ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи Карпатського національного університету імені Василя Стефаника
кандидат медичних наук, професор
_____ Едуард ЛАПКОВСЬКИЙ
"26" листопада 2025 р.

ВИТЯГ

з протоколу № 2 від 19 листопада 2025 р. фахового семінару факультету управління Карпатського національного університету імені Василя Стефаника.

ПРИСУТНІ:

Дерев'янко Сергій Миронович – доктор політичних наук, професор, професор кафедри політичних інститутів та процесів – голова семінару;

Драбчук Наталія Юріївна – доктор філософії за спеціальністю 051 Економіка, асистент кафедри публічного управління та адміністрування – секретар семінару;

Сурай Інна Геннадіївна – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування – гарант ОНП «Публічне управління та адміністрування»;

Нагорняк Михайло Миколайович – доктор політичних наук, професор кафедри міжнародних відносин – науковий керівник, член семінару;

Жук Ольга Іванівна – кандидат економічних наук, доцент, завідувач кафедри публічного управління та адміністрування – член семінару;

Якубів Валентина Михайлівна – доктор економічних наук, професор, ректор Університету – член семінару;

Дєгтяр Олег Андрійович – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування – член семінару;

Кафка Софія Михайлівна – доктор економічних наук, професор, професор кафедри менеджменту та бізнес-адміністрування – член семінару;

П'ятничук Ірина Дмитрівна – кандидат економічних наук, доцент, декан факультету управління – член семінару;

Хом'як Іван Васильович – доктор філософії за спеціальністю 281 Публічне управління та адміністрування, асистент кафедри публічного управління та адміністрування;

Малишівський Тарас Володимирович – доктор філософії за спеціальністю 281 Публічне управління та адміністрування, викладач кафедри менеджменту та бізнес-адміністрування – член семінару;

Гой Наталія Василівна – кандидат економічних наук, доцент, доцент кафедри публічного управління та адміністрування – член семінару.

З присутніх – 6 докторів наук та 3 кандидати наук, 3 доктори філософії – фахівці за профілем представленої дисертації.

Головуючий на фаховому семінарі – професор Дерев'янко Сергій Миронович

СЛУХАЛИ:

1. Результати дисертаційного дослідження Лазаріва Владислава Олеговича, аспіранта IV денної контрактної форми навчання за спеціальністю 281 Публічне управління та адміністрування на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід»», поданого на здобуття наукового ступеня доктора філософії з галузі знань 28 Публічне управління та адміністрування за спеціальністю 281 Публічне управління та адміністрування.

Тему дисертаційної роботи «Механізми забезпечення безпеки даних у наданні публічних послуг в органах державної влади» затверджено на засіданні Вченої ради Прикарпатського національного університету імені Василя Стефаника, протокол № 6 від 27 червня 2022 р. та уточнено на засіданні Вченої ради "Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід" 26 травня 2025 року, протокол № 7.

Науковий керівник – доктор політичних наук, професор Нагорняк М. М.

2. Виступ здобувача Лазаріва Владислава Олеговича:

Шановні члени спеціалізованої вченої ради! Дозвольте представити Вашій увазі результати дисертаційного дослідження на здобуття наукового ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування» на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід»

Актуальність теми дисертаційного дослідження зумовлена пришвидшенням процесів цифровізації публічного управління, активним розвитком електронних послуг та зростанням рівня кіберзагроз, що потребують розробки ефективних механізмів забезпечення інформаційної безпеки. В умовах трансформації публічного управління та підвищених очікувань громадян щодо прозорості, доступності та захищеності публічних сервісів, інформаційна безпека постає як критично важлива складова надання електронних послуг. Особливої значущості проблематика набуває в контексті збройної агресії російської федерації проти України, що супроводжується інтенсивними кіберзагрозами як складовою гібридних атак.

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.

Об'єкт дослідження: суспільні відносини, що виникають при забезпеченні інформаційної безпеки надання електронних послуг в умовах цифрової трансформації та сучасних безпекових викликів.

Предмет дослідження: світовий досвід формування та реалізації механізмів публічного управління інформаційною безпекою надання електронних послуг

Для досягнення поставленої мети в дисертаційному дослідженні визначено такі *завдання*:

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

– проаналізувати понятійно-категоріальний апарат дослідження механізмів публічного управління інформаційною безпекою надання електронних послуг;

– систематизувати проблеми публічного управління інформаційною безпекою надання електронних послуг;

– здійснити аналіз стану публічного управління інформаційною безпекою електронних послуг в країнах ЄС;

– дослідити розвиток публічного управління інформаційною безпекою електронних послуг в Азійських країнах;

– охарактеризувати модернізацію публічного управління інформаційною безпекою електронних послуг в США;

– оцінити сучасні механізми публічного управління інформаційною безпекою електронних послуг в Україні;

– аргументувати запровадження інноваційного управління у систему інформаційною безпекою електронних послуг в умовах цифрової трансформації;

– обґрунтувати модель механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації У результаті проведеного дослідження планується:

