систематизацію та наукове обґрунтування методичних підходів протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft;

–концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію інформаційної безпеки на засадах прозорості та гласності та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування);

дістали подальшого розвитку:

–поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів:

інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб'єкти: держава, громадянське суспільство, бізнес; об'єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб'єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об'єктів правової охорони;

–систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики;

–теоретичні засади стратегічного управління інформаційною безпекою (ІБ) шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ);

узагальнено та систематизовано перелік сучасних викликів та тенденцій розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні

мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів)

Практичне значення одержаних результатів. Основні ідеї та висновки дослідження доведено до конкретних положень, методик і рекомендацій. Вони можуть бути використані у практичній діяльності органами публічного управління на національному й регіональному рівнях, підприємствами, громадськими організаціями.

Результати дисертації були впроваджені у діяльність Національної акціонерної компанії «Надра України» (довідка про впровадження НАК «Надра України»). Зокрема, розроблені у межах дослідження рекомендації використані для удосконалення механізмів захисту інформаційного простору національної акціонерної компанії, забезпечення кіберстійкості державних підприємств та протидії інформаційним загрозам в умовах воєнного стану. Результати наукового дослідження були впроваджені у діяльність Національного агентства кваліфікацій в таких напрямах: оцінка ризиків у сфері кваліфікаційної безпеки (інтегровано методику класифікації інформаційних загроз та ризиків в регламенти роботи із даними Реєстру кваліфікацій); модернізація аналітичних систем (алгоритми прогнозування загроз, запропоновані в дисертації, стали основою вдосконалення цифрової інфраструктури аналітичних модулів); оновлення професійних стандартів (наукові положення використано при оновленні кваліфікаційних вимог для фахівців з кібербезпеки, зареєстрованих у Національному реєстрі кваліфікацій); аналітична підтримка державної політики (висновки дисертації включено до експертних матеріалів щодо гармонізації українських кваліфікаційних норм з європейськими рамками) (довідка Національного агентства кваліфікацій від 22.07.2025 р. № 01/01.01-06/1647).

Результати дисертації були впроваджені у діяльність Департаменту кадрової політики Міністерства оборони України (довідка про впровадження

Департаменту кадрової політики Міністерства оборони України). Зокрема, розроблені у межах дослідження автора рекомендації використані для удосконалення механізмів захисту інформаційного простору департаменту та протидії інформаційним загрозам в умовах воєнного стану.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії та розділи в колективних монографіях:

1. Загородня А.С., Котляров В. Управління економічною безпекою: стратегічні цілі та механізми реалізації. Київ: Національний університет біоресурсів і природокористування, 2024. 200 с. *Особистий внесок: розроблено механізми управління економічною безпекою в системі публічного управління.*

Статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

2. Zbarsky, V.K., Reznik, N.P., Ostapchuk, A.D., Alekseieva, K.A., Kotliarov, V.O. (2025). Institutional and Informational Prerequisites of Secure Development of Farms in the Agrarian Economy Model of Ukraine. In: Alareeni, B., Elgedawy, I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 546. Springer, Cham. https://doi.org/10.1007/978-3-031-65207-3_53. Особистий внесок: розроблено концептуальну модель інформаційної безпеки аграрних господарств, адаптованої до умов цифрової трансформації та європейських стандартів.

3. Rogovskii, I., Kotliarov, V., Bondarenko, V., Havrylyuk, V., Gaojiang, C., Zehao, L. (2024). Engineering and Security Management of Smart Technology of Agrotronics of Crop Production. In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer,

Cham. https://doi.org/10.1007/978-3-031-75960-4_10 Особистий внесок: формалізовано ризики кібербезпеки в агротехнологічних системах та розробці алгоритмів управління інформаційними загрозами в агровиробництві.полягає у формалізації ризиків інформаційної безпеки в агротрониках.

4. Cherep A., Voronkova V., Cherep O., Ohrenych Y., Dashko I., Kotliarov V. (2024). Impact of Artificial Intelligence on the Level of Socio-Economic Security of Ukraine in the Conditions of Current European Integration Challenges. In: Alareeni, B., Hamdan, A. (eds) Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation. ICBT 2024. Lecture Notes in Networks and Systems, vol 1082. Springer, Cham. https://doi.org/10.1007/978-3-031-67434-1_30. Особистий внесок: визначено критичні точки впливу штучного інтелекту на соціально-економічну стабільність України та розробці рекомендацій щодо інформаційного захисту.

5. Kotliarov V.O., Kovalchuk O.V., Kovalchuk O.V., Kovalchuk T.V., Kovalchuk O.V. Study of Structural Imbalances in Agricultural Engineering. E3S Web of Conferences. 2022. Vol. 363. Article 01037. URL: https://doi.org/10.1051/e3sconf/202236301037. Особистий внесок: виявлено інформаційні дисбаланси у системах агроінжинірингу та обгрунтуванні напрямів їх оптимізації з точки зору стратегічної безпеки.

