

Голові спеціалізованої вченої ради
ДФ 71
Національного аерокосмічного
університету «Харківський
авіаційний інститут»
д. держ. упр., професору
Олексію КРЮКОВУ

РЕЦЕНЗІЯ
на дисертаційну роботу
Кушнікова Вадима Вадимовича «Управління інформаційною безпекою
держави в умовах гібридних загроз», поданої на здобуття наукового
ступеня доктора філософії за спеціальністю 281 – публічне управління та
адміністрування

Рецензія на дисертаційну роботу Кушнікова Вадима Вадимовича «Управління інформаційною безпекою держави в умовах гібридних загроз» дозволяє сформулювати узагальнені висновки щодо її актуальності, ступеня обґрунтованості основних наукових положень, висновків, рекомендацій, достовірності, наукової новизни, практичного значення, а також загальної оцінки роботи.

Актуальність теми дисертаційного дослідження.

Однією з фундаментальних наукових проблем, які вирішуються нині, є розробка теоретико-методичних засад забезпечення інформаційної безпеки особистості, суспільства, держави. Вона передбачає наявність підходів, котрі забезпечують протидію впливам деструктивного характеру в межах глобального інформаційного простору та способи ідентифікації змістовних впливових процесів на масову свідомість й особистість, а також ризики й небезпеки, спричинені негативними наслідками маніпуляції свідомістю. Виходячи з цього, актуальною є модернізація процесів управління інформаційною безпекою держави в умовах гібридних загроз, що дозволить забезпечити ефективне функціонування та успішний розвиток як інформаційної сфери, так і соціуму в цілому. У цьому зв'язку Кабінетом Міністрів України було введено в дію Розпорядження «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025

року» від 30 березня 2023 р. № 272-р. У зв'язку з цим, дисертаційна робота Кушнікова В.В. «Управління інформаційною безпекою держави в умовах гібридних загроз» є своєчасною та актуальною.

Основні наукові положення, висновки і рекомендації, сформульовані в дисертації, ступень її обґрунтованості і достовірності.

Мета дисертаційної роботи полягає в науковому обґрунтуванні теоретичних засад і розробленні практичних рекомендацій щодо вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз.

Мета, поставлена дисертантом, досягається завдяки вирішенню комплексу наукових завдань, зокрема:

- з'ясувати сутність інформаційної безпеки як об'єкту публічного управління;
- охарактеризувати сучасний стан організаційно-правового механізму управління інформаційною безпекою України;
- оцінити поточні виклики та суперечності публічного управління інформаційною безпекою в Україні в умовах гібридних загроз;
- проаналізувати досвід зарубіжних країн стосовно управління інформаційною безпекою держави;
- обґрунтувати стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз;
- виокремити шляхи модернізації механізмів управління інформаційною безпекою держави;
- здійснити моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

Об'єктом дослідження є управління захистом інформаційного простору держави.

Предмет дослідження – управління інформаційною безпекою держави в умовах гібридних загроз.

Для вирішення окреслених завдань та отримання необхідних результатів дисертант використав різноманітні загальнонаукові та спеціальні наукові методи дослідження:

– гіпотетико-дедуктивний – для уточнення сутності предмета дослідження;

– узагальнюючий і порівняльний – для оцінки діючих механізмів управління інформаційною безпекою в умовах гібридних загроз в Україні та зарубіжних країнах;

– суб’єктно-об’єктний – для розробки комплексного механізму протидії інформаційно-політичним ризикам і загрозам;

– метод рефлексивного управління – для виокремлення стратегічних орієнтирів захисту єдиного інформаційного простору України в умовах гібридних загроз;

– структурно-функціональний підхід – для сценарного моделювання інформаційно-політичного впливу;

– експертне опитування та багатовимірний аналіз – для оцінки значимості інформаційно-критичних елементів у конкретному варіанті політичної структури;

– ризикоорієнтований підхід – для моделювання ризиків для інформаційно-критичних елементів політичної інфраструктури в умовах гібридних загроз.

Інформаційно-аналітичною основою дисертаційної роботи є законодавчі та підзаконні акти України, які регулюють питання, пов’язані з інформаційною безпекою держави, наукові здобутки вітчизняних і закордонних дослідників, статистичні дані органів державної влади та місцевого самоврядування, власні авторські напрацювання.