Для вирішення поставлених у дослідженні завдань застосовано комплекс загальнонаукових і спеціалізованих методів, які забезпечують цілісне та системне осмислення сутності, структури та функціонування механізмів публічного управління інформаційною безпекою у системі надання електронних послуг. На етапі формування теоретико-методичних засад дослідження використано методи аналізу, синтезу, індукції, дедукції, узагальнення, систематизації та логічного структурування. Застосування цих методів дало змогу здійснити критичне переосмислення наукових підходів, нормативно-правового регулювання та практики впровадження механізмів публічного управління у сфері забезпечення інформаційної безпеки. Для уточнення понятійно-категоріального апарату дослідження, структури, ознак і функціонального змісту механізмів публічного управління інформаційною безпекою застосовано методи класифікації, типологізації, функціонального аналізу, а також методи гносеологічного пізнання з метою виявлення внутрішніх взаємозв'язків і причинно-наслідкових залежностей між елементами досліджуваного управлінського явища. Під час аналізу світового досвіду реалізації механізмів публічного управління в галузі інформаційної безпеки електронних сервісів використовувалися методи компаративного аналізу, узагальнення міжнародних статистичних, нормативних і практичних матеріалів, що дозволило ідентифікувати ефективні моделі управлінських механізмів, релевантні до сучасних викликів цифрової безпеки та до умов функціонування електронного врядування. У третьому розділі, присвяченому розробці напрямів підвищення ефективності впровадження механізмів публічного управління інформаційною безпекою електронних послуг, застосовано методи моделювання, прогнозування, сценарного аналізу та стратегічного планування. Їх використання ґрунтується на оцінці актуальних тенденцій у сфері

інформаційної безпеки, адаптації провідних світових практик до національного контексту, а також на узагальненні результатів попереднього емпіричного дослідження.

Зазначені методи дозволили сформувати концептуальну модель механізмів публічного управління, здатну забезпечити стійкість, адаптивність та ефективність функціонування системи надання електронних публічних послуг в умовах цифрової трансформації, воєнних загроз і потреб післявоєнного відновлення.

Наукова новизна 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 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;

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 проєктування;

набули подальшого розвитку:

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

- понятійно-категоріальний 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.

Центральним поняттям дослідження є «механізми публічного управління». У процесі наукового осмислення природи та змісту механізмів публічного управління у сучасній управлінській науці сформувалося кілька методичних підходів, кожен з яких висвітлює окремі аспекти функціонування, побудови та цільового призначення цих механізмів. Їх розгляд у межах функціонального, інституційного, процесного та системного підходів дозволяє комплексно оцінити механізми як складні управлінські утворення, що мають як структурну

завершеність, так і динамічну здатність до трансформації. Порівняння зазначених підходів на основі ключових характеристик і дослідницьких пріоритетів дозволяє забезпечити цілісне теоретико-методологічне підґрунтя для подальшого аналізу, моделювання та вдосконалення механізмів публічного управління, зокрема у сфері забезпечення інформаційної безпеки під час надання електронних послуг. Запропоновані підходи були виділені в дослідженні на основі аналізу літературних джерел та наукових концепцій авторів, що працювали над проблематикою теоретичного осмислення механізмів публічного управління.

У науковій літературі пропонується розрізняти кілька ключових складових механізмів публічного управління інформаційною безпекою. По-перше, це нормативно-правові інструменти, що формують основу державної політики та визначають стандарти, регламенти, правила функціонування і відповідальність за порушення у сфері інформаційної безпеки. По-друге, організаційно-управлінські інструменти охоплюють створення спеціалізованих органів, визначення їх компетенцій, розподіл функцій і завдань між різними рівнями управління, формування механізмів координації та контролю. По-третє, важливою складовою є технологічні інструменти – апаратні та програмні рішення, методи криптографічного захисту, системи виявлення вторгнень, засоби моніторингу, аналізу ризиків і управління інцидентами. По-четверте, соціально-комунікаційні інструменти відображають культурні та освітні аспекти: формування культури інформаційної безпеки серед державних службовців, проведення навчання, інформування громадян про правила користування електронними послугами, забезпечення прозорості й довіри. Таким чином, механізми публічного управління інформаційною безпекою є комплексними, багаторівневими та соціотехнічними за своєю природою. Вони передбачають інтеграцію різних підсистем – інфраструктури, даних, людей та процесів – в єдину систему, здатну адаптуватися до змін середовища і протидіяти як зовнішнім, так і внутрішнім загрозам.

Вони виступають не лише засобом захисту, а й способом формування довіри громадян до держави, підвищення ефективності публічного управління та забезпечення безперервності надання електронних послуг навіть в умовах кризових чи надзвичайних ситуацій.

На нашу думку, механізми публічного управління інформаційною безпекою доцільно розглядати як комплекс інституційних, організаційних, правових, технологічних та соціальних інструментів, за допомогою яких держава забезпечує захищеність інформаційних ресурсів, інформаційних систем та електронних сервісів у публічному секторі. Вони не є суто технічними