ВІДГУК

офіційного опонента доктора наук з державного управління, професора Щепанського Едуарда Валеріївича 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

Сучасна система публічного управління функціонує в умовах, коли інформація стала не лише ресурсом ухвалення управлінських рішень, а й простором безпосереднього протиборства, інструментом впливу на поведінку громадян, чинником легітимності влади та умовою збереження керованості державних процесів. Для України це питання має особливу вагу, оскільки інформаційні загрози супроводжують усі ключові сфери суспільного розвитку: оборону, економіку, цифровізацію, соціальну комунікацію, міжнародну підтримку, діяльність органів влади та місцевих громад.

Повномасштабна агресія російської федерації проти України переконливо засвідчила, що у XXI столітті інформаційна безпека не може бути відокремлена від стійкості державного управління. Маніпулятивні кампанії, кібервтручання, поширення недостовірних повідомлень, атаки на критичні інформаційні ресурси, використання цифрових платформ для психологічного тиску на населення потребують від держави системних, своєчасних і координованих дій. Ідеться не лише про протидію окремим інформаційним інцидентам, а про побудову цілісної управлінської архітектури, здатної прогнозувати ризики, мобілізувати інституційні ресурси та підтримувати суспільну довіру.

Актуальність теми посилюється тим, що інформаційна безпека дедалі більше залежить від поєднання державного регулювання, технологічної компетентності, стратегічних комунікацій, правових гарантій і участі недержавних суб’єктів. Органи публічної влади повинні одночасно

забезпечувати захист інформаційного простору, розвиток цифрових сервісів, доступ громадян до достовірної інформації, дотримання прав людини, взаємодію з бізнесом і громадянським суспільством. Така багатовимірність проблеми зумовлює потребу у науковому осмисленні механізмів реалізації інформаційної безпеки саме в системі публічного управління.

Дисертація Котлярова В.О. є своєчасною також з огляду на необхідність переосмислення управлінських моделей, що застосовуються в Україні у сфері інформаційної та кібербезпеки. Традиційні адміністративні підходи, побудовані переважно на вертикальному розподілі повноважень, не завжди відповідають швидкості поширення загроз, мережевому характеру інформаційних процесів і потребі в оперативній міжвідомчій взаємодії. Саме тому науковий інтерес становлять запропоновані автором підходи до інтегративної моделі, адаптивної архітектури, стратегічного управління та національної цифрової стійкості.

Отже, обрана тема має вагоме теоретичне, методологічне і практичне значення. Вона безпосередньо пов’язана з модернізацією механізмів державного управління, зміцненням національної безпеки, розвитком цифрової держави, підвищенням спроможності органів влади реагувати на гібридні загрози та формуванням демократично збалансованої політики 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). Зміст дисертації відповідає спрямуванню зазначеної теми, оскільки охоплює теоретичне обґрунтування інформаційної безпеки як управлінського феномену, аналіз правових та інституційних механізмів, узагальнення міжнародного досвіду, дослідження сучасних інформаційних загроз і розроблення стратегії-моделі національної цифрової стійкості України.

Особистий внесок здобувача полягає у комплексному дослідженні механізмів реалізації інформаційної безпеки в публічному управлінні,

визначенні ролі ключових суб'єктів, розкритті взаємозв'язку правового регулювання, стратегічних комунікацій, кіберстійкості та міжсекторальної взаємодії. Така спрямованість роботи підтверджує її відповідність науковим планам установи та актуальним потребам розвитку галузі знань «Публічне управління та адміністрування».

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

Мета дисертації 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 з'ясуванні особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період. Така постановка мети є науково виправданою, оскільки поєднує теоретичний, методологічний і прикладний рівні дослідження.

Для досягнення мети автор послідовно вирішує коло взаємопов'язаних завдань: обґрунтовує інтегративну модель механізмів реалізації інформаційної безпеки, уточнює теоретико-методологічні засади дослідження, розкриває інституційний і правовий механізми, систематизує методичні підходи протидії загрозам, формує модель переходу до адаптивної архітектури, розвиває теоретичні засади стратегічного управління, узагальнює сучасні виклики та тенденції, а також пропонує стратегію-модель національної цифрової стійкості України. Логіка завдань загалом відповідає заявленій меті й дозволяє розкрити предмет дослідження у достатньому обсязі.