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

6. Котляров В.О. Еволюція міжнародно-політичної взаємодії у сфері інформаційних відносин. Публічне управління і адміністрування в Україні. 2023. Вип. 37. С. 76–81. DOI: 10.32782/pma2663-5240-2023.37.14

7. Котляров В.О. Комплексний підхід щодо розуміння інформаційної безпеки. Публічне управління і адміністрування в Україні. 2023. Вип. 38. С. 168–172. DOI https://doi.org/10.32782/pma2663-5240-2023.38.30

8. Котляров В.О. Особливості категорії «Інформаційна безпека» у міжнародному контексті. Наукові праці МАУП. Політичні науки та публічне

управління. 2023. № 4(70). С. 21–26. DOI: 10.32689/2523-4625-2023-4(70)-3

9. Котляров В.О. Система забезпечення інформаційної безпеки України. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 2(74). С. 40–44. DOI: 10.32689/2523-4625-2024-2(74)-6

10. Котляров В.О. Інформаційне забезпечення безпеки вітчизняної та світової спільноти. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 45–52. DOI: 10.32689/2523-4625-2024-1(73)-6

11. Котляров В.О. Теоретичні засади сутності та концепції інформаційної безпеки. Наукові перспективи. 2023. № 6(36). С. 131–142. DOI: 10.52058/2708-7530-2023-6(36)-131-142

12. Котляров В.О. Формування державної політики кібергігієни. Наукові перспективи. 2025. № 7(61). С. 162–174. DOI: 10.52058/2708-7530-2025-7(61)-162-174

13. Котляров В.О. Категоріальний апарат інформаційної безпеки. Суспільство та національні інтереси. 2025. № 8(16). С. 615–629. DOI: 10.52058/3041-1572-2025-8(16)-615-629

14. Котляров В.О. Стратегічні цілі інформаційної безпеки: державне планування та механізми моніторингу ефективності. Національні інтереси України. 2025. № 8(13). С. 903–914. DOI: 10.52058/3041-1793-2025-8(13)-903-914%20

15. Котляров В.О. Інформаційна безпека України: цілі, механізми та адаптація до стандартів ЄС і НАТО. Наукові інновації та передові технології. 2025. № 8(48). С. 180–192. DOI: 10.52058/2786-5274-2025-8(48)-180-192

16. Котляров В.О. Інформаційна безпека як система правовідносин: теоретико-правовий вимір. Актуальні питання у сучасній науці. 2025. № 8(38). С. 245–259. DOI: 10.52058/2786-6300-2025-8(38)-245-259

17. Котляров В.О. Механізми раннього виявлення інформаційних атак: роль штучного інтелекту в прогнозуванні. Успіхи і досягнення у науці. 2025. № 8(18). С. 443–455. DOI: 10.52058/3041-1254-2025-8(18)-443-455

18. Котляров В.О. Інформаційна безпека в умовах глобальної взаємозалежності: міжнародно-правовий контекст та стратегічні практики.

Успіхи і досягнення у науці. 2025. № 7(17). С. 474–486. DOI: 10.52058/3041-1254-2025-7(17)-474-486

19. Котляров В.О. Механізми управління репутаційними ризиками у державній інформаційній політиці. Суспільство та національні інтереси. 2025. № 9(17). С. 624–637. DOI: 10.52058/3041-1572-2025-9(17)-624-637

20. Котляров В.О. Методологічні засади дослідження інформаційної безпеки в умовах трансформаційних викликів. Наукові інновації та передові технології. 2025. № 9(49). С. 187–199. DOI: 10.52058/2786-5274-2025-9(49)-187-199

21. Котляров, В.О. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2023, 5(71), 46-54. DOI: 10.32689/2523-4625-2023-5(71)-6

22. Котляров В.О. Правовий механізм забезпечення інформаційної безпеки: структура, принципи та інституційна модель України. Наукові перспективи. 2025. № 8 (62). С. 907-919. DOI: 10.52058/2708-7530-2025-8(62)-907-919.

23. Котляров В.О. Проблеми інформаційної боротьби у контексті забезпечення національних інтересів. Наукові інновації та передові технології. 2023, № 1(15), DOI: 10.52058/2786-5274-2023-1(15)-499-51

Статті в інших періодичних виданнях України

24. Котляров, В.О. Стратегічне управління інформаційною безпекою України. Київський економічний науковий журнал, 2024, 6, 66-69. DOI: 10.32782/2786-765X/2024-6-9

25. Котляров В.О. Стратегічне управління безпекою організацій. Mechanism of an Economic Regulation, 2024, 1 (103), 41-45. DOI: 10.32782/mer.2024.103.06

26. Котляров В.О. Особливості державної системи стратегічного планування національної безпеки в умовах інформатизації суспільства. Український журнал прикладної економіки та техніки. Том 7, № 4, 2022, С. 225–

233. DOI: 10.36887/2415-8453-2022-4-33.

27. Котляров В.О. Стратегічна безпека підприємства: підходи, особливості, механізм та проблеми забезпечення. Український журнал прикладної економіки та техніки. 2022. №3. 214-222 pp. DOI: 10.36887/2415-8453-2022-3-29.

