

## **ВІДГУК**

офіційного опонента доктора наук з державного управління, професора Антонової Людмили Володимирівни на дисертацію Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління», подану на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління

### **Актуальність теми дисертаційного дослідження**

Динаміка сучасного державотворення переконливо засвідчує, що інформаційна безпека дедалі менше може розглядатися як допоміжний технічний або вузькосекторальний напрям діяльності держави. У цифровому суспільстві інформаційні потоки, дані, комунікаційні платформи, алгоритмічні сервіси та мережеві взаємодії безпосередньо впливають на якість управлінських рішень, довіру до публічних інституцій, функціонування критичної інфраструктури, стійкість громад, економічну безпеку та здатність держави реалізовувати свої стратегічні пріоритети. Саме тому дослідження механізмів реалізації інформаційної безпеки у системі публічного управління є своєчасним і таким, що відповідає ключовим викликам розвитку України.

Особлива значущість теми зумовлена тим, що Україна вже тривалий час перебуває під впливом не лише військової, а й комплексної інформаційної агресії. Дезінформаційні кампанії, маніпулятивні інформаційно-психологічні операції, кібератаки, використання соціальних мереж для радикалізації суспільних настроїв, спроби підриву легітимності органів влади та дискредитації європейського й євроатлантичного вибору України актуалізують потребу у науково обґрунтованій системі публічно-управлінських рішень. За таких умов інформаційна безпека стає не лише складовою національної безпеки,

а й умовою безперервності державного управління, захисту демократичного ладу та збереження суспільної консолідації.

Водночас воєнний стан, швидке оновлення технологій, зростання ролі штучного інтелекту, великих даних, цифрових платформ і транскордонних комунікацій створюють для органів публічної влади завдання нового рівня складності. Йдеться не лише про реагування на вже виявлені загрози, а про формування прогнозної, адаптивної та багаторівневої системи управління, здатної забезпечувати інформаційну стійкість держави, суспільства й окремої людини. У цьому контексті дисертація Котлярова В.О. є актуальною, оскільки спрямована на пошук збалансованої моделі поєднання правових, інституційних, організаційних, комунікаційних, освітніх і міжсекторальних інструментів реалізації інформаційної безпеки.

Актуальність дисертаційного дослідження також визначається необхідністю подальшого розвитку науки державного управління у частині осмислення інформаційної безпеки як складної системи суспільних відносин. Потребують наукового уточнення межі компетенції суб'єктів забезпечення інформаційної безпеки, механізми координації між органами сектору безпеки і оборони, інституціями цифрової трансформації, гуманітарними органами, приватним сектором та громадянським суспільством. Важливими залишаються питання адаптації міжнародних практик, гармонізації з європейськими підходами, підвищення медіаграмотності, забезпечення прозорості державних рішень та збереження балансу між безпековими потребами і правами людини. Саме такі аспекти становлять предметний центр дисертації та підтверджують її наукову і практичну значущість.

### **Зв'язок роботи з науковими програмами, планами, темами**

Дисертацію виконано в межах науково-дослідної роботи Національного аерокосмічного університету «Харківський авіаційний інститут» за темою

«Механізми реалізації інформаційної безпеки у системі публічного управління» (2025–2026). У межах зазначеної тематики здобувачем опрацьовано теоретико-методологічні засади забезпечення інформаційної безпеки в умовах глобалізації, розкрито структуру механізму правового забезпечення інформаційної безпеки в Україні, узагальнено міжнародні норми та практики, охарактеризовано сучасні загрози інформаційній безпеці України, а також запропоновано стратегію-модель національної цифрової стійкості України. Такий зміст дослідження свідчить про його відповідність профілю наукової роботи установи та про спрямованість на вирішення актуальної науково-прикладної проблеми галузі державного управління.

