Голові спеціалізованої вченої ради Карпатського національного університету імені Василя Стефаника ДФ 20 051.170, д.держ.упр., проф.
Сурай Інні Геннадіївні

ВІДГУК

офіційного опонента доктора наук з державного управління, професора Пархоменко-Куцевіл Оксани Ігорівни на дисертаційну роботу Лазаріва Владислава Олеговича на тему: «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід», поданої до захисту у спеціалізовану вчену раду Карпатського національного університету імені Василя Стефаника на здобуття наукового ступеня доктора філософії за спеціальністю 281 – публічне управління та адміністрування

Актуальність теми дисертації, зв'язок з науковими програмами, темами

Стрімка цифрова трансформація публічного управління, зокрема перехід до електронних форм надання адміністративних послуг, зумовлює якісно нові виклики у сфері захисту інформації та забезпечення довіри громадян до державних інституцій. Розширення обсягів електронної взаємодії між органами влади, бізнесом і населенням супроводжується зростанням ризиків несанкціонованого доступу до персональних даних, кібератак, маніпуляцій інформаційними ресурсами та порушення цілісності державних інформаційних систем. За таких умов інформаційна безпека стає не лише технічним завданням, а й ключовою управлінською функцією, що потребує системних, інституційно врегульованих механізмів публічного управління.

Світова практика демонструє різноманіття моделей і інструментів забезпечення інформаційної безпеки електронних послуг — від комплексних національних стратегій кібербезпеки та чітких регуляторних рамок до міжвідомчої координації, державно-приватного партнерства і впровадження принципів «безпека за замовчуванням» та «орієнтація на користувача». Досвід провідних держав свідчить, що ефективність електронного урядування безпосередньо залежить від якості управлінських рішень у сфері інформаційної

безпеки, рівня інституційної спроможності органів публічної влади та узгодженості національних підходів із міжнародними стандартами.

Для країн, що перебувають у процесі євроінтеграції та одночасно стикаються з гібридними загрозами й кіберпросторовими викликами, особливого значення набуває осмислення та адаптація світового досвіду публічного управління інформаційною безпекою електронних послуг. Це створює наукове підґрунтя для формування ефективних механізмів державної політики, здатних забезпечити стійкість цифрових сервісів, захист прав громадян і стабільне функціонування публічної адміністрації в умовах зростаючої цифрової взаємозалежності.

За таких умов дисертаційна робота Лазаріва Владислава Олеговича є важливим кроком в науковому обґрунтуванні механізмів публічного управління інформаційною безпекою надання електронних послуг з урахуванням світового досвіду. Відтак, робота є актуальною та має вагоме наукове значення.

Дисертаційна робота виконана відповідно до плану науково-дослідних робіт Карпатського національного університету імені Василя Стефаника за темою: «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (номер 21 державної реєстрації 0120U100494).

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

Автором розглянуто та використано ґрунтовні наукові дослідження з історії, теорії та методології державного управління й суспільствознавчих наук, що сприяло формуванню специфічного поля дослідження та виробленню системного підходу до аналізу предмету дослідження. Джерельну базу дослідження склали загальнодержавні законодавчі та нормативно-правові документи, зокрема: закони України, укази Президента України, постанови та розпорядження Кабінету Міністрів України, міжнародні угоди, наукові праці вітчизняних і зарубіжних вчених тощо.

Поставлена автором мета дисертаційної роботи – 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 – логічно розкрита.

У першому розділі *«Теоретичні засади механізмів публічного управління інформаційною безпекою надання електронних послуг»* систематизовані

наукових підходів до механізмів публічного управління інформаційною безпекою надання електронних послуг. Проаналізований понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг. Зазначено, що механізми публічного управління інформаційною безпекою надання електронних послуг доцільно визначити 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. Таке авторське визначення акцентує увагу на кількох ключових аспектах: нормативно-правовий компонент – закони, стандарти та регламенти, що створюють обов'язкові правила гри для суб'єктів, які надають або користуються е-послугами; організаційно-інституційний компонент – система органів, установ і підрозділів (центри реагування на інциденти, служби захисту інформації, контролюючі інститути), які забезпечують координацію та підзвітність; технологічний компонент – застосування інформаційно-комунікаційних технологій і методів (системи управління інформаційною безпекою, криптографія, аудит, автоматизовані засоби моніторингу та виявлення загроз); соціально-комунікативний компонент – підвищення обізнаності користувачів, формування культури безпеки, розвиток довіри до державних цифрових сервісів. Здійснена систематизація проблем публічного управління інформаційною безпекою надання електронних послуг. В умовах воєнного стану проблеми публічного управління інформаційною безпекою надання електронних послуг виявилися комплексними та багатовимірними, поєднуючи технічні, організаційно-адміністративні, правові й соціальні чинники.