28. Котляров В.О. Поняття стратегічного управління національною безпекою. Український журнал прикладної економіки та техніки. 2023. №1. 159-165 pp. DOI: 10.36887/2415-8453-2023-1-23

29. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. Український журнал прикладної економіки та техніки. 2023. №2. 314-321 pp. DOI: 10.36887/2415-8453-2023-2-45

30. Bytov V., Horbach L., Kotliarov V.O. Production as a Main Source of Consumer Goods to Society in the Current Environment. Economic Forum. 2022. Vol. 12, No. 3. P. 138–144. DOI: 10.36910/6775-2308-8559-2022-3-18. Особистий внесок: розроблено аналітичну модель взаємозв'язку між виробничими процесами та рівнем забезпечення суспільства споживчими товарами, з урахуванням інформаційно-економічних чинників сучасного середовища.

31. Котляров В.О. Механізм стратегічного управління економічною безпекою підприємства. Наука та освіта як основа модернізації світоустрою, 2023, № 25-01, с. 183–194. DOI: 10.30890/2709-2313.2023-25-00-024

32. Котляров, В.О. Принципи управління безпекою організацій. Mechanism of an Economic Regulation, 2023, 4 (102), 25-28. DOI: 10.32782/mer.2023.102.04

Тези конференцій:

33. Kotliarov V.O. Strategic Security of the Enterprise. 3rd International Conference on Corporation Management (ICCM-2023). 29.06.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICCM/ICCM-2023/paper/view/547

34. Reznik N.P., Kotliarov V.O. Information Security: Challenges to the Global Information Society. ICEAF-2023. 15.12.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2023/paper/view/696.

Особистий внесок: класифіковано глобальні виклики інформаційній безпеці та формуванні аналітичної моделі оцінки їх впливу на міжнародні інститути.

35. Reznik N.P., Kotliarov V.O. Особливості системи забезпечення стратегічної безпеки компанії. II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology». 15–17.11.2023. Варшава, Польща. URL: https://isu-conference.com/en/archive/modern-approaches-to-problem-solving-in-science-and-technology; PDF. Особистий внесок: розроблено структурну модель корпоративної інформаційної безпеки з урахуванням репутаційних ризиків.

36. Reznik N.P., Kotliarov V.O. Аспекти державної системи стратегічного планування національної безпеки України. III International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research». 29.11–01.12.2023. Амстердам, Нідерланди. URL: https://isu-conference.com/en/archive/collective-thinking-unifying-scientific-approaches-in-multifaceted-research; PDF. Особистий внесок: змоделювано інформаційний компонент державної системи стратегічного планування та обґрунтуванні його ролі в національній безпеці.

Наукове дослідження з комплексного теоретичного обґрунтування стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки (ІБ) у системі публічного управління як автономного, системно організованого феномену в контексті сучасних трансформаційних викликів, як окремої наукової проблеми, виконано самостійно, з використанням останніх досягнень галузі науки державного управління. Теоретичні положення та висновки обґрунтовано на основі особистих досліджень автора у сфері теорії та практики державного управління, механізмів реалізації інформаційної безпеки у системі публічного управління України, аналізу відповідної вітчизняної та зарубіжної літератури, а також нормативно-правової бази, що регулює окремі питання проблематики дослідження. При використанні наукових доробків інших учених для обґрунтування власних міркувань автора на них зроблено відповідні

посилання. Особистий внесок дисертанта у колективні наукові роботи конкретизовано у списку праць здобувача, наведеному вище.

Запропоновано офіційних опонентів, які є провідними фахівцями із заявленої спеціальності та тематики дисертаційної роботи:

ПомазаПономаренко Аліна Леонідівна, доктор наук з державного управління, професор, завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту навчально-наукового інституту цивільного захисту Національного університету цивільного захисту України;

Антонова Людмила Володимирівна, доктор наук з державного управління, професор, професор кафедри обліку і аудиту Чорноморського національного університету імені Петра Могили;

Щепанський Едуард Валерійович, доктор наук з державного управління, професор, завідувач кафедри публічного управління та адміністрування Хмельницького університету управління та права імені Леоніда Юзькова.

Загальний висновок. За актуальністю, ступенем наукової новизни, обґрунтованості, теоретичного та практичного значення здобутих результатів дисертаційна робота Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» відповідає спеціальності 25.00.02 – механізми державного управління та вимогам до дисертацій на здобуття наукового ступеня доктора наук, а саме вимогам пунктів 7, 8, 9 Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою КМУ від 17.11.2021 р. № 1197.

Автор роботи, Котляров Валерій Олександрович, може бути представлений до публічного захисту наукових досягнень у формі дисертації на здобуття ступеня доктора наук за спеціальності 25.00.02 – механізми державного управління .

Рекомендувати дисертацію Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» для здобуття наукового ступеня доктора наук з державного

управління за спеціальністю 25.00.02 – механізми державного управління в спеціалізованій вченій раді для попереднього розгляду і захисту.

Рецензенти:

Доктор наук з державного управління, доцент — Діна ТЮРІНА

Доктор наук з державного управління, професор — Вікторія ШВЕДУН

Доктор наук з державного управління, професор — Андрій ДЄГТЯР