### **Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації**

Мета дисертаційного дослідження сформульована як теоретичне обґрунтування та науково-практичний аналіз механізмів реалізації інформаційної безпеки у системі публічного управління, визначення їх стратегічних цілей і функціонального призначення, а також з'ясування особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період. Її досягнення забезпечено через послідовне вирішення комплексу завдань, пов'язаних із розробленням інтегративної моделі механізмів реалізації інформаційної безпеки, уточненням теоретико-методологічних засад, обґрунтуванням інституційного механізму, розкриттям правового регулювання, аналізом протидії загрозам в умовах військової агресії, формуванням адаптивної архітектури забезпечення інформаційної безпеки, розвитком стратегічного управління та обґрунтуванням стратегії-моделі національної цифрової стійкості України.

Об'єктом дослідження визначено інформаційну безпеку держави як систему суспільних відносин у сфері публічного управління, предметом –

механізми реалізації інформаційної безпеки у системі публічного управління. Зазначене співвідношення об'єкта і предмета є виправданим, оскільки дає змогу розглядати інформаційну безпеку не фрагментарно, а як управлінську систему, що охоплює правові норми, інституційні зв'язки, організаційні процедури, технологічні рішення, комунікаційні практики та взаємодію держави з недержавними акторами.

Методологічну основу дисертації становить поєднання системного, історико-ретроспективного, компаративного, структурно-функціонального, проблемного і прогностичного підходів, а також методів аналізу, синтезу, узагальнення, класифікації, індукції та дедукції. Завдяки такому інструментарію автор зміг розкрити інформаційну безпеку як багатовимірний феномен публічного управління, визначити її правову та інституційну природу, порівняти зарубіжні моделі управління, виявити особливості української практики й запропонувати напрями удосконалення відповідних механізмів.

Наукові положення, висновки і рекомендації дисертації є достатньо аргументованими. Вони спираються на аналіз широкого кола наукових джерел, нормативно-правових актів, міжнародних підходів, практик діяльності суб'єктів публічного управління, а також на узагальнення загроз, що актуалізувалися в умовах повномасштабної війни. Висновки за розділами і загальні висновки кореспондують із поставленими завданнями, відображають зміст проведеного дослідження та характеризують авторський підхід до формування цілісної архітектури інформаційної безпеки у системі публічного управління.

Позитивної оцінки заслуговує прагнення здобувача поєднати стратегічний, правовий, інституційний та комунікаційний виміри інформаційної безпеки. У роботі простежується усвідомлення того, що ефективність відповідних механізмів залежить не лише від нормативного закріплення повноважень, а й від здатності суб'єктів публічного управління координувати дії, прогнозувати ризики, підтримувати довіру суспільства, залучати приватний

сектор і громадськість, а також адаптувати міжнародний досвід до українських умов.

### **Наукове значення дисертаційного дослідження, достовірність і новизна наукових положень**

Дисертаційна робота побудована логічно та охоплює ключові блоки проблематики: теоретико-методологічне осмислення інформаційної безпеки, характеристику правових та інституційних механізмів, аналіз стратегічного управління, систематизацію сучасних загроз, порівняння управлінських моделей і розроблення стратегії-моделі національної цифрової стійкості України. Структура дослідження дає змогу простежити рух авторської думки від загальної концептуалізації інформаційної безпеки до формування конкретних управлінських пропозицій.

Наукова новизна результатів полягає у комплексному теоретичному обґрунтуванні стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки у системі публічного управління як автономного, системно організованого феномену. Серед найбільш вагомих результатів слід відзначити розроблення інтегративної моделі механізмів реалізації інформаційної безпеки в Україні, яка поєднує міжсекторальний і комунікаційно-стратегічний підходи, удосконалену інституційно-правову конструкцію ключових суб'єктів, критерії функціональної діагностики управлінських обмежень в умовах воєнного стану та концепцію стратегічного управління інформаційною безпекою.

Науково значущим є поглиблення теоретико-методологічних засад дослідження інформаційної безпеки як системи суспільних відносин та як об'єкта правової охорони. Автор структурує суб'єктний, об'єктний, регулятивний та інституційний виміри цієї сфери, звертає увагу на роль держави, громадянського суспільства, бізнесу, інформаційного середовища,

громадянської участі, інформаційної грамотності, етики й відповідальності. Такий підхід має значення для розвитку категоріального апарату науки державного управління.