Об'єктом дослідження визначено інформаційну безпеку держави як систему суспільних відносин у сфері публічного управління, предметом – механізми реалізації інформаційної безпеки у системі публічного управління. Такий підхід дає змогу розглядати інформаційну безпеку не як ізольовану галузь технічного захисту, а як комплекс управлінських відносин, у межах яких

взаємодіють держава, громадянське суспільство, бізнес, інститути безпекового сектору, органи цифрової трансформації та гуманітарні структури.

Методологічна база дослідження є достатньо широкою. Автор використовує системний, історико-ретроспективний, компаративний, структурно-функціональний, проблемний і прогностичний підходи, а також методи аналізу, синтезу, узагальнення, класифікації, індукції та дедукції. Застосування такого інструментарію дозволило простежити розвиток категорії інформаційної безпеки, порівняти міжнародні моделі, оцінити сучасні загрози, розкрити інституційні зв'язки та запропонувати власні управлінські рішення.

Обґрунтованість наукових положень забезпечується використанням значного масиву наукової літератури, нормативно-правових актів, міжнародних документів і практик, а також аналізом діяльності ключових суб'єктів забезпечення інформаційної безпеки. Висновки дисертації пов'язані зі змістом розділів, відповідають поставленим завданням і в основному випливають з проведеного дослідження. Рекомендації мають як теоретичне, так і прикладне спрямування, оскільки стосуються удосконалення правового регулювання, інституційної координації, стратегічних комунікацій, цифрової стійкості та протидії інформаційним загрозам.

Позитивно слід оцінити прагнення дисертанта поєднати у межах одного дослідження різні рівні аналізу: від категоріального осмислення інформаційної безпеки до розроблення моделі національної цифрової стійкості. Завдяки цьому робота не обмежується описом окремих проблем, а пропонує цілісне бачення функціонування механізмів інформаційної безпеки у публічному управлінні.

Наукове значення дисертаційного дослідження, достовірність і новизна наукових положень

Наукове значення дисертації полягає у розробленні та обґрунтуванні комплексного підходу до реалізації інформаційної безпеки у системі публічного управління України. Автор розглядає інформаційну безпеку як багаторівневу управлінську систему, у якій правові норми, інституційні зв'язки, технологічні

інструменти, стратегічні комунікації, освітні ініціативи та міжсекторальна взаємодія мають функціонувати узгоджено.

До найбільш значущих результатів належить обґрунтування інтегративної моделі механізмів реалізації інформаційної безпеки у системі публічного управління України. Її особливість полягає в орієнтації на поєднання інституційно-правового, комунікаційно-стратегічного та міжсекторального вимірів. У межах цієї моделі автор акцентує увагу на ролі РНБО, Центру протидії дезінформації, Міністерства культури, органів цифрової трансформації, сектору безпеки, приватних суб'єктів і громадянського суспільства.

Важливим теоретичним результатом є поглиблення розуміння інформаційної безпеки як системи суспільних відносин і як об'єкта правової охорони. Дисертант структурує її ключові елементи – суб'єктів, об'єкти, інститути, цілі, регулювання, громадянську участь, інформаційну грамотність, етичні засади та відповідальність. Такий підхід сприяє переходу від статичного опису інформаційної безпеки до аналізу її як динамічного процесу управління.

Наукової уваги заслуговує запропонована автором модель взаємодії Служби безпеки України, Ради національної безпеки і оборони України та Міністерства цифрової трансформації України за логікою «моніторинг – координація – впровадження». Вона дозволяє переосмислити інституційний механізм не як простий перелік повноважень, а як функціонально пов'язану систему управлінських дій, спрямованих на забезпечення інформаційної стійкості.

У дисертації розкрито сутнісні характеристики механізму правового регулювання інформаційної безпеки, зокрема через поєднання регулювання інформаційної діяльності та розвитку інформаційного середовища. Заслуговує на увагу також авторське осмислення взаємозв'язку інформаційної безпеки з правом людини на інформацію, принципами законності, прозорості, пропорційності, відповідальності, технологічної адаптивності, міжвідомчої координації та безперервності.

