

Голові спеціалізованої вченої ради
Д 64.707.03 Національного університету
цивільного захисту України,
д.держ.упр., професору, заслуженому
працівнику освіти України
Світлані ДОМБРОВСЬКІЙ

ВІДГУК

офіційного опонента доктора наук з державного управління, професора **Щепанського Едуарда Валерійовича** на дисертацію Новікова Владислава Олександровича «Інституційні механізми публічного управління в умовах інформаційно-гібридних війн», подану до захисту у спеціалізовану вчену раду Д 64.707.03 Національного університету цивільного захисту України на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку

Актуальність теми дисертації, її зв'язок з науковими програмами, планами, темами. Стрімкий розвиток інформаційних технологій, що зумовлюють збільшення можливостей щодо застосування різних засобів впливу на людську свідомість (у тому числі заборонених), загрожує зниженню рівня інформаційної безпеки. Сфера її дії не має чітких меж, окрім як національні інтереси, що включають державні, суспільні й окремо взятої особистості. На жаль, Україна змушена відчувати на собі негативний вплив розвитку новітніх технологій та інформаційних загроз, що трансформувалися в гібридну війну, яка ведеться з боку рф останніми роками. Ці процеси почалися задовго до відкритої зовнішньої агресії у 2014 р. і повномасштабної війни у 2022 р. Увесь час із моменту проголошення незалежності нашої держави рф планомірно створювала необхідне підґрунтя для дестабілізації соціальної безпеки в Донецькій і Луганській областях, Автономній Республіці Крим та інших вітчизняних регіонах. Як результат, держава-

агресор мала підтримку серед частини українців, які були «проросійсько» налаштовані. Усе це відбулося насамперед через вдале використання новітніх технологій та інформації загалом. Саме дослідженню цих аспектів присвячена тема опонованої дисертаційної роботи, які є злободенним проблемними питаннями для України, що потребують нагального та системного вирішення. Інакше наша держава не буде визнаватися дієвим гравцем на міжнародній арені, і не матиме повагу власних же громадян, серед яких поширюватимуться соціальна апатія, хаос, конфлікти та інші негативні процеси й явища.

Таким чином, сьогодні варто говорити про проблеми інформаційного захисту громадян, відповідно до сучасного суспільного запиту й загроз, що вимагають механізмів протидії негативному інформаційному впливу на індивідуальну, групову та суспільну свідомість. Ці механізми передбачають удосконалення системи забезпечення публічного управління інформаційною безпекою суспільства України в умовах інформаційно-гібридної війни. У той же час, потрібно розуміти, що в середньостроковій перспективі вітчизняним органам публічної влади повинні застосовувати заходи системного забезпечення національної й інформаційної безпеки. На ці вектори розвитку інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і звертає увагу дисертант, обґрунтовуючи сценарії реагування на ці війни – проактивний і реактивний (с. 153, 154, 159 тощо). Їхня реалізація на сучасному етапі розвитку та в майбутньому України дозволить підвищити рівень національної й інформаційної безпеки суспільства у системі публічного управління, що забезпечить реалізацію конституційних прав і свобод людини та громадянина, сталий соціально-економічний розвиток, обороноздатність і безпеку нашої держави.

Крім того, тема дисертаційного дослідження є актуальною та практично значущою, що, зокрема, підтверджується зв'язком з науково-дослідними роботами за темою «Розробка наукових основ державного управління у сфері безпеки ринку соціально-економічних послуг України з

точки зору цивільного захисту» (ДР № 0115U002035). У процесі виконання вищезазначеної науково-дослідної роботи дисертантом визначено формування інституційних механізмів публічного управління невизначеностями в умовах інформаційно-гібридних війн, розкрито актуальні проблеми публічного управління в період інформаційно-гібридної війни.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, їх вірогідність. Вивчення дисертації Новікова В.О. дає підстави для висновку про те, що наукові положення, висновки та рекомендації є обґрунтованими та достовірними, містять наукову новизну. Теоретико-методологічною основою дисертаційного дослідження стали фундаментальні положення теорії державного управління, відповідні дослідження вітчизняних та зарубіжних учених. Нормативно-інформаційну базу дисертації склали закони України, укази Президента України, нормативно-правові акти Кабінету Міністрів України, органів державної влади України, матеріали та результати особистих напрацювань автора, а також зарубіжні та вітчизняні джерела з досліджуваної проблематики. Це підтверджується кількістю (225 найменувань) опрацьованих здобувачем наукових праць та проаналізованих нормативно-правових актів.