Важливим результатом дисертації є обґрунтування підходів до інституційного механізму забезпечення інформаційної безпеки. Здобувач запропонував багатofункціональну архітектурну модель взаємодії Служби безпеки України, Ради національної безпеки і оборони України, Міністерства цифрової трансформації України та інших суб'єктів у межах співвідношення «моніторинг – координація – впровадження». Це дозволяє розглядати забезпечення інформаційної стійкості не як суму ізольованих повноважень, а як систему взаємопов'язаних функцій.

Новизна роботи проявляється також у концептуалізації механізму правового регулювання інформаційної безпеки через поєднання регулювання інформаційної діяльності, розвитку інформаційного середовища, гарантування права людини на інформацію та закріплення принципів законності, захисту прав і свобод, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, пропорційності, відповідальності й безперервності. Такий результат має теоретичне значення для подальшого формування правової моделі інформаційної безпеки в Україні.

Суттєвим внеском є систематизація методичних підходів до протидії загрозам інформаційній безпеці України в умовах військової агресії. Автор виокремлює нормативно-правові та організаційні механізми, технічні засоби кіберзахисту, інформаційно-психологічну безпеку, освітні ініціативи з підвищення цифрової грамотності та міжнародну співпрацю. Комплексне поєднання цих складників дає змогу розглядати протидію загрозам як багаторівневу управлінську діяльність, а не лише як реагування спеціалізованих безпекових органів.

Заслуговує на увагу розроблена концептуальна модель переходу до адаптивної архітектури забезпечення інформаційної безпеки. Її трирівнева структура – стратегічний, оперативний і тактичний рівні – дозволяє узгодити прогнозування, сценарне планування, міжвідомче реагування та локальні алгоритми дій. Такий підхід відповідає потребам управління в умовах мінливого безпекового середовища, де традиційні лінійні моделі часто не забезпечують достатньої швидкості й гнучкості.

Окрему наукову цінність становить аналіз міжнародних моделей стратегічного управління інформаційною безпекою. На основі досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю автор виокремлює правове регулювання, інституційну структуру, міжнародну співпрацю та інноваційні технології як ключові параметри відповідних систем. Порівняльний аналіз дає можливість не копіювати зарубіжні практики механічно, а використовувати їх як аналітичну основу для адаптації до українських інституційних умов.

У дисертації розкрито сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави. До позитивних аспектів роботи належить системний розгляд глобально-політичних, технологічних і соціально-комунікаційних ризиків, зокрема гібридних війн, дезінформації, інформаційної асиметрії, штучного інтелекту, Big Data, deepfake-технологій, алгоритмічних процесів цифрових платформ і соціальних мереж. Автор обґрунтовує необхідність поєднання поведінкового, освітнього, інституційного та правового вимірів протидії ризикам.

Вагомим підсумковим результатом є стратегія-модель національної цифрової стійкості України, яка представлена як інтегральна трирівнева система із залученням державного управління, приватного сектору і громадянського суспільства. У моделі акцентовано принципи проактивності, багаторівневої координації, гнучкості та демократичного контролю, що дає підстави оцінювати

її як науково обґрунтовану спробу переходу від реактивного до прогнозно-превентивного управління інформаційною безпекою.

### **Значення одержаних результатів для науки й практики та рекомендації щодо їх можливого використання**

Дисертація Котлярова В.О. має істотне значення для розвитку науки державного управління, оскільки поглиблює розуміння інформаційної безпеки як управлінського феномену, що поєднує правові, інституційні, технологічні, комунікаційні та соціальні складники. Результати дослідження можуть бути використані для подальшого наукового аналізу механізмів державного управління у сфері інформаційної безпеки, цифрової стійкості, стратегічних комунікацій, кібергігієни, захисту критичної інфраструктури та протидії дезінформації.

Практична цінність роботи полягає у можливості застосування її положень у діяльності органів державної влади, органів місцевого самоврядування, суб'єктів сектору безпеки і оборони, інституцій цифрової трансформації, підрозділів стратегічних комунікацій, а також організацій, що забезпечують кіберзахист і інформаційну стійкість критичної інфраструктури. Запропоновані автором підходи можуть бути використані під час розроблення стратегічних документів, удосконалення нормативно-правової бази, формування міжвідомчих процедур, підготовки програм медіаграмотності та підвищення цифрової культури населення.