У другому розділі *«Кращі світові практики публічного управління інформаційною безпекою надання електронних послуг»* здійснений аналіз публічного управління інформаційною безпекою електронних послуг в Німеччині, Естонії, Данії, Литві, Сінгапурі, Південній Кореї, Тайвані, США. Зазначено, що досвід провідних країн світу у сфері публічного управління інформаційною безпекою електронних послуг демонструє широкий спектр підходів, які поєднують технологічні інновації, інституційні механізми та нормативно-правове забезпечення. Звернуто увагу, що ефективне публічне управління інформаційною безпекою електронних послуг ґрунтується на таких універсальних принципах: стратегічна інтеграція кіберзахисту у систему державного управління; постійний розвиток нормативно-правового поля відповідно до динаміки загроз; високий рівень міжвідомчої та міжнародної координації; партнерство держави, бізнесу та громадянського суспільства;

інвестиції в інновації, цифрову освіту та формування культури кібербезпеки. Водночас кожна країна адаптує ці принципи до власних політичних, економічних та безпекових умов, що забезпечує стійкість і довіру громадян до цифрової держави.

У третьому розділі *«Модель механізмів публічного управління інформаційною безпекою електронних послуг в Україні в умовах цифрової трансформації»* визначені сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні. Сформовано 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. Запропоновано запровадження інноваційного управління у систему інформаційною безпекою електронних послуг в умовах цифрової трансформації. Зазначено, що запровадження інноваційного управління у систему інформаційної безпеки електронних послуг в умовах цифрової трансформації постає як стратегічний пріоритет, що виходить за рамки суто технічного захисту і охоплює цілісну управлінську парадигму. Обґрунтована модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації. Модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації має цілісний, багаторівневий і стратегічно орієнтований характер, який відображає як національні потреби України, так і кращі міжнародні практики у сфері кіберзахисту. Передусім, ключовим досягненням є інтеграція інституційного механізму у вигляді Національної ради з питань інформаційної безпеки електронних послуг, яка виступає центральним координатором у системі управління. Її діяльність забезпечує взаємодію між центральними органами виконавчої влади, регуляторами, адміністраторами реєстрів, національними командами CSIRT та міжнародними партнерами. Такий підхід запобігає дублюванню функцій і фрагментації відповідальності, створюючи єдиний центр прийняття рішень на стратегічному рівні. Модель містить механізм управління ризиками, заснований на міжнародних стандартах ISO 27005 і NIST SP 800-30, а також передбачає визначення RTO і RPO для критичних сервісів.

Обґрунтованість одержаних результатів забезпечується шляхом комплексного використання в дисертаційній роботі загальнонаукових і спеціальних методів. Обрані методи відповідають сутності об’єкта дослідження. Об’єкт (суспільні відносини, що виникають при забезпеченні інформаційної безпеки надання електронних послуг в умовах цифрової трансформації та сучасних безпекових викликів) і предмет (світовий досвід формування та

реалізації механізмів публічного управління інформаційною безпекою надання електронних послуг) дослідження відповідають заявленій темі. Поставлені дисертантом завдання розкривають мету дослідження. Структура дисертації логічна, матеріали розділів викладено відповідно до мети і поставлених завдань.

Викладене вище свідчить про достатній рівень обґрунтованості наукових положень, висновків і рекомендацій дисертаційного дослідження. Висновки в цілому відповідають поставленим завданням, відповідно відтворюються в оприлюдненому тексті анотації.