Значний інтерес становить систематизація методичних підходів протидії загрозам інформаційній безпеці України в умовах військової агресії. Автор виокремлює нормативно-правові та організаційні механізми, технічні засоби кіберзахисту, інформаційно-психологічну безпеку і протидію дезінформації, освітні ініціативи, підвищення цифрової грамотності та міжнародну співпрацю. Така кластеризація демонструє комплексне бачення проблеми та її управлінських інструментів.

Окремим результатом є концептуальна модель переходу до адаптивної архітектури забезпечення інформаційної безпеки. Вона передбачає стратегічний рівень прогнозування і сценарного планування, оперативний рівень міжвідомчого реагування та тактичний рівень локальних сценаріїв дій на рівні відомств і територіальних громад. У цьому полягає значний потенціал для подальшого розвитку практики кризового та превентивного управління.

Достовірність отриманих результатів підтверджується відповідністю методів поставленим завданням, широкою джерельною базою, опорою на сучасні наукові підходи, узгодженістю висновків із матеріалами дослідження та апробацією основних положень у наукових публікаціях. Наукова новизна роботи полягає не лише в окремих дефініційних уточненнях, а й у спробі сформувати цілісну логіку управління інформаційною безпекою в умовах гібридних загроз, цифрової трансформації та воєнного стану.

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

Результати дисертації мають важливе значення для науки державного управління, оскільки розширюють уявлення про інформаційну безпеку як предмет управлінського впливу. Запропоновані підходи можуть бути використані у подальших наукових дослідженнях, присвячених механізмам державного управління, інформаційній політиці, кіберстійкості, стратегічним комунікаціям, протидії дезінформації та міжсекторальній взаємодії у сфері національної безпеки.

Практичне значення дисертації полягає у можливості застосування її висновків органами державної влади, суб'єктами сектору безпеки і оборони, органами місцевого самоврядування, інституціями цифрової трансформації, структурами стратегічних комунікацій, освітніми установами та організаціями, що працюють у сфері кіберзахисту і захисту критичної інфраструктури. Окремі положення можуть бути використані під час підготовки стратегічних документів, удосконалення нормативно-правової бази, формування міжвідомчих регламентів, розроблення програм медіаграмотності та підвищення кваліфікації публічних службовців.

Суттєвим підтвердженням прикладної спрямованості роботи є впровадження її результатів у діяльність Національної акціонерної компанії «Надра України», Національного агентства кваліфікацій, Департаменту кадрової політики Міністерства оборони України, Центрального науково-дослідного інституту Збройних Сил України та Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв'язку та захисту інформації України. Це свідчить про затребуваність запропонованих положень у практичній управлінській, безпековій та освітньо-аналітичній діяльності.

Матеріали дисертації доцільно використовувати у навчальному процесі закладів вищої освіти при викладанні дисциплін з публічного управління та адміністрування, національної безпеки, інформаційної політики, інформаційної безпеки, кібербезпеки, стратегічних комунікацій і цифрового врядування. Вони також можуть бути корисними при розробленні навчально-методичних матеріалів, програм підвищення кваліфікації та аналітичних документів для органів публічної влади.

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

Основні положення дисертації достатньо повно висвітлені у наукових публікаціях здобувача. За темою роботи 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 та 4 тези доповідей на науково-практичних конференціях.

Публікації охоплюють ключові напрями дисертаційного дослідження: теоретичні засади сутності та концепції інформаційної безпеки, категоріальний апарат, міжнародний контекст інформаційних відносин, інформаційну безпеку України у вимірі стандартів ЄС і НАТО, інформаційну безпеку як систему правовідносин, стратегічні цілі, кібергігієну, механізми раннього виявлення інформаційних атак, управління репутаційними ризиками, методологічні засади дослідження та правовий механізм забезпечення інформаційної безпеки.

Апробація результатів здійснювалася 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 підтверджує, що основні результати дослідження були представлені науковій спільноті та пройшли належне обговорення.

Ідентичність змісту реферату і основних положень дисертації

Реферат дисертації відображає основні положення кваліфікаційної наукової праці Котлярова В.О. У ньому наведено загальну характеристику роботи, актуальність теми, зв’язок із науковими програмами, мету і завдання, об’єкт і предмет, методи дослідження, наукову новизну, практичне значення, апробацію результатів, публікації здобувача та висновки.