Сформульована, дисертантом, мета дисертаційної роботи, а саме: визначення науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розроблення практичних рекомендацій щодо вдосконалення таких механізмів в Україні – повністю досягнута, розкрита та логічно висвітлена у змісті дисертації.

Тема та структура дисертації є взаємозумовленими та логічно пов'язаними. Дослідження містить чіткий розподіл тексту дисертації на окремі частини, що структурно підпорядковані між собою та відображають загальну цілісну ідею дослідження. Такий підхід до викладення матеріалу

сприяв цілісності розгляду порушеної проблематики та системності висновків за результатами дослідження.

Перший розділ дослідження присвячено теоретичним засадам соціо-гуманітарних технологій сучасних інформаційно-гібридних війн у системі публічного управління. У підрозділі 1.1 автором розкрито особливості феномену інформаційно-гібридної війни як інструменту соціо-гуманітарного протиборства в системі публічного управління (с. 25-30). Узагальнено існуючі у науковій літературі підходи до трактування поняття «інформаційна безпека» (державницький, філософсько-гуманітарний, екологічний та інші підходи). Результатом урахування положень цих підходів, а також застосування системного підходу є надане автором уточнене визначення поняття інформаційної безпеки (с. 75, 117). При цьому автор слушно визначив ключове завдання системи публічного управління у сфері забезпечення інформаційної безпеки, що полягає в нейтралізації негативного впливу інформаційно-психологічної війни, пропаганди щодо нівелювання української мови та культури, унеможливлення формування російськими ЗМІ альтернативної інформаційної дійсності шляхом викривленої справжньої картини світу, підвищення позитивного іміджу України на міжнародній арені. Зазначено основні фактори виникнення інформаційно-гібридних війн і їхній вплив на систему публічного управління.

У підрозділі 1.2 розглянуто структурно-функціональний механізм виникнення інформаційних війн у глобалізованому світі, а також турбулентність сучасного етапу світового розвитку, яка характеризується швидкими змінами, нестабільністю та великою кількістю невизначеностей, що ускладнює передбачення та управління сучасним світом (с. 40-45). Доведено, що головною небезпекою інформаційно-гібридної війни є потенційна можливість цільового інформаційного, у тому числі негативного, впливу на об'єктивно закладені та наявні суперечності практично на всіх рівнях державного та суспільного устрою у будь-якій

країні чи регіоні з метою їх примусового прояву із заданим рівнем інтенсивності та у завідомо визначеному напрямку (с. 37). Визначено наслідки інформаційно-гібридних війн, що впливають на політичну, економічну, соціальну та військову ситуацію в країні або регіоні. При цьому автором виокремлено завдання, які вирішують сили і засоби інформаційної війни з початком військових дій (с. 40-41). Наголошено на тому, що деструктивні фактори гібридної війни можуть призводити до загрози порушення прав людини, зниження якості життя та загальної стабільності суспільства. Життя особистості в умовах гібридної війни змушує людину перебувати в стані постійного емоційного напруження.

Підрозділ 1.3 присвячено механізмам формування інформаційної реальності як чинника забезпечення національної безпеки (с. 49-60). У підрозділі виділено три складові у забезпеченні такої безпеки: можливість перенесення психології конфлікту в інформаційний простір (с. 50), маніпулювання світовими фінансами та дестабілізація фондового ринку (с. 51) та масове культивування серед окремих груп (на основі врахування їх соціальних та національних особливостей) певного способу життя та стилю соціальної поведінки (с. 51).

Другий розділ дослідження присвячено сучасному стану функціонування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн. У підрозділі 2.1 розглянуто сутнісні характеристики понять «інформаційний ризик», «інформаційна небезпека», «інформаційна загроза» (с. 66-80). Зокрема, це здійснено з позиції дослідження особливостей і ризиків функціонування інституційних механізмів публічного управління України в умовах інформаційно-гібридної війни (рис. 2.1, 2.2). У цьому контексті автором визначено, по-перше, що інституційні механізми публічного управління в умовах інформаційно-гібридних загроз і війн безпосередньо пов'язані з ключовими категоріями «правовий інститут» та «інституції» (органи публічної влади), а, відтак, з

процесами щодо формування правових інститутів, удосконалення структури та діяльності цих органів (с. 70). А по-друге, функціональну карту інституційної реалізації публічного управління в умовах загроз інформаційного характеру й інформаційно-гібридної війни в Україні (табл. 2.1).

