ВІДГУК

офіційного опонента доктора наук з державного управління, професора Помази-Пономаренко Аліни Леонідівни 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

Інформаційна безпека у сучасних умовах є однією з базових передумов стійкого функціонування держави, суспільства та системи публічного управління. Вона охоплює не лише захист інформаційних ресурсів, інформаційно-комунікаційних систем і критичної цифрової інфраструктури, а й здатність державних інституцій забезпечувати цілісність, достовірність, доступність та безпечне використання інформації у процесах вироблення й реалізації публічної політики. Заумов цифрової трансформації, глобальної взаємозалежності, інтенсивного розвитку штучного інтелекту, великих даних і платформних комунікацій інформаційна сфера перетворюється на простір одночасно управлінських можливостей і безпекових ризиків. Саме тому наукове опрацювання механізмів реалізації інформаційної безпеки в системі публічного управління має важливе теоретичне, методологічне та практичне значення.

Особливої актуальності проблематика дисертації Котлярова В.О. набуває у зв’язку з повномасштабною збройною агресією російської федерації проти України, яка супроводжується системними інформаційно-психологічними операціями, кібератаками, дезінформаційними кампаніями, спробами дестабілізації публічних інституцій та підриву довіри громадян до державної політики. У таких умовах інформаційна безпека стає не допоміжним, а

стратегічним напрямом публічного управління, пов’язаним із захистом національних інтересів, демократичних цінностей, прав людини, стійкості критичної інфраструктури, інформаційної гігієни суспільства та ефективності міжвідомчої координації. Дисертаційне дослідження спрямоване на осмислення зазначених викликів і формування науково обґрунтованих підходів до побудови цілісної моделі забезпечення інформаційної безпеки України.

Актуальність роботи посилюється тим, що в українській науці державного управління, попри наявність значної кількості праць з питань національної, інформаційної та кібербезпеки, залишається потреба у комплексному узагальненні інституційно-правових, організаційних, комунікаційно-стратегічних і міжсекторальних складників механізмів інформаційної безпеки. Здобувач виходить із необхідності поєднання правового регулювання, стратегічного управління, міжвідомчої взаємодії, публічно-приватного партнерства, громадянської участі та міжнародного досвіду. Такий ракурс відповідає сучасним запитам державної політики, адже ефективне реагування на гібридні загрози потребує не фрагментарних управлінських заходів, а адаптивної, прогнозної та багаторівневої архітектури публічного управління у сфері інформаційної безпеки.

Зв’язок роботи з науковими програмами, планами, темами

Дисертаційне дослідження виконано в межах науково-дослідної роботи Національного аерокосмічного університету «Харківський авіаційний інститут» за темою «Механізми реалізації інформаційної безпеки у системі публічного управління» (2025–2026). Науковий доробок здобувача полягає у теоретичному обґрунтуванні засад забезпечення інформаційної безпеки в умовах глобалізації та цифровізації, визначенні структури механізму правового забезпечення інформаційної безпеки в Україні, аналізі міжнародних норм і практик, характеристиці сучасних інформаційних загроз, а також у розробленні стратегії-

моделі національної цифрової стійкості України. Зазначене свідчить про відповідність теми дисертації профілю наукових досліджень установи та про спрямованість роботи на розв'язання актуальної науково-прикладної проблеми галузі державного управління.

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

Метою дисертаційного дослідження є 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 й функціонування інформаційно-безпекового середовища України в особливий період. Поставлена мета є логічно пов'язаною з предметом дослідження і розкривається через комплекс завдань, що охоплюють розроблення інтегративної моделі механізмів реалізації інформаційної безпеки, уточнення теоретико-методологічних засад дослідження, обґрунтування інституційного механізму, систематизацію методологічних підходів, розкриття сутнісних характеристик правового регулювання, аналіз протидії загрозам в умовах військової агресії, побудову адаптивної архітектури забезпечення інформаційної безпеки, розвиток стратегічного управління, узагальнення сучасних викликів і тенденцій та наукове обґрунтування стратегії-моделі національної цифрової стійкості України.

Об'єктом дослідження визначено інформаційну безпеку держави як систему суспільних відносин у сфері публічного управління, а предметом – механізми реалізації інформаційної безпеки у системі публічного управління. Таке співвідношення об'єкта і предмета є коректним, оскільки дозволяє розглядати інформаційну безпеку не лише як техніко-правовий або

правоохоронний сегмент, а як складну управлінську систему, у якій взаємодіють державні органи, приватний сектор, громадянське суспільство, міжнародні партнери та цифрові інфраструктури.

Достовірність і належний рівень обґрунтованості наукових положень забезпечено використанням системного, історико-ретроспективного, компаративного, структурно-функціонального, прогностичного та проблемно-аналітичного підходів, а також методів аналізу, синтезу, класифікації, узагальнення, індукції і дедукції. Комплексність методологічної бази дала змогу здобувачеві поєднати аналіз категоріального апарату, правового механізму, інституційної архітектури, міжнародного досвіду та практичних інструментів протидії інформаційним загрозам. У роботі простежується прагнення автора перейти від опису окремих інструментів до моделювання цілісної управлінської системи, здатної діяти в умовах невизначеності, воєнного стану та динамічних гібридних загроз.

Дисертаційна робота спирається на значний масив наукових джерел, нормативно-правових актів, міжнародних документів, аналітичних матеріалів і практик функціонування суб’єктів публічного управління у сфері інформаційної та кібербезпеки. Висновки дисертації узгоджені з поставленими завданнями, відображають зміст проведеного дослідження та містять науково-практичні рекомендації щодо удосконалення механізмів забезпечення інформаційної безпеки. Позитивним є те, що автор розглядає інформаційну безпеку у взаємозв’язку з національною безпекою, правами людини, цифровою стійкістю, стратегічними комунікаціями та демократичним контролем.

Наукове значення дисертаційного дослідження, достовірність і новизна наукових положень

Структура дисертації є логічною, послідовною та відповідає заявленій меті дослідження. Робота складається зі вступу, п’яти розділів, висновків,

списку використаних джерел і додатків, що забезпечує комплексне висвітлення теоретичних, методологічних, інституційних, правових, стратегічних та прикладних аспектів теми. Матеріал викладено у взаємозв'язку між розділами: від уточнення понятійного апарату й методології – до розроблення моделей, механізмів і рекомендацій для практики публічного управління.

Наукова новизна одержаних результатів полягає у комплексному теоретичному обґрунтуванні стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки у системі публічного управління як автономного, системно організованого феномену в умовах трансформаційних, цифрових і воєнних викликів. Найбільш вагомими є положення, які стосуються інтегративної моделі механізмів реалізації інформаційної безпеки, теоретико-методологічних засад формування механізмів забезпечення інформаційної безпеки, а також стратегії-моделі національної цифрової стійкості України.

Уперше у дисертації обґрунтовано інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України. Її цінність полягає у поєднанні міжсекторального та комунікаційно-стратегічного підходів, урахуванні інституційно-правової конструкції ключових суб'єктів забезпечення інформаційної стійкості, визначенні критеріїв функціональної діагностики управлінських обмежень в умовах воєнного стану та формуванні концепції стратегічного управління інформаційною безпекою. Така модель дозволяє розглядати інформаційну безпеку як сферу, у якій захист критичної інфраструктури, протидія дезінформації, медіаграмотність, стратегічні комунікації та громадянська стійкість мають бути взаємопов'язаними управлінськими процесами.

Важливим науковим результатом є обґрунтування теоретико-методологічних засад формування механізмів забезпечення інформаційної безпеки через систематизацію централізованої, децентралізованої та публічно-

приватної моделей управління. Автор не обмежується їх описом, а визначає переваги й обмеження кожної моделі для українських умов, акцентуючи на необхідності поєднання швидкого реагування, уніфікації стандартів, секторної гнучкості, технологічної експертизи приватного сектору та належної координації між державними органами.

Науково значущою є розроблена здобувачем стратегія-модель національної цифрової стійкості України, що має трирівневу будову – стратегічний, тактичний і операційний рівні. Вона ґрунтується на принципах проактивності, багаторівневої координації, гнучкості та демократичного контролю. Особливе значення має орієнтація моделі на перехід від реактивного реагування до прогнозно-превентивного управління інформаційною безпекою, а також на створення Єдиного національного центру стратегічних комунікацій як координуючої інституції, спроможної інтегрувати моніторинг загроз, стратегічні комунікації та міжрівневу взаємодію.

Удосконалено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління. Здобувач розкриває подвійну природу інформаційної безпеки як системи суспільних відносин і як об’єкта правової охорони, структурує її елементи, визначає суб’єктів, об’єкт, регулятивні засади, інститути й цілі. Такий підхід сприяє переходу від статичного тлумачення інформаційної безпеки як стану захищеності до динамічного розуміння її як управлінського процесу, що потребує постійної координації, прогнозування, адаптації та контролю.

Позитивної оцінки заслуговує розвиток підходів до інституційного механізму забезпечення інформаційної безпеки. У дисертації запропоновано мультифункціональну архітектурну модель взаємодії Служби безпеки України, Ради національної безпеки і оборони України та Міністерства цифрової трансформації України за логікою «моніторинг – координація – впровадження».

Окремо обґрунтовано роль Міністерства культури та стратегічних комунікацій України як суб'єкта забезпечення культурно-інформаційної стійкості й нормативно-правового регулювання інформаційної політики, що доповнює техніко-правові та правоохоронні сегменти.

Суттєвим є авторське розкриття механізму правового регулювання інформаційної безпеки, у межах якого поєднано регулювання інформаційної діяльності, розвиток інформаційного середовища, право людини на інформацію, принципи законності, захисту прав і свобод, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці, пропорційності, відповідальності та безперервності. У роботі аргументовано, що інформаційна безпека не повинна протиставлятися праву людини на інформацію, а має бути спрямована на забезпечення його реальної та безпечної реалізації.

Дістали подальшого розвитку методичні підходи до протидії загрозам інформаційній безпеці України в умовах військової агресії. Здобувач виокремлює нормативно-правові та організаційні механізми, технічні засоби кіберзахисту, інформаційно-психологічну безпеку, освітні ініціативи з цифрової грамотності та інтеграцію міжнародної співпраці. Така кластеризація дозволяє комплексно оцінювати загрози й формувати багатовимірну систему реагування, що охоплює як державні інституції, так і суспільні, освітні та міжнародні компоненти.

Заслуговує на увагу концептуальна модель переходу до адаптивної архітектури забезпечення інформаційної безпеки, побудована на засадах прозорості, гласності, сценарного планування та багаторівневого управління. У ній стратегічний рівень пов'язано з прогнозуванням і аналітикою, оперативний – зі створенням спільних міжвідомчих центрів реагування, а тактичний – із розробленням локальних сценаріїв дій на рівні відомств і територіальних

громад. Це розширює практичну цінність роботи, оскільки пропонує не лише загальну концепцію, а й логіку розподілу управлінських функцій.

Значущими є результати дисертації щодо стратегічного управління інформаційною безпекою. Автор систематизує міжнародні моделі, аналізує досвід США, ЄС, Великої Британії, Ізраїлю та Китаю, виокремлює рівні цілей стратегічного управління – захист, розвиток і стійкість, а також акцентує на правовому регулюванні, інституційній структурі, міжнародній співпраці та інноваційних технологіях. Такий підхід є корисним для адаптації зарубіжного досвіду до українських реалій без механічного копіювання інституційних моделей.

У дисертації узагальнено сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави. Автор аналізує глобально-політичні, технологічні та соціально-комунікаційні ризики, зокрема гібридні війни, дезінформацію, інформаційну асиметрію, штучний інтелект, Big Data, deepfake-технології, алгоритмічну архітектуру цифрових платформ і соціальних мереж. Важливо, що ці ризики розглянуто не ізольовано, а як взаємопов’язані фактори, здатні посилювати один одного та потребувати поєднання поведінкових, освітніх, інституційних і правових засобів протидії.

Наукове значення одержаних результатів для науки й практики та рекомендації щодо їх можливого використання

Дисертаційна робота Котлярова В.О. є завершеним самостійним науковим дослідженням, у якому сформульовано теоретичні положення, методологічні підходи та практичні рекомендації щодо реалізації інформаційної безпеки у системі публічного управління. Її результати можуть бути використані органами державної влади, суб’єктами сектору безпеки і оборони, органами місцевого самоврядування, установами, відповідальними за цифрову

трансформацію, стратегічні комунікації, кіберзахист, захист критичної інфраструктури та протидію дезінформації.

Практичне значення роботи полягає у доведенні основних ідей і висновків до рівня конкретних положень, методик і рекомендацій. Результати дослідження впроваджено 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. Зазначені впровадження підтверджують прикладну спрямованість дисертації та її значення для удосконалення управлінських, аналітичних і безпекових процедур у сфері інформаційної стійкості.

Наукові результати можуть бути використані під час удосконалення нормативно-правового забезпечення інформаційної безпеки, розроблення стратегій цифрової стійкості, організації міжвідомчої взаємодії, формування програм медіаграмотності й кібергігієни, підготовки методичних матеріалів для органів публічного управління, а також у навчальному процесі закладів вищої освіти за спеціальностями, пов'язаними з публічним управлінням, національною безпекою, кібербезпекою та стратегічними комунікаціями.

Окремої підтримки заслуговує орієнтація здобувача на інтеграцію демократичного контролю, прав людини та принципу пропорційності в механізми забезпечення інформаційної безпеки. Такий підхід має важливе практичне значення, оскільки в умовах воєнного стану й гібридної агресії держава повинна одночасно забезпечувати захист інформаційного простору, зберігати довіру громадян, не допускати невиправданого обмеження свобод і підтримувати правову визначеність публічно-управлінських рішень.

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

Основні положення дисертаційного дослідження пройшли належну апробацію на міжнародних науково-практичних конференціях, зокрема «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). Це свідчить про обговорення результатів роботи у науковому середовищі та їх відповідність сучасній проблематиці публічного управління й інформаційної безпеки.

За темою дисертації опубліковано 36 наукових праць загальним обсягом 29,3 обл.-вид. арк., з яких 24,7 обл.-вид. арк. належать автору. Серед них – 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, 18 статей у наукових фахових виданнях з державного управління, 9 статей в інших періодичних виданнях України, 4 тези доповідей на науково-практичних конференціях. Кількість і якість публікацій є достатніми для висвітлення основних наукових результатів докторської дисертації.

Опубліковані праці розкривають ключові напрями дисертації: еволюцію міжнародної взаємодії у сфері інформаційних відносин, категоріальний апарат інформаційної безпеки, стратегічні цілі інформаційної безпеки, правовий механізм її забезпечення, кібергігієну, управління репутаційними ризиками, адаптацію до стандартів ЄС і НАТО, протидію кібертероризму та інші аспекти інформаційної стійкості. Зміст публікацій корелює з розділами дисертації й підтверджує повноту апробації наукових положень, висновків і рекомендацій.

Ідентичність змісту реферату й основних положень дисертації

Аналіз змісту реферату та дисертації дає підстави констатувати їх відповідність за структурою, логікою викладу, формулюванням мети, завдань, об'єкта, предмета, наукової новизни, практичного значення та висновків. Реферат відображає основні теоретичні положення, результати наукового пошуку, апробацію, публікації та практичну значущість дисертаційного дослідження. Зміст реферату достатньо повно репрезентує ключові здобутки дисертації Котлярова В.О. і дає можливість скласти цілісне уявлення про її наукову новизну та практичну спрямованість.

Оформлення дисертації та реферату загалом відповідає вимогам, що висуваються до кваліфікаційних наукових праць на здобуття наукового ступеня доктора наук з державного управління. Виклад матеріалу є послідовним, термінологічний апарат здебільшого витриманий у межах предметного поля дослідження, а результати роботи узгоджені з публікаціями здобувача.

Дискусійні положення та зауваження щодо змісту дисертації

Загалом позитивно оцінюючи дисертаційне дослідження Котлярова В.О., його наукову новизну, практичну спрямованість і значення для розвитку науки державного управління, доцільно висловити окремі зауваження та пропозиції дискусійного характеру:

1. У дисертації потребують додаткової чіткості та структурної узгодженості базові дефініції «механізм правового регулювання забезпечення інформаційної безпеки» та «інформаційна безпека як об'єкт публічного управління» (підрозділ 1.1). У той же час, автору слід конкретизувати, де проходить межа у чому полягає різниця між «інформаційною безпекою як станом захищеності» і «механізмом її забезпечення як системою інституційних, правових і організаційних інструментів». На наш погляд, це покликано забезпечити подальшу операціоналізацію понятійно-категоріального апарату

державного управління.

2. Автор дисертації слушно пропонує застосовувати інтегративний підхід до поєднання централізованої, децентралізованої та публічно-приватної моделей управління інформаційною безпекою (с. 345–346). Разом із тим уважаємо, що роль кожної з означених моделей у конкретних умовах (мирний час, воєнний стан, післявоєнна відбудова) потребує додаткової деталізації. Дисертація тільки б виграла, якби її автор конкретизував, за яких політико-правових та інституційних передумов доцільно посилювати централізований компонент, а за яких має переважати впровадження децентралізованого або мережевого підходів.

3. У роботі значна увага приділяється множинності суб'єктів публічного управління інформаційною безпекою (СБУ, РНБО, Міністерство цифрової трансформації, інші органи) (підрозділи 1.3, 5.2, 5.3). Однак уважаємо за доцільне зазначити, що запропоновані механізми міжвідомчої координації (підрозділ 5.2) мають переважно концептуальний характер і не завжди супроводжуються визначенням процедурних регламентів (зокрема, щодо обміну інформацією, розподілу відповідальності та уникнення дублювання повноважень). На наш погляд, це певною мірою обмежує можливості практичного впровадження розробленої автором моделі публічного управління інформаційною безпекою.

4. Дисертант цілком обґрунтовано наголошує на застосуванні людиноцентричного підходу та необхідності поєднання інформаційної безпеки з гарантіями прав людини (підрозділ 2.2). Уважаємо, що дисертаційна робота тільки б виграла, якби її автор визначив баланс між захистом інформаційного простору та забезпеченням свободи слова і доступу до інформації не тільки на рівні загальних принципів. Це потрібно зреалізувати з огляду на важливість унеможливлення появи зайвих наукових дискусій у межах досліджуваної проблематики дослідження.

5. У дисертації справедливо вказується на важливість розвитку публічно-приватного партнерства у забезпеченні інформаційної та кібербезпеки, зокрема у взаємодії державних органів з ІТ-сектором та операторами критичної інфраструктури. Водночас варто зауважити, що організаційно-правові інструменти такого партнерства описані в дисертації переважно у вигляді загальних моделей, без достатньої диференціації за типами суб'єктів (критична інфраструктура, малий бізнес, громадський сектор) і без аналізу ризиків конфлікту інтересів та механізмів їхньої мінімізації.

У той же час, уважаємо, що вищенаведені зауваження мають дискусійний характер, спрямовані на поглиблення окремих положень дисертації та не знижують загальної позитивної оцінки проведеного дослідження, його наукової новизни і практичної значущості для розвитку механізмів державного управління у сфері інформаційної безпеки.

Загальний висновок

Дисертаційне дослідження Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» є завершеною самостійною науковою працею, у якій розв'язано важливу науково-прикладну проблему теоретичного обґрунтування та практичного удосконалення механізмів реалізації інформаційної безпеки у системі публічного управління України в умовах цифрової трансформації, гібридних загроз і воєнного стану.

Актуальність теми, обґрунтованість наукових положень, достовірність отриманих результатів, належний рівень апробації, достатня кількість публікацій, практичне впровадження результатів і відповідність змісту реферату основним положенням дисертації дають підстави для висновку, що подана робота відповідає вимогам МОН України, постанові Кабінету міністрів України «Про порядок присудження та позбавлення наукового ступеня доктора наук»

від 17 листопада 2021 р. № 1197, а її автор – Котляров Валерій Олександрович – заслуговує на присудження наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління.

Офіційний опонент
завідувач науково-дослідної лабораторії
з дослідження проблем управління у сфері цивільного захисту
навчально-наукового інституту цивільного захисту
Національного університету
цивільного захисту України
д.держ.упр., професор Аліна ПОМАЗА-ПОНОМАРЕНКО

Підпис Аліни Помаза-Пономаренко
засвідчую
Учений секретар
к.техн.н., с.н.с. Андрій Пайдак