Сформульовані дисертантом наукові положення, висновки та рекомендації є достатньо обґрунтованими та таким, що базуються на належному використанні наукових розробок зарубіжних та українських вчених-дослідників як з теорії публічного управління, так і з нормативно-правової бази, яка регулює відносини у сфері управління інформаційною безпекою держави в умовах гібридних загроз, а також власних авторських дослідженнях.

Структура дисертаційної роботи побудована з дотриманням принципів логічності викладу дослідженого матеріалу, послідовно та повністю розкриває

зміст наукової праці, поданої на рецензування. Висновки за розділами та загальні висновки дисертації в достатній мірі є обґрунтованими та логічно пов'язаними, базуються на переконливих аргументах проведеного дослідження та отриманих результатах.

Найсуттєвіші результати дисертаційного дослідження, які містять наукову новизну, полягають у тому, що:

вперше:

– побудовано комплексний механізм протидії інформаційно-політичним ризикам і загрозам негативістського й компліментарного характеру, котрий складається з політичного, організаційного, економічного, правового та соціально-психологічного компонентів із вбудованими алгоритмами моніторингу та адаптації, та який передбачає вирішення проблем технічного, організаційного й правового характеру через формування спеціальних інформаційних контурів у діючих інформаційно-критичних елементах політичної структури, націлених на виявлення інформаційних загроз;

удосконалено:

– методичний підхід до запобігання явищ інформаційного тероризму в межах інституційної, нормативної, комунікативної, культурно-ідеологічної та функціональної підсистем політичної системи через інформаційно-психологічний вплив на окремі особистості, громадські й соціальні групи та на все населення загалом з метою збереження цілісності організаційних, технічних й інформаційних зв'язків цієї системи;

– теоретичний підхід до модернізації державної політики у сфері інформаційної безпеки через виокремлення в ній нормативно-правової, організаційної, технологічної та кадрової складових, що уможлиблює своєчасне виявлення інформаційних загроз безпеці особистості, суспільства і держави та протидію ним, а також реалізацію стратегічних інтересів держави у складному конкурентному інформаційному просторі сьогодення на основі загальновизнаних принципів та норм міжнародного права щодо забезпечення інформаційної безпеки;

– практичний підхід до сценарного моделювання інформаційно-політичного впливу, котрий передбачає взаємопов'язану реалізацію

наступних модельних блоків: «структура інформаційно-політичної загрози», «політична структура», «визначення інформаційно-критичних елементів політичної структури», «операційно-тимчасова модель інформаційно-політичного впливу», «оцінка поточного стану інформаційно-політичного впливу», котрий враховує інформаційний фактор у процесі формування й розвитку загрози, та дозволяє визначити основні інформаційно-критичні елементи політичної системи з урахуванням інформаційно-ресурсного потенціалу;

дістали подальшого розвитку:

– зміст напрямів створення державної системи реагування на інформаційно-психологічні контентні загрози, яка забезпечує інформаційну та роз'яснювальну роботу органів державної влади та місцевого самоврядування щодо культури інформаційної безпеки та поєднує в собі єдиний реєстр ресурсів, котрі містять протиправну інформацію; систему аналітики інформації на наявність протиправного контенту; програму з використанням контентної фільтрації, та яка уможливорює блокування протиправного контенту;

– стратегічні орієнтири захисту єдиного інформаційного простору України в умовах гібридних загроз, котрі базуються на прогнозуванні, виявленні та оцінці джерел і характеру інформаційно-політичних загроз, основних суб'єктів інформаційно-політичного впливу та інформаційно-критичних елементів політичної системи, що в сукупності забезпечує захист інформаційної інфраструктури України в цілому й інформаційної інфраструктури політичної системи зокрема від негативних інформаційних впливів;

– змістовно-категорійний апарат науки «Публічне управління та адміністрування» через уточнення сутнісної характеристики таких понять: *«інформаційна безпека держави»* в якості стійкого стану інформаційної сфери, котрий спрямований на сприяння гармонізації процесів розвитку інформаційного суспільства через забезпечення своєї цілісності та захисту об'єктів за наявності зовнішніх і внутрішніх впливів несприятливого характеру як результат усвідомлення соціальними суб'єктами своїх життєво важливих

інтересів, цінностей та цілей розвитку; *«інформаційно-критично важливий елемент політичної структури»* як акт маніпуляційного інформаційного впливу, щодо якого порушено (чи припинено) функціонування інформаційної складової, що, своєю чергою, може призвести до втрати керованості в масштабах країни або окремої частини її території, а також до важких дисфункцій в інфраструктурі та економіці на тривалий період.