Підрозділ 2.2 присвячено аналізу сучасної концепції інформаційно-гібридної війни. У ньому зазначено, що методи деструктивного інформаційного впливу постійно еволюціонують, оскільки з'являються нові технології та можливості для розповсюдження дезінформації, маніпуляцій і здійснення кібератак і кібероперацій (с. 90, 92 тощо). Виділено види війн, зокрема, традиційні та нетрадиційні, до останніх належать інформаційно-гібридні (с. 85-87). Захист суспільної свідомості від негативних інформаційних впливів є важливим завданням у сучасному світі, тому автором слушно визначено шляхи забезпечення цього захисту. При цьому дисертант зауважує, що методи протидії інформаційним загрозам зміщується у бік широкого застосування політичних, економічних, інформаційних, гуманітарних та інших невійськових заходів, що реалізуються із залученням протестного потенціалу населення (с. 89).

У підрозділі 2.3 проаналізовано визначено інструменти дисфункціоналізації інституційних механізмів публічного управління в умовах інформаційно-гібридної війни (с. 98-115). Серед цих інструментів автор виокремлює технології «м'якої» і «жорсткої» сили. Зазначено, що технологіям «м'якої сили» варто відводити особливе місце, тому що вони передбачають здійснення щодо держави-об'єкта (держави-мішені) неоголошеної гібридної війни з боку держави-актора, нейтралізувати негативний інформаційний вплив якої рекомендовано із застосуванням ризик-орієнтованих підходів, напрацьованих за кордоном (с. 99-102). Крім того, автор наполягає на забезпеченні публічними інституціями розвитку «інформаційного суспільства» (с. 11-112).

Останній розділ дослідження присвячено пріоритетним напрямкам вдосконалення інституційних механізмів публічного управління в умовах інформаційно-гібридних війн.

У підрозділі 3.1 проаналізовано основні підходи публічного управління щодо забезпечення інформаційної безпеки суспільства в умовах інформаційно-гібридних війн, що (підходи) мають взаємодіяти та поєднуватися для створення комплексної системи публічного управління інформаційною безпекою (с. 121-137). Серед цих підходів автором ключове місце відведено ризик-орієнтованим підходам, що мають упроваджуватися із урахуванням міжнародних стандартів ISO 73:2009. Застосування запропонованих наукових підходів дозволило обґрунтувати особливості прогнозування розвитку інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління на пострадянському просторі (с. 159, 160 тощо). При цьому автором наполягається на комплексному вирішенні проблем, пов'язаних із обставинами декларативного законодавчого визначення гібридних й інформаційно-гібридних війн в Україні, що можливо, зокрема, шляхом розробки та впровадження Концепції інформаційної безпеки України (с. 127, 129). Ця Концепція має враховувати сутність спеціальних понять «інформаційні війни», «терористичні війни», «біологічні війни», «кібервійни», «прикордонні війни», «санкційні війни» та ін., що набувають у сучасних реаліях іншого значення (с. 128, 131, 132 тощо).

У підрозділі 3.2 обґрунтовано шляхи вдосконалення інституційної системи публічного управління України в умовах інформаційно-гібридних війн (с. 138-156). Серед цих шляхів виокремлено ті, що пов'язані із реалізацією «проактивного» або «реактивного» сценарію функціонування інституційної системи публічного управління. Акцентовано, що для будь-якої держави важливе значення мають насамперед сценарії, які супроводжуються стратегічним плануванням і поступальним забезпеченням

сталого розвитку. У дисертації обґрунтовано необхідність створення єдиного координаційно-аналітичного центру/ради в Україні, на зразок американського Бюро протидії гібридній війні, яке напрацювало дієві управлінські практики реагування на інформаційні загрози, а також налагодження результативної взаємодії України з іншими державами та міжнародними організаціями в напрямку вчасного протистояння цим загрозам (с. 176-177 тощо).