Достовірність та наукова новизна одержаних результатів, повнота їх викладу в опублікованих працях

Достовірність отриманих результатів і обґрунтованість сформульованих висновків зумовлені використанням чітко вибудуваної методологічної основи дослідження, що поєднує загальнонаукові та спеціальні методи пізнання. Реалізація поставленої мети та виконання визначених завдань стали можливими завдяки застосуванню комплексу загальнологічних дослідницьких підходів.

Під час розроблення теоретико-методичних засад було задіяно методи аналізу й синтезу, індукції та дедукції, узагальнення, систематизації й логічного впорядкування наукового матеріалу. Це дало змогу здійснити ґрунтовне осмислення існуючих наукових концепцій, особливостей нормативно-правового регулювання та практики реалізації механізмів публічного управління у сфері забезпечення інформаційної безпеки. Для поглиблення та уточнення понятійно-категоріального апарату, визначення структури, характеристик і функціонального наповнення механізмів публічного управління інформаційною безпекою було використано методи класифікації, типологізації та функціонального аналізу, а також гносеологічні підходи, спрямовані на виявлення внутрішніх взаємозв’язків і причинно-наслідкових залежностей між складовими досліджуваного управлінського процесу.

Аналіз зарубіжного досвіду впровадження механізмів публічного управління у сфері інформаційної безпеки електронних послуг здійснювався із застосуванням компаративного аналізу, узагальнення міжнародних статистичних даних, нормативних актів і практичних напрацювань, що дало можливість визначити найбільш результативні управлінські моделі, адекватні сучасним викликам цифрової безпеки та умовам розвитку електронного врядування. У межах третього розділу, присвяченого обґрунтуванню напрямів підвищення ефективності функціонування відповідних механізмів, використовувалися методи моделювання, прогнозування, сценарного аналізу й стратегічного планування, які спиралися на оцінку поточних тенденцій у сфері інформаційної

безпеки, адаптацію кращих світових практик до національних реалій та узагальнення результатів попередніх емпіричних досліджень.

Застосування зазначеного методичного інструментарію дало змогу сформувати цілісну концептуальну модель механізмів публічного управління, орієнтовану на забезпечення стійкості, гнучкості та результативності системи надання електронних публічних послуг в умовах цифрових трансформацій, воєнних загроз і завдань післявоєнного відновлення.

Погоджуючись із сформульованими в дисертації конкретними положеннями, які визначають наукову новизну отриманих результатів, особливо хочу відзначити окремі з них, що є найбільш важливими.

У роботі вперше: обґрунтована модель механізмів публічного управління інформаційною безпекою надання 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 представлений Національною радою 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.

До методологічних здобутків автора слід віднести: удосконалення 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; систематизацію 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; виокремлення закономірностей публічного управління інформаційною безпекою електронних послуг в Німеччині, Естонії, Данії, Литві, Сінгапурі, Південній Кореї, Тайвані, США, зокрема виокремленні: 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; визначення сучасних механізмів 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; обґрунтування механізмів 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.

Основні положення дисертаційної роботи опубліковано в чотирьох статтях у наукових фахових виданнях України, семи тезах за матеріалами науково-практичних конференцій.

Практичне значення і впровадження одержаних результатів дослідження

Результати дисертаційного дослідження були використані в діяльності асоціацій, підрозділів органів місцевого самоврядування, ІТ-компаній, закладів 26 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.).

Зазначене підтверджує прикладну спрямованість результатів дослідження, їхню наукову обґрунтованість і практичну цінність для вдосконалення механізмів публічного управління, зокрема у сфері цифровізації, розвитку електронних послуг та забезпечення інформаційної безпеки. Використання отриманих висновків і рекомендацій у діяльності органів місцевого самоврядування сприяє підвищенню ефективності управлінських рішень, удосконаленню організаційних процедур та посиленню інституційної спроможності у впровадженні сучасних цифрових сервісів. Залучення результатів дослідження в практику ІТ-компаній засвідчує їх релевантність потребам цифрового середовища та можливість використання при розробленні й супроводі інформаційних систем електронного врядування.

Впровадження напрацювань дисертації в освітній процес закладу вищої освіти забезпечує оновлення змісту навчальних дисциплін, формування сучасних управлінських компетентностей у здобувачів вищої освіти та підготовку фахівців, здатних ефективно діяти в умовах цифрової трансформації публічного управління. Сукупно це свідчить про значний практичний потенціал результатів дослідження та можливість їх подальшого використання у науковій, управлінській і освітній діяльності.