Зміст реферату узгоджується з положеннями дисертації та репрезентує її основні результати без суттєвих розбіжностей. Формулювання наукової новизни, практичного значення і висновків у рефераті відповідають логіці та змісту дисертаційного дослідження. Це дає підстави стверджувати про належну ідентичність реферату основним положенням дисертації.

Дискусійні положення та зауваження щодо змісту дисертації

Загалом позитивно оцінюючи дисертаційне дослідження Котлярова В.О., його наукову новизну, теоретичну ґрунтовність і практичне спрямування, слід висловити такі зауваження дискусійного характеру:

1. Теоретична частина дисертації відзначається ґрунтовністю, однак структура викладу місцями є перевантаженою повторними зверненнями до одних і тих самих підходів різних авторів. Це ускладнює виділення власної позиції дисертанта та його авторських акцентів. Доцільним видається чіткіше відмежувати оглядово-описові фрагменти від тих місць, де пропонується оригінальне бачення категорій та механізмів інформаційної безпеки в системі публічного управління.

2. У роботі інформаційна безпека розглядається у тісному зв’язку з кібербезпекою, проте цей взаємозв’язок не завжди послідовно витримано на рівні категоріального апарату та висновків. В окремих розділах кібербезпека фактично зводиться до технічної складової, тоді як в інших – трактується як повноцінний елемент публічного управління. Відсутність чіткого розмежування (чи, навпаки, ієрархії) цих понять може спричиняти різночитання при практичній інтерпретації запропонованих механізмів.

3. Хоча в дисертації задекларовано триєдність «держава – бізнес – громадянське суспільство» у забезпеченні інформаційної безпеки, фактичний аналіз ролі громадських організацій та медіа-ініціатив є менш розгорнутим, ніж аналіз державних і приватних акторів. Практичні інструменти залучення громадянського суспільства (механізми участі, співрегулювання, громадського

контролю) окреслено лише фрагментарно. Це певною мірою звужує заявлену ідею багатосуб'єктності публічного управління у сфері інформаційної безпеки.

4. Дисертація концентрується переважно на загальнодержавному рівні системи публічного управління, тоді як регіональний та місцевий рівні розкриті значно слабше. Зокрема, практично відсутній аналіз ролі обласних військових адміністрацій, органів місцевого самоврядування, комунальних підприємств у реалізації політики інформаційної безпеки. За умов децентралізації та воєнного стану це є суттєвим аспектом, який потребує більшої уваги для забезпечення повноти запропонованої моделі.

5. У роботі справедливо наголошується на важливості стратегічних комунікацій, проте конкретні механізми комунікації органів публічної влади з населенням в умовах інформаційних загроз окреслено загально. Не деталізовано, яким чином запропоновані моделі впливають на практику інформування громадян, протидії панічним настроям, спростування дезінформації на рівні повсякденних управлінських рішень. Це послаблює зв'язок між концептуальними засадами інформаційної безпеки та реальними комунікаційними практиками держави.

Висловлені зауваження не знижують загальної позитивної оцінки дисертаційного дослідження, а мають рекомендаційний і дискусійний характер. Вони можуть бути враховані автором у подальшій науковій роботі та при практичній деталізації запропонованих механізмів реалізації інформаційної безпеки у системі публічного управління.

Загальний висновок

Дисертація Котлярова Валерія Олександровича «Механізми реалізації інформаційної безпеки у системі публічного управління» є самостійною, завершеною кваліфікаційною науковою працею, у якій отримано науково обґрунтовані результати, що мають істотне значення для розвитку механізмів державного управління у сфері інформаційної безпеки України.

За актуальністю теми, ступенем обґрунтованості наукових положень, достовірністю висновків, науковою новизною, практичним значенням, повнотою апробації та опублікуванням основних результатів 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 кафедри публічного управління та адміністрування Хмельницького університету управління та права імені Леоніда Юзькова, доктор наук з державного управління, професор Едуард ЩЕПАНСЬКИЙ

Підпис Едуарда Щепанського
ЗАСВІДЧУЮ
Нач. ВК ХУУП
імені Леоніда Юзькова