У підрозділі 3.3 визначено концептуальні засади прогнозування інформаційно-гібридних війн у контексті розвитку інституційних механізмів публічного управління (с. 159-179). Автор висловив гіпотезу та довів її щодо тенденцій розвитку інформаційно-гібридних війн на пострадянському і вітчизняному просторі, на які впливають зовнішні та внутрішні фактори. Серед них найбільш загрозливими на сучасному етапі визнано соціальні, пов'язані з рівнем міграції громадян, їхнього добробуту, безробіття, демографічного розвитку та ін.

Таким чином у дисертації успішно здійснено теоретичне узагальнення та розв'язання наукового завдання, яке полягає у визначенні науково-теоретичних засад формування інституційних механізмів публічного управління в умовах інформаційно-гібридних війн і розробленні практичних рекомендацій щодо вдосконалення таких механізмів в Україні.

Достовірність та наукова новизна результатів дослідження, повнота їх викладу в опублікованих працях. Достовірність положень, висновків і рекомендацій, наведених у дисертації забезпечена системним комплексним використанням дисертанткою наукової методології.

Також достовірність одержаних результатів підтверджується їх успішною практичною апробацією. Так, окремі положення та висновки дисертаційного дослідження були використані: у роботі Управління Служби безпеки України в Харківській області (довідка № 70/4-8859-1 від

14.11.2022 р.); у роботі і Черкаської районної ради (довідка № 10/01-13 від 06.02.2024 р.); у навчальному процесі Національного університету цивільного захисту України, зокрема, при викладанні здобувачам вищої освіти другого (магістерського) рівня вищої освіти (спеціальність 281 «Публічне управління та адміністрування») таких дисциплін, як «Інформаційна політика в Україні» і «Сучасні геополітичні процеси: світ і Україна» (акт № 22-20 від 28.11.2023 р.).

Основні положення та результати дисертаційної роботи представлено в 11 наукових працях, із них: 6 статей у вітчизняних наукових фахових виданнях, включених до категорії Б; 1 стаття у закордонному науковому виданні за напрямком дослідження; 4 тез доповідей на конференціях. Одержані в дисертації наукові результати та висновки достатньою мірою апробовані в тезах доповідей і виступах на науково-практичних міжнародних і вітчизняних конференціях.

Оцінка ідентичності автореферату та основних положень дисертації. Дисертація та автореферат оформлені відповідно до вимог Порядку присудження наукових ступенів МОН України. Зміст автореферату ідентичний основним положенням дисертації та не містить інформації, відсутньої в дисертації. Наведені в авторефераті наукові положення, висновки та рекомендації розкриті й аргументовані в тексті дисертаційної роботи.

Дисертація виконана у формі рукопису. Дисертаційна робота складається з анотації, вступу, трьох розділів, логічно об'єднаних у 9 підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 218 сторінок, із них 186 сторінок основного тексту. Список використаної літератури налічує 225 найменувань і займає 24 сторінки. Дисертація містить 5 додатків, а також 4 рисунки і 1 таблицю.

Значення одержаних результатів для науки і практики та рекомендації щодо їх можливого використання. Основні теоретичні положення, рекомендації, висновки дисертації щодо обґрунтування організаційних засад публічного управління у сфері забезпечення інформаційної безпеки в умовах інформаційно-гібридної війни, сприяють розвитку теорії державного управління та місцевого самоврядування у сфері національної й інформаційної безпеки України. Окремі аспекти дисертаційної роботи є основою для вирішення практичних завдань і можуть бути використані органами державної влади та органами місцевого самоврядування, іншими державними і громадськими інституціями при розробленні законодавчих та нормативно-правових актів.

Перспективами реалізації науково-методичних аспектів дисертаційної роботи є розробка фундаментальних праць в галузі державного управління та місцевого самоврядування, інформаційної політики, теорії управління, у законотворчій діяльності, що стосується розвитку регулювання сфери інформаційної безпеки України.

Дискусійні положення та зауваження щодо змісту дисертації. Відзначаючи загальний високий рівень обґрунтованості теоретико-методологічних положень дисертаційної роботи, її цілісність та логіку викладення матеріалу, але тим самим доречно зробити декілька зауважень і звернути увагу на дискусійні положення дисертаційної роботи.

