Голові разової спеціалізованої вченої ради ДФ 20.051.170 Карпатського національного університету імені Василя Стефаника
доктору наук з державного управління, професору, професору кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника
Сурай Інні Геннадіївні

РЕЦЕНЗІЯ

доктора наук з державного управління, професора кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника
Дєгтяра Олега Андрійовича
на дисертаційну роботу Лазаріва Владислава Олеговича
на тему**: «*Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід*»** подану до захисту в разову спеціалізовану вчену раду Карпатського національного університету імені Василя Стефаника на здобуття ступеня доктора філософії з галузі знань 28 Публічне управління та адміністрування за спеціальністю 281 Публічне управління та адміністрування

Актуальність теми дисертаційного дослідження Актуальність теми дисертаційного дослідження зумовлена трансформаційними процесами у сфері цифрового врядування, які супроводжуються масштабним впровадженням електронних сервісів у практику публічного управління та комунікації між державою і суспільством. Поглиблення цифровізації створює якісно нові можливості для прозорості, відкритості та підзвітності публічних інституцій, проте одночасно формує спектр нових загроз, що безпосередньо впливають на інформаційну безпеку держави, органів влади та громадян. Зростання ризиків несанкціонованого доступу до інформації, кібератак на критичну цифрову інфраструктуру, порушення конфіденційності та цілісності даних актуалізують потребу у створенні ефективної системи захисту електронних послуг.

Особливого значення ця проблематика набуває в умовах триваючої воєнної агресії проти України, яка супроводжується широким застосуванням інформаційно-психологічних операцій, кіберагресії та технологічних

диверсій, спрямованих на дестабілізацію цифрового середовища. Відновлення та модернізація державних інституцій післявоєнного періоду вимагають стратегічного посилення стійкості інформаційних систем, підвищення рівня кіберзахищеності електронних послуг і формування комплексних механізмів публічного управління у цій сфері.

Таким чином, актуальність дослідження визначається необхідністю наукового обґрунтування та практичної розробки механізмів публічного управління інформаційною безпекою електронних послуг, що здатні забезпечити їх безперервність, функціональну надійність і відповідність європейським стандартам цифрової стійкості та захисту персональних даних.

Ступінь обґрунтованості й достовірність основних наукових положень, висновків і рекомендацій сформульованих в дисертації.

Дисертаційне дослідження виконано на високому теоретико-методичному та прикладному рівнях, відзначається чітко вибудуваною логікою побудови, послідовним викладом результатів і спрямованістю на реалізацію визначеної мети. Сформульовані мета та завдання дослідження корелюють з об'єктом і предметом дослідження та перебувають у логічному взаємозв'язку з положеннями наукової новизни. Така узгодженість забезпечує цілісність дисертаційної роботи та належний рівень обґрунтованості отриманих наукових результатів.

Для досягнення мети дисертаційного дослідження та реалізації сформульованих завдань використано інтегрований комплекс загальнонаукових і спеціалізованих методів, спрямованих на цілісне, системне й багаторівневе осмислення природи, змісту, структурної організації та особливостей функціонування механізмів публічного управління інформаційною безпекою у системі надання електронних послуг. На етапі обґрунтування теоретико-методичних засад застосовано методи аналізу, синтезу, індукції, дедукції, узагальнення, систематизації та логічного структурування, що дало змогу здійснити глибоку критичну інтерпретацію наукових концепцій, нормативно-правових підходів і практичних рішень у сфері публічного управління інформаційною безпекою. З метою конкретизації понятійно-категоріального апарату дослідження, розкриття структури, характеристик і функціонального змісту механізмів публічного управління інформаційною безпекою було використано методи класифікації, типологізації, функціонального аналізу, а також гносеологічні підходи до пізнання. Їх застосування забезпечило виявлення внутрішніх взаємозв'язків та причинно-наслідкових залежностей між елементами досліджуваного управлінського феномену, що стало підґрунтям для формування системного бачення об'єкта дослідження. Під час опрацювання світового досвіду побудови та реалізації механізмів публічного управління у сфері інформаційної безпеки електронних сервісів використано методи

компаративного аналізу, узагальнення міжнародних статистичних даних, нормативних документів і практичних кейсів. Це дозволило виокремити результативні моделі управлінських механізмів, релевантні сучасним викликам цифрової безпеки та умовам функціонування систем електронного врядування. У третьому розділі, орієнтованому на розробку напрямів підвищення результативності запровадження механізмів публічного управління інформаційною безпекою електронних послуг, застосовано методи моделювання, прогнозування, сценарного аналізу та стратегічного планування. Їх використання базується на оцінці актуальних трендів у сфері інформаційної безпеки, адаптації провідних міжнародних практик до українських реалій, а також на узагальненні результатів попереднього емпіричного дослідження.