Відсутність (наявність) порушення академічної доброчесності

Дисертація та наукові публікації, у яких висвітлені основні наукові результати дисертації, не містять порушень академічної доброчесності (академічного плагіату, фабрикації, фальсифікації).

Дискусійні положення та зауваження щодо змісту дисертації

Позитивно оцінюючи отримані Лазарівим Владиславом Олеговичем результати виконаного ним дослідження, підкреслюючи їх наукову та практичну цінність, водночас слід вказати на такі недоліки та пропозиції дискусійного характеру:

1. У параграфі 1.2 «Понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг» здобувачем здійснено ґрунтовний аналіз ключових категорій дослідження, зокрема таких понять, як «механізми», «механізми

публічного управління», «інформаційна безпека», «механізми публічного управління інформаційною безпекою», «електронні послуги», «механізми публічного управління інформаційною безпекою надання електронних послуг». Позитивно слід відзначити спробу автора чітко розмежувати поняття «механізми» та суміжні категорії – інструменти, методи, важелі тощо, що сприяє уточненню теоретико-методологічних засад дослідження.

Водночас, робота виграла б за умови більш чіткого концептуального розмежування таких понять, як «механізми державного управління інформаційною безпекою», «механізми управління інформаційною безпекою» та «механізми публічного управління інформаційною безпекою». У представленому тексті відсутнє достатньо аргументоване пояснення відмінностей між зазначеними категоріями, що ускладнює розуміння специфіки саме публічно-управлінського підходу порівняно з класичною моделлю державного управління.

Крім того, доцільним було б доповнити понятійно-категоріальний апарат аналізом поняття «механізми публічного управління кібербезпекою», з урахуванням його співвідношення з інформаційною безпекою в умовах цифровізації та розвитку електронних послуг. Таке розширення теоретичної бази дозволило б підвищити системність дослідження, уточнити міждисциплінарні зв’язки та посилити наукову обґрунтованість авторських висновків.

2. У параграфі 1.3 «Проблеми публічного управління інформаційною безпекою надання електронних послуг» автором здійснена спроба систематизувати проблеми, які виникають у системі публічного управління інформаційною безпекою надання електронних послуг. Водночас, попри поділ на технічний, організаційно-адміністративний та правовий виміри проблем, в окремих частинах тексту відбувається їх змішування. Наприклад, архітектурна централізація ІТ-систем або залежність від хмарних провайдерів подається переважно як технічна проблема, хоча фактично вона є наслідком управлінських рішень у сфері закупівель, стратегічного планування та регуляторного дизайну. Це дещо розмиває логіку причинно-наслідкових зв’язків.

Крім того, хоча текст коректно спирається на наукові огляди та міжнародні рекомендації, емпіричні приклади з української практики переважно подаються узагальнено. Це створює ризик надмірної універсалізації проблем без достатнього показу їх специфіки саме для української моделі публічного управління в умовах війни.

3. У параграфі 1.3 «Проблеми публічного управління інформаційною безпекою надання електронних послуг» подано узагальнені висновки, зміст яких логічно не випливає з аналізу, представленого в межах цього параграфа. Зокрема, після ґрунтовної систематизації та аналізу проблем публічного

управління інформаційною безпекою у сфері надання електронних послуг без належного логічного переходу формулюється висновок щодо систематизації наукових підходів до механізмів публічного управління інформаційною безпекою надання електронних послуг, що за змістом належить до іншого предметного поля дослідження. Така структурна неузгодженість знижує цілісність викладу й негативно впливає на сприйняття першого розділу загалом. З метою усунення плутанини доцільно чітко розмежувати змістові акценти параграфів і відповідно конкретизувати назви підсумкових висновків у межах розділів, забезпечивши їх безпосередній зв'язок із матеріалом, що аналізується.

Аналогічні зауваження до параграфів 2.3, 3.3.