Практичне значення одержаних результатів дослідження полягає в обґрунтуванні та розробці пропозицій, орієнтованих на вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз. З наукових праць, опублікованих у співавторстві, використано лише ті положення, які є результатом особистої роботи здобувача, що полягає у дослідженні комплексу питань, пов'язаних з удосконаленням механізмів розвитку інформаційних технологій в контексті модернізації політики інформаційної безпеки.

Розробки, представлені в дисертаційному дослідженні, знайшли практичне застосування в діяльності Департаменту культури і туризму обласного комунального закладу «Харківський організаційно-методичний центр туризму» Харківської обласної військової адміністрації в контексті підвищення результативності функціонування державної системи реагування на інформаційно-психологічні контентні загрози (довідка про впровадження № 26/15 від 21.04.2026 р.), у Національному агентстві акредитації України Міністерства економіки, довкілля та сільського господарства України щодо впровадження теоретичного підходу до модернізації державної політики у сфері інформаційної безпеки (довідка про впровадження № 20-06К від 20.05.2026 р.), а також у Директораті європейської та євроатлантичної інтеграції Міністерства освіти і науки України (довідка про впровадження № 2/43-26 від 22.05.2026 р.) щодо формування державної політики у сфері інформаційної безпеки.

Повнота викладення наукових положень, висновків та рекомендацій в опублікованих працях дисертанта.

Основні наукові положення та здобутки дисертаційного дослідження викладено у 11 публікаціях, із них 5 статей – у фахових журналах і збірниках

наукових праць; 6 – тези доповідей на конференціях. Загальний обсяг публікацій становить 4,5 авт. арк.

Загальні висновки до дисертації відповідають її змісту, конкретно висвітлюючи отримані наукові та практичні результати. Слід зазначити, що дисертація є закінченою науковою працею, в якій містяться нові наукові доробки, що мають певну теоретичну та практичну цінність.

Дискусійні положення та зауваження щодо дисертаційного дослідження.

Позитивно оцінюючи в цілому рецензоване дисертаційне дослідження Кушнікова В.В. «Управління інформаційною безпекою держави в умовах гібридних загроз», стало можливим висловити певні зауваження та вказати на дещо дискусійний характер окремих положень:

1. У дисертаційній роботі показано, що необхідним є комплексне дослідження й оцінювання організаційно-правових механізмів протидії використанню інформаційно-комунікаційних технологій у терористичних цілях щодо комп'ютерної та інформаційної інфраструктури, проте не зовсім чітко розкрито цілі такого дослідження.

2. Доцільно було б докладніше розкрити стратегічні пріоритети протидії інформаційно-політичним загрозам (стор. 199–200 дисертації).

3. Потребують додаткової деталізації ознаки впливу на інформаційно-критичні елементи політичної системи України через Інтернет (стор. 201 роботи).

4. У дисертаційній роботі недостатньо докладно описано послідовність етапів формування системи протидії тероризму в інформаційному просторі.

Але, в цілому, зазначені зауваження та дискусійний характер певних суджень автора не знижують загальну позитивну оцінку дисертаційної роботи.

Загальна оцінка дисертаційної роботи.

Дисертаційна робота є завершеним науковим дослідженням, що вирішує поставлене наукове завдання, яке полягає в обґрунтуванні науково-теоретичних підходів та розробці практичних рекомендацій вдосконалення процесів управління інформаційною безпекою держави в умовах гібридних загроз.

Представлена дисертаційна робота на тему: «Управління інформаційною безпекою держави в умовах гібридних загроз» відповідає вимогам постанови Кабінету Міністрів України «Про затвердження порядку присудження наукового ступеня доктора філософії» від 12 січня 2022 року №44, а її автор, Кушніков Вадим Вадимович, заслуговує на присудження наукового ступеня доктора філософії в галузі управління та адміністрування (спеціальність 281 – публічне управління та адміністрування).

Офіційний рецензент:
кандидат наук з державного
управління, доцент,
доцент кафедри економіки та
публічного управління
Національного аерокосмічного
університету «Харківський
авіаційний інститут»

Надія КАРПЕКО