Важливим підтвердженням прикладного значення результатів є їх упровадження у діяльність Національної акціонерної компанії «Надра України», Національного агентства кваліфікацій, Департаменту кадрової політики Міністерства оборони України, Центрального науково-дослідного інституту Збройних Сил України, а також Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв'язку та

захисту інформації України. Такі впровадження демонструють затребуваність результатів дисертації для управлінської, аналітичної, освітньої та безпекової практики.

Рекомендації дисертаційного дослідження можуть бути корисними також у навчальному процесі закладів вищої освіти під час підготовки фахівців з публічного управління та адміністрування, національної безпеки, інформаційної безпеки, кібербезпеки, стратегічних комунікацій і цифрової трансформації. Матеріали дисертації доцільно використовувати при розробленні освітніх компонентів, методичних рекомендацій, аналітичних записок, програм підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядування.

### **Повнота викладу наукових положень, висновків і рекомендацій дисертації в опублікованих працях**

Основні результати дисертаційного дослідження належним чином висвітлені в опублікованих працях здобувача. За темою дисертації опубліковано 36 наукових праць загальним обсягом 29,3 обл.-вид. арк., з яких 24,7 обл.-вид. арк. належать автору. До їх складу входить розділ у колективній монографії, 4 статті у періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України та у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, 17 статей у наукових фахових виданнях з державного управління, 10 статей в інших періодичних виданнях України та 4 тези доповідей на науково-практичних конференціях.

Тематика публікацій узгоджується зі змістом дисертації та охоплює її ключові напрями: міжнародно-політичну взаємодію у сфері інформаційних відносин, комплексне розуміння інформаційної безпеки, категоріальний апарат, стратегічні цілі інформаційної безпеки, адаптацію України до стандартів ЄС і НАТО, інформаційну безпеку як систему правовідносин, механізми раннього

виявлення інформаційних атак, кібергігієну, репутаційні ризики, методологічні засади дослідження інформаційної безпеки та правовий механізм її забезпечення.

Апробація результатів дослідження здійснювалася на міжнародних науково-практичних конференціях, серед яких «3rd International Conference on Corporation Management (ICCM-2023)» (Естонія, 2023), «ICEAF-2023» (Естонія, 2023), «II International Scientific and Practical Conference “Modern Approaches to Problem Solving in Science and Technology”» (Варшава, Польща, 2023), «II International Scientific and Practical Conference “Collective Thinking: Unifying Scientific Approaches in Multifaceted Research”» (Амстердам, Нідерланди, 2023). Наведені дані підтверджують, що наукові положення, висновки і рекомендації були представлені та обговорені у науковому середовищі.

### **Ідентичність змісту реферату і основних положень дисертації**

Зміст реферату відповідає основним положенням дисертації Котлярова В.О. У ньому відображено актуальність теми, зв'язок роботи з науковими програмами, мету і завдання, об'єкт та предмет, методологічну основу, наукову новизну, практичне значення, апробацію результатів, публікації здобувача і загальні висновки. Структурна логіка реферату узгоджується з логікою дисертаційного дослідження та дає можливість скласти цілісне уявлення про зміст, результати і внесок автора.

Основні положення, винесені до реферату, не суперечать змісту дисертації, а стисло репрезентують її ключові теоретичні й практичні результати. Формулювання наукової новизни, характеристика методів, практичного значення і публікацій відповідають матеріалам дисертаційної роботи. Оформлення дисертації та реферату загалом відповідає вимогам, що висуваються до кваліфікаційних наукових праць відповідного рівня.

## Дискусійні положення та зауваження щодо змісту дисертації

Позитивно оцінюючи дисертаційне дослідження, його наукову новизну, теоретичну насиченість і практичну спрямованість, необхідно висловити такі зауваження дискусійного характеру:

1. Автор позиціонує інформаційну безпеку не лише як галузь політики, а як «загальнодержавну парадигму публічного управління». Разом із тим, у тексті дисертації ця теза залишається переважно програмною: не показано, які саме традиційні підходи до публічного управління вона замінює або коригує, які управлінські практики змінює, а які лише доповнює. Це знижує переконливість заявленого положення новизни, оскільки не до кінця зрозуміло, в чому полягає «парадигмальність» запропонованого підходу – у змісті, інструментарії чи лише в актуалізації проблематики.