Сукупність застосованих методів дала можливість сформувати концептуальну модель механізмів публічного управління, орієнтовану на забезпечення стійкості, адаптивності та результативності функціонування системи надання електронних публічних послуг в умовах цифрової трансформації, воєнних загроз і потреб післявоєнного відновлення.

Розділ 1. У розділі здійснюється критичний аналіз та систематизація існуючих наукових підходів до розуміння сутності, змісту та класифікації механізмів публічного управління в контексті забезпечення інформаційної безпеки електронних послуг. Проводиться порівняння різних концепцій, моделей та теоретичних шкіл, які інтерпретують роль держави, інституцій публічної влади та зацікавлених сторін у формуванні й реалізації відповідних механізмів. Сормовано й уточнено ключові поняття, що становлять концептуальне ядро дослідження. Аналізуються існуючі дефініції, їхні відмінності та обмеження, пропонуються авторські трактування з урахуванням сучасних викликів цифровізації, кіберзагроз та трансформації системи електронного врядування. Уточнення понятійно-категоріального апарату слугує основою для подальшого теоретичного моделювання й практичних рекомендацій.

У другому розділі «Кращі світові практики публічного управління інформаційною безпекою надання електронних послуг» здійснюється оцінка сучасного стану публічного управління інформаційною безпекою електронних послуг у державах – членах Європейського Союзу, США та азійських країнах. Аналізуються нормативно-правові рамки, інституційні моделі, стратегічні документи, стандарти та практичні інструменти, що регулюють сферу інформаційної безпеки. Розглядаються специфіка державної політики, роль національних регуляторів, стратегій кібербезпеки, а також технологічні й організаційні інновації, що впроваджуються для захисту електронних сервісів. На цій основі обґрунтовуються принципи та орієнтири, які доцільно врахувати під час розробки моделі механізмів публічного управління інформаційною безпекою електронних послуг в Україні.

У розділі 3 «Модель механізмів публічного управління інформаційною безпекою електронних послуг в Україні в умовах цифрової трансформації» розглядаються нормативно-правові засади, інституційна структура, організація

взаємодії між органами державної влади, органами місцевого самоврядування та іншими суб'єктами у сфері інформаційної безпеки. Оцінюється ефективність наявних механізмів, виявляються прогалини, дублювання функцій, ризики та виклики, посилені цифровою трансформацією та воєнними діями. Обґрунтовуються підходи до впровадження інноваційних форм та інструментів публічного управління в системі забезпечення інформаційної безпеки електронних послуг. Розглядаються можливості застосування цифрових платформ, інтелектуальних систем моніторингу, методів управління ризиками, а також механізмів публічно-приватного партнерства в сфері кібербезпеки.

Обґрунтованість отриманих результатів підтверджується логічною узгодженістю теоретичних положень, аналітичних висновків і практичних рекомендацій, їх відповідністю меті та завданням дисертаційної роботи, а також апробацією основних положень дослідження у наукових публікаціях і науково-практичних конференціях.

Достовірність та наукова новизна отриманих результатів дисертаційного дослідження.

Наукова новизна дисертаційного дослідження полягає в комплексному теоретико-методичному обґрунтуванні та розробці концептуальних засад механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації, зростаючих безпекових викликів та необхідності адаптації міжнародного досвіду до національного контексту.

уперше:

- обґрунтована модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації, яка має цілісний, багаторівневий і стратегічно орієнтований характер та відображає як національні потреби України, так і кращі міжнародні практики у сфері кіберзахисту, до основних елементів якої віднесені: інституційний механізм у вигляді Національної ради з питань інформаційної безпеки електронних послуг; нормативно-правовий механізм ґрунтується на гармонізації українського законодавства з міжнародними стандартами; фінансовий механізм формує довгострокову та багатоканальну модель фінансування заходів кіберзахисту; кадровий механізм передбачає створення професійного корпусу державних службовців; контрольний механізм передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації; інформаційно-комунікативний механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві;

удосконалено:

- поняття «механізми публічного управління інформаційною безпекою надання електронних послуг» як сукупність взаємопов'язаних нормативно-правових, організаційно-інституційних, технологічних та соціально-комунікативних інструментів, за допомогою яких органи публічної влади формують, реалізують і контролюють політику захисту електронних послуг

від інформаційних загроз, забезпечуючи конфіденційність, цілісність, доступність і довіру до цифрових сервісів;

- систематизація проблем публічного управління інформаційною безпекою надання електронних послуг через виокремлення наступних кластерів: вразливість державних ІТ-систем, які здебільшого проєктувалися у мирний час без урахування масштабних кризових сценаріїв; фрагментація відповідальності між різними суб'єктами; нестача фахівців у державному секторі; запровадження обмежувальних заходів задля захисту національної безпеки та зобов'язання щодо дотримання прав людини і прозорих процедур оскарження; проблема доступу та цифрової рівності, адже перебої в електро-й телекомунікаційних мережах ставлять під загрозу реалізацію базових прав громадян через неможливість отримання електронних послуг; потреба у розробці національної стратегії кіберстійкості та створення багаторівневих резервних механізмів; потреба в удосконаленні нормативного регулювання з гарантіями прав людини, формалізацію публічно-приватного партнерства та посилення координації між організаційними підрозділами або спеціалізованими командами реагування на комп'ютерні надзвичайні події, операторами критичної інфраструктури та правоохоронними органами;

- закономірності публічного управління інформаційною безпекою електронних послуг в Німеччині, Естонії, Данії, Литві, Сінгапурі, Південній Кореї, Тайвані, США та виокремленні наступні: системність у формуванні інформаційної безпеки; чіткі нормативно-правові засади формування інформаційної безпеки; прозорість процедур; розвиток державно-приватного партнерства; обов'язковість виконання вимог до критичної інфраструктури; стійкість та передбачуваність управлінських рішень; побудова національної системи кіберзахисту; координація та контроль у діяльності інституцій; формування культури кібербезпеки та забезпечення довіри громадян до цифрових послуг;

- сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні та сформовані концептуальні засади побудови функціонально-ієрархічної моделі механізмів публічного управління інформаційною безпекою електронних послуг, що враховують як сучасні виклики кіберсередовища, так і потреби стратегічного розвитку цифрового врядування;

- механізми запровадження інноваційного управління в систему інформаційної безпеки електронних послуг в умовах цифрової трансформації, які орієнтуються на принципах «безпеки за дизайном» та «приватності за дизайном» та інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування;

набули подальшого розвитку:

- наукові підходи до механізмів публічного управління інформаційною безпекою надання електронних послуг;

- категоріально-понятійний апарат дослідження, зокрема: поняття «інформаційна безпека електронних послуг» визначено як структурно

інтегрований стан забезпечення конфіденційності, цілісності, доступності та стійкості інформації у процесі надання публічних цифрових сервісів;

- пропозиції щодо імплементації світового досвіду публічного управління інформаційною безпекою надання електронних послуг до національної системи механізмів публічного управління, яка дозволяє адаптувати міжнародні стандарти інформаційної безпеки до українського контексту шляхом інтеграції організаційних, нормативних і цифрових компонентів у цілісну систему публічного управління.

Повнота викладу основних положень дисертації в опублікованих працях.

Аспірант Лазарів Владислав Олегович особисто провів дослідження. За результатами дослідження опубліковано 11 наукових праць загальним обсягом 3,5 друк. арк., що належать особисто автору, з яких: 4 статті у виданнях України, які входять до фахових періодичних видань категорії Б, 7 тез доповідей та матеріалів міжнародних науково-практичних конференцій.

У публікаціях висвітлено ключові аспекти дисертаційної роботи, зокрема положення щодо удосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг. Отримані результати були належним чином апробовані під час участі автора у науково-практичних конференціях, що підтверджує їх наукову обґрунтованість. Зміст анотації дисертації є узгодженим з основними положеннями роботи та відображає її наукові результати.

Оцінка оформлення та змісту дисертації.

Дисертаційне дослідження виконано й оформлено відповідно до чинних вимог Міністерства освіти і науки України, що регламентують підготовку наукових праць на здобуття ступеня доктора філософії. Робота характеризується системною та логічно впорядкованою структурою, що охоплює вступ, три розділи, висновки, список використаних джерел та додатки.

Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 233 сторінки, із них 177 сторінка основного тексту. Список використаних джерел налічує 242 найменувань.

Зміст дисертації повністю відповідає обраній темі, відображає визначену мету та поставлені завдання, забезпечує розкриття наукової новизни й практичної значущості отриманих результатів щодо механізмів публічного управління інформаційною безпекою надання електронних послуг. Матеріал викладено послідовно, аргументовано та з дотриманням

вимог наукового стилю, що забезпечує цілісність сприйняття дослідження та логічну узгодженість його основних положень.

Ілюстративний матеріал та додатки використано обґрунтовано та доцільно, вони доповнюють основний текст і сприяють більш повному, наочному представленню результатів проведеного дослідження.

Практичне значення одержаних результатів дослідження.

Практичне значення отриманих результатів полягає в тому, що теоретичні положення, висновки, практичні рекомендації дисертації можуть бути використані в діяльності центральних органів державної влади для удосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг з урахуванням світового досвіду.

Результати дисертаційного дослідження були використані в діяльності асоціацій, підрозділів органів місцевого самоврядування, ІТ-компаній, закладів вищої освіти, а саме: Івано-Франківського регіонального відділення ВАОМС «Асоціація міст України» (акт впровадження № 131/2025 від 18.09.2025 р.), Департаменту інфраструктури, житлової та комунальної політики Івано-Франківської міської ради (акт впровадження), ТОВ «Н-ІКС ДЕЛІВЕРІ» (довідка № 1-1/19-09/2025 від 19.09.2025 р.), Карпатського національного університету імені Василя Стефаника на кафедрі публічного управління та адміністрування (довідка № 03.04-29/22 від 30.10.2025 р.)

Дискусійні положення щодо змісту дисертаційної роботи.

В цілому, позитивно оцінюючи дисертаційну роботу, необхідно водночас звернути увагу на деякі дискусійні положення.

1. Попри обґрунтовану потребу застосування системного підходу до аналізу механізмів публічного управління інформаційною безпекою, дисертанту слід було звернути увагу на причини, з яких саме цей підхід, а не ризик-орієнтований, інституційний чи соціально-технічний, обрано як базовий методологічний каркас дослідження. Бажаним видається глибше зіставлення альтернативних підходів та аргументація, чому застосування системного підходу забезпечує найбільш повне вирішення поставленої наукової проблеми (розділ 1).

2. У роботі (розділ 2) автором проведено ґрунтовний опис моделей публічного управління інформаційною безпекою в окремих країнах, попри це, доцільно було провести порівняльння кількісних індикаторів (наприклад, рівень інцидентності, витрати на кіберстійкість, індекси цифрової безпеки), які, на наш погляд, могли б підсилити доказову базу та дати змогу об’єктивно оцінити результативність конкретних механізмів у різних юрисдикціях.

3. Запропонована автором концептуальна модель механізмів публічного управління інформаційною безпекою (розділ 3), є структурно деталізованою й комплексною. Однак, варто було б приділити більшу увагу практичним інструментам реалізації моделі, зокрема щодо: етапності

впровадження; інституційного забезпечення координації; механізмів бюджетного формування; потенційних ризиків імплементації .

4. У дисертації автор слушно відзначив зростання ролі інтелектуальних систем у виявленні загроз та управлінні інцидентами. Водночас для повноцінного методологічного обґрунтування запропонованої моделі(розділ 3), враховуючи стрімкий розвиток ШІ, слід було більшу увагу звернути на правові та етичні питання застосування штучного інтелекту.

5. Дисертант послідовно розкриває сутність інформаційної безпеки (розділ 1),однак у роботі не повністю систематизовано співвідношення понять «інформаційна безпека», «кібербезпека» та «кіберстійкість». У ряді випадків ці поняття використовуються як близькі або взаємозамінні, що може створювати термінологічну неоднозначність. Для посилення концептуальної чіткості доцільно провести розмежування цих категорій та пояснити, яку роль кожна з них відіграє у побудові моделі механізмів публічного управління.

В цілому зауваження мають рекомендаційний характер, суттєво не впливають на високу теоретико-методичну та практичну цінність дисертаційного дослідження.

Загальний висновок на дисертаційну роботу.

Дисертаційна робота Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» є цілісним, завершеним і самостійно виконаним науковим дослідженням, присвяченим актуальній проблематиці публічного управління інформаційною безпекою надання електронних послуг. У роботі отримано результати, що характеризуються науковою новизною та мають практичну цінність для формування і реалізації державної політики у сфері публічного управління інформаційною безпекою надання електронних послуг. Дисертація виконана на належному науковому рівні, виклад матеріалу є логічним, послідовним і взаємопов’язаним, а наукові положення, висновки та рекомендації, подані до захисту, є результатом самостійної дослідницької роботи автора. У процесі виконання дисертаційного дослідження здобувачем дотримано принципів академічної доброчесності.

З урахуванням актуальності обраної теми, рівня наукової новизни, теоретичної та практичної значущості отриманих результатів, їх обґрунтованості й достовірності можна дійти висновку, що дисертаційна робота Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» за своїм змістом відповідає спеціальності 281 Публічне управління та адміністрування, а також вимогам до оформлення дисертацій, визначеним наказом Міністерства освіти і науки України від 12 січня 2017 року № 40 (зі змінами) та «Порядку присудження ступеня доктора філософії та скасування

рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 (зі змінами).

Автор дисертаційної роботи Лазарів Владислав Олегович заслуговує на присудження ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування у галузі знань 28 Публічне управління та адміністрування.

Рецензент
доктор наук з державного управління, професор,
професор кафедри публічного управління та
адміністрування
Карпатського національного
університету імені Василя Стефаника Олег ДЄГТЯР