

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**

кандидата економічних наук, доцента,  
декана факультету управління  
Карпатського національного університету імені Василя Стефаника  
П'ятничук Ірини Дмитрівни  
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.** Розвиток інформаційного суспільства та інтенсивне впровадження цифрових технологій формують нову архітектуру цивілізаційного поступу, у межах якої інформація постає як базовий стратегічний ресурс для всіх сфер суспільного життя, зокрема для публічного управління. У країнах із високим рівнем розвитку цифрова трансформація охоплює економічні й соціальні підсистеми, а також інституційні механізми надання електронних публічних послуг. Відповідно, формування та впровадження дієвих механізмів публічного управління інформаційною безпекою стає визначальним фактором забезпечення стабільності та безперервності цифрового розвитку. Система публічного управління у цій сфері виконує функції координації інституційної взаємодії, регламентації управлінських процесів, моніторингу ризиків і розробки адаптивних рішень, що забезпечують належний рівень захищеності інформаційного простору. Рівень цифрової спроможності та суспільної довіри до держави безпосередньо залежить від здатності органів

влади розробляти, впроваджувати й модернізувати механізми публічного управління інформаційною безпекою у сфері електронних послуг. Ці механізми охоплюють нормативно-правові, організаційно-інституційні, технологічні, кадрові та комунікаційні складові, інтегровані в єдину управлінську систему, орієнтовану на протидію загрозам і забезпечення цифрової стійкості. Інформаційна безпека електронних публічних сервісів постає складовою внутрішньої та зовнішньої політики держави, що актуалізує потребу у створенні комплексних і гнучких механізмів публічного управління. Вектор європейської інтеграції України, орієнтація на принципи прозорості, відкритості, підзвітності та безпеки в публічному управлінні зумовлюють потребу у створенні надійних управлінських механізмів, здатних не лише виконувати технологічні й правові функції, а й відображати інституційну відповідальність держави як суб'єкта демократичного врядування у цифрову добу. Загрози інформаційній безпеці набули особливої гостроти в умовах повномасштабної військової агресії російської федерації проти України. До першочергових ризиків віднесено масоване поширення дезінформації, фейкових повідомлень, хакерські атаки на державні ресурси, маніпулятивні технології впливу на громадську думку, незаконний збір та використання персональних даних. У цих умовах завдання із забезпечення стійкості інформаційної інфраструктури, що підтримує функціонування електронних послуг, набуває статусу критично важливого напряму публічного управління. Реалізація такого завдання передбачає системне розгортання комплексних механізмів публічного управління, побудованих на принципах кіберстійкості, правової визначеності, технологічної інноваційності та інституційної кооперації органів державної влади з приватним сектором і громадянським суспільством. Зазначені механізми повинні гарантувати безперервність управлінських процесів, оперативне реагування на загрози, а також прозорість і підзвітність діяльності органів влади у сфері інформаційної безпеки.

Таким чином, формування, впровадження та вдосконалення механізмів публічного управління інформаційною безпекою у сфері електронних послуг в умовах цифрової трансформації та постійних безпекових викликів набуває як теоретичної цінності, так і високої практичної значущості.

### **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 вибудованою 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.

Метою дисертаційного дослідження є обґрунтування та розробка концептуальних теоретико-методичних і науково-практичних підходів до формування, впровадження та вдосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг в умовах цифрової трансформації, гібридних загроз і глобальних безпекових викликів.

Перший розділ «Теоретичні засади механізмів публічного управління інформаційною безпекою надання електронних послуг» присвячено формуванню фундаментального теоретико-методичного підґрунтя дослідження механізмів публічного управління інформаційною безпекою у сфері надання електронних послуг. У цьому розділі здійснено системну реконструкцію наукових підходів до розуміння природи механізмів публічного управління, їх структурної організації та функціонального призначення в умовах цифрової трансформації.

У другому розділі «Кращі світові практики публічного управління інформаційною безпекою електронних послуг» проведено комплексний порівняльний аналіз міжнародних моделей забезпечення інформаційної безпеки у сфері електронних послуг, що дозволило виокремити ефективні управлінські механізми та принципи їх функціонування. Узагальнення світових практик дає змогу окреслити універсальні принципи ефективного управління інформаційною безпекою: стандартизацію, регуляторну визначеність, координацію між суб'єктами, розвиток кадрового потенціалу, інвестиції в інновації та культуру безпеки. Розділ створює аналітичний фундамент для адаптації міжнародного досвіду до українського контексту.

У третьому розділі сформовано авторську концептуальну модель механізмів публічного управління інформаційною безпекою електронних послуг, яка враховує світовий досвід, сучасні виклики, українські інституційні реалії та стратегічні пріоритети цифрової трансформації. Розділ завершується висновками щодо стратегічних орієнтирів формування державної політики у сфері інформаційної безпеки.

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 у систему інформаційною безпекою 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 проектування;

*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 10 наукових праць, що належать особисто автору, з яких: 4 статті у виданнях України, які входять до фахових періодичних видань категорії Б, 6 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.

Дисертаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 233 сторінки, із них 177 сторінок 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. Автор ґрунтовно провів систематизацію підходів до визначення механізмів публічного управління, однак варто було звернути більшу увагу аналізу відмінностей між національними та міжнародними підходами (підрозділ 1.2).

2. У підрозділі 1.2 дефініція «інформаційна безпека електронних послуг» подана комплексно, проте слід було звернути увагу на питання етичної складової захисту даних. В цьому плані, вважаю доцільно визначити чи варто розглядати інформаційну безпеку лише крізь технічний і правовий аспекти, чи доцільно інтегрувати соціально-поведінкові фактори у теоретико-методичне забезпечення цього поняття.

3. Аналіз проблем публічного управління інформаційною безпекою окреслює низку організаційних та технічних бар'єрів, але водночас, на наш погляд, недостатньо акцентована увага на правовій колізії, дублювання норм і розрив між національним та європейським регулюванням (підрозділ 1.3), що не дозволяє повністю оцінити масштаб юридичних чинників, що уповільнюють розвиток системи електронних послуг в Україні.

4. Підрозділ 3.2 переконливо демонструє потенціал інноваційних технологій для управління інформаційною безпекою. Проте, важливо було, більшу увагу приділити питанням ризиків їх застосування та проблемам відповідальності за автоматизовані рішення, помилкових спрацювань систем ШІ, та вказати на потреби у незалежному аудиті алгоритмів та можливих етичних суперечностей.

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

кандидат економічних наук, доцент,  
декан факультету управління  
Карпатського національного університету  
імені Василя Стефаника

Ірина П'ЯТНИЧУК