2. У роботі подано деталізовану архітектуру суб'єктів забезпечення інформаційної безпеки (органи безпекового сектору, органи цифрової трансформації, гуманітарні інституції, приватний сектор). Проте у висновках не завжди чітко розмежовано, які саме функції пропонується посилити, а які – зменшити або передати іншим суб'єктам. Наприклад, не до кінця прозорою є логіка розподілу відповідальності між органами сектору безпеки та органами, відповідальними за цифровий розвиток, особливо в частині профілактики інформаційних загроз. Це робить заявлену інституційну інновацію менш прозорою з точки зору практичного впровадження.

3. Дисертант пропонує низку правових удосконалень (оновлення дефініцій, уточнення повноважень, перегляд окремих норм), які позиціонуються як результат наукового дослідження. Однак більшість таких рекомендацій подано у форматі загальних напрямів («передбачити», «уточнити», «закріпити»), без розкриття хоча б орієнтовних формулювань або структурних змін до конкретних законодавчих чи підзаконних актів. Через це складно оцінити, наскільки ці пропозиції виходять за межі декларативного рівня і

можуть бути використані як основа для нормотворчої діяльності органів публічної влади.

4. У дисертації сформульовано масштабні цілі (посилення стійкості інформаційного простору, адаптивність системи публічного управління, інтеграція з європейськими підходами). Водночас логіка переходу від цих цілей до конкретних завдань і далі – до очікуваних результатів (у вигляді нових моделей, механізмів, рекомендацій) у деяких розділах виглядає не повністю узгодженою. Наприклад, частина висновків стосується суто теоретичних уточнень, які важко на пряму співвіднести із заявленими на початку дослідження прикладними орієнтирами. Це створює враження певної дисбалансованості між теоретичною та практичною складовими роботи.

5. Автор справедливо враховує специфіку воєнного стану, проте значна частина запропонованих механізмів описана як універсальні – без чіткого розмежування між короткостроковими антикризовими заходами та довгостроковими інституційними змінами. Заумов швидкоплинної безпекової ситуації це створює ризик, що окремі пропозиції втратять актуальність або потребуватимуть суттєвої адаптації одразу після зміни фаз конфлікту чи зовнішньополітичних умов. У роботі варто було б сильніше акцентувати, які механізми розраховані насамперед на особливий період, а які – на стабільну фазу розвитку системи публічного управління.

Наведені зауваження не заперечують загальної позитивної оцінки дисертації, однак окреслюють напрями, які можуть бути враховані автором у подальших дослідженнях і під час практичного впровадження запропонованих механізмів реалізації інформаційної безпеки у системі публічного управління.

### **Загальний висновок**

Дисертаційне дослідження Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління»

є завершеною самостійною науковою працею, у якій отримано нові науково обґрунтовані результати, що в сукупності розв'язують важливу науково-прикладну проблему розвитку механізмів реалізації інформаційної безпеки в системі публічного управління України.

Таким чином, слід зазначити, що дисертаційна робота Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління», відповідає вимогам МОН України, постанові Кабінету міністрів України “Про порядок присудження та позбавлення наукового ступеня доктора наук” від 17 листопада 2021 р. № 1197 а саме: є завершеною кваліфікаційною науковою працею, у якій отримано нові науково обґрунтовані результати в галузі науки державного управління, що розв'язують конкретну наукову проблему, а її автор заслуговує на присудження наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління.

Офіційний опонент  
професор кафедри обліку і аудиту  
Чорноморського національного  
університету імені Петра Могили,  
д.держ.упр., професор

  
А.В. Антонова

*Підпис Антонової Л.В. засвідчую*  
*Вчений секретар*  
*Чорноморського національного університету*  
*імені Петра Могили*

*Вікторія ЧОРНА*

« \_\_\_\_\_ » 2026 р.