1. На с. 117 дисертант визначає, що вдосконалив визначення інформаційної безпеки, яка передбачає застосування комплексу заходів із метою унеможливлення трансформації ризиків і загроз інформаційного характеру у небезпеки для *країни* та війни. Уважаємо, що заміна слова «державна» на «країна» у даному визначенні є недоцільною, зважаючи на відмінність цих понять. Країна – це заселена територія з визначеними кордонами, яка може бути частиною іншої держави, і при цьому не залежати

від останньої. Держава ж представляє собою суверенне політичне утворення, що має особливу систему органів й організацій, що здійснюють свої повноваження в окремо взятому регіоні або в масштабах усієї держави. У державі, на відміну від країни, наявна верховна влада та правові норми, установлені нею. Разом із тим, у тексті дисертації неодноразово зустрічається формулювання щодо стану захищеності саме держави та її системи безпеки від інформаційних загроз, наприклад, на рис. 2.2. На цій підставі вважаємо, що дисертанту слід уніфікувати термінологію, якою він послуговується в дослідженні.

2. Слід також вказати на ще одне зауваження, яке стосується термінології, що використана дисертантом. На с. 53 він послуговується терміном «злив наявної інформації». Не можемо однозначно погодитися з даною позицією автора щодо необхідності введення в науковий обіг такого спеціального поняття. На наше переконання, коректніше застосовувати терміноконструкції, які вже наявні в науковому обігу, а саме: унеможливлення «відтоку інформації», формування у цьому контексті «культури інформаційної безпеки» тощо.

3. На с. 118 автор зазначає, що «ризики в системі публічного управління чинять істотний вплив на всі сфери суспільної життєдіяльності, позначаючись негативно на соціальній свідомості інформаційної безпеки». На нашу думку, це не дуже вдале визначення. У безпеки не може бути свідомості, безпека це насамперед стан об'єкту захисту. Тому, на наш погляд, доцільно було б назвати це інформаційною культурою користувача.

4. На с. 131–132 автор стверджує, що однією з найбільш стратегічних проблем державного значення є кібербезпека, захист персональних даних тощо. Твердження, що саме кібербезпека – це стратегічна, тобто довгострокова державна проблема, є суб'єктивною позицією, яка потребує додаткового обґрунтування.

5. На рис. 2.3 дисертації розглядаються види війни, і зазначено їхні наслідки, що впливають на політичну, економічну, соціальну, військову та ін. ситуацію в країні або регіоні. В історіографії проблем гібридної війни визнано, що гібридна війна має не види, а виміри: воєнний, дипломатичний, політичний, правовий, психологічний, фінансово-економічний, соціальний, ідеологічний, інформаційний. Як правило, гібридна війна реалізується через поєднання всіх цих вимірів у різних масштабах, а проксі війна є частиною гібридної війни, її військова складова. На цій підставі вважаємо, що потребує уточнення зазначена позиція автора.

Разом із тим, висловлені зауваження та рекомендації носять переважно дискусійний характер і не знижують загального високого теоретико-методологічного рівня представленої дисертаційної роботи.

Загальний висновок та оцінка дисертації. З огляду на актуальність, новизну, важливість одержаних автором наукових результатів, їх обґрунтованість і достовірність, а також практичну цінність сформульованих положень і висновків вважаємо, що дисертаційна робота Новікова Владислава Олександровича «Інституційні механізми публічного управління в умовах інформаційно-гібридних війн» є самостійним, завершеним науковим дослідженням, у якому вирішено актуальне завдання щодо обґрунтування концептуальних засад розвитку інституційної системи публічного управління в умовах інформаційних загроз, проаналізовано сучасний стан та розроблено практичні рекомендації щодо удосконалення цієї системи, спрямованої на забезпечення інформаційної безпеки суспільства, що в сукупності має суттєве значення для галузі науки «Публічне управління та адміністрування».

На підставі вищезазначеного можна зробити висновок, що дисертаційна робота відповідає п. 11 Порядку присудження наукових

ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (зі змінами), а її автор – Новіков Владислав Олександрович – заслуговує на присудження наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку.

Офіційний опонент:

завідувач кафедри публічного управління та адміністрування Хмельницького університету управління та права імені Леоніда Юзькова, доктор наук з державного управління, кандидат економічних наук, професор

Едуард ЩЕПАНСЬКИЙ

Підпис *Едуарда Щепанського*
ЗАСВІДЧУЮ:
Нач. ВК ХУУП
імені Леоніда Юзькова *Едуард Щепанський*