У тексті параграфа 1.3 використано формулювання: «Матеріали цього розділу оприлюднені в таких публікаціях автора: [43; 44; 49]», яке є змістовно й структурно неоднозначним. З контексту не зрозуміло, до якого саме структурного елемента першого розділу відноситься зазначене твердження – параграфа 1.1, 1.2 чи безпосередньо 1.3. За наявної логіки викладу створюється враження, що йдеться саме про параграф 1.3 та його висновки, що, своєю чергою, може бути інтерпретовано як твердження про їх оприлюднення одразу у трьох публікаціях. З метою уникнення двозначності та забезпечення коректності наукового викладу доцільно чітко конкретизувати, матеріали якого саме параграфа або підрозділу були апробовані та відображені у зазначених публікаціях. Аналогічні зауваження до параграфів 2.3, 3.3.

4. У параграфі 2.1. «Аналітична оцінка стану публічного управління інформаційною безпекою електронних послуг у країнах ЄС» детально подано нормативно-інституційні та технічні особливості моделей Німеччини, Естонії, Данії та Литви, проте відсутня чітко окреслена методика порівняльної аналітичної оцінки (критерії, показники, індикатори або узагальнена модель аналізу). Водночас, фактичний виклад має переважно описово-оглядовий характер, що ускладнює виокремлення спільних закономірностей, відмінностей і причинно-наслідкових зв'язків між національними підходами до публічного управління інформаційною безпекою електронних послуг. Доцільним було б на початку параграфа визначити єдині аналітичні критерії (інституційні, правові, організаційні, технічні, управлінські), а в завершальній частині – подати узагальнювальну порівняльну характеристику країн ЄС, що відповідала б заявленій «аналітичній оцінці», а не лише опису окремих кейсів.

5. У параграфі 3.1. «Сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні» незважаючи на значну теоретичну насиченість та детальний опис проблемного поля публічного управління інформаційною безпекою електронних послуг в Україні, у тексті недостатньо чітко розмежовано аналітичний і конструктивно-модельний рівні

дослідження. Значна частина розділу присвячена одночасно діагностиці системних проблем, обґрунтуванню потреби в реформуванні та детальному опису запропонованої функціонально-ієрархічної моделі. Така концентрація різнорівневого матеріалу у межах одного підрозділу ускладнює логіку сприйняття та створює враження перевантаженості викладу. Доцільним було б чіткіше структурувати розділ, виокремивши аналітичну частину (оцінку стану та ключових вразливостей системи управління ІБ) і власне модельну частину (опис структури, функцій та індикаторів), що підвищило б методологічну прозорість і наукову чіткість результатів.

Запропонована у розділі 3.1 функціонально-ієрархічна модель механізмів публічного управління інформаційною безпекою електронних послуг є концептуально обґрунтованою та логічно побудованою, однак її практична реалізовуваність потребує додаткової конкретизації. Зокрема, індикаторна система ефективності (F1-F5), хоча й коректно визначена на концептуальному рівні, не супроводжується методикою їх розрахунку, джерелами даних та інституційною відповідальністю за моніторинг. Відсутність таких уточнень ускладнює можливість емпіричної перевірки дієвості запропонованої моделі та її адаптації до реального управлінського середовища. Доцільним було б доповнити розділ прикладами застосування індикаторів або посиланням на конкретні механізми їх впровадження в практику органів публічної влади.

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

Загальний висновок та оцінка дисертації

Дисертаційне дослідження Лазаріва Владислава Олеговича на тему: «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» є самостійним, завершеним науковим дослідженням, виконаним на актуальну тему, містить положення наукової новизни, має теоретичне та практичне значення та відповідає спеціальності 281 «Публічне управління та адміністрування».

Дисертаційна робота Лазаріва Владислава Олеговича на тему: «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» відповідає вимогам Постанови Кабінету Міністрів України “Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії” від 12 січня 2022 року № 44 (зі змінами) та вимогам наказу Міністерства освіти і науки України від

12 січня 2017 року № 40 “Про затвердження вимог до оформлення дисертації” (із змінами, внесеними згідно з наказом Міністерства освіти і науки України від 31 травня 2019 року № 759), а її автор – Лазарів Владислав Олегович – заслуговує на присудження ступеня доктора філософії за спеціальністю 281 “Публічне управління та адміністрування”.

Офіційний опонент:
доктор наук з державного управління, професор,
завідувач кафедри публічного управління
та адміністрування Університету
Григорія Сковороди в Переяславі **О. І. Пархоменко-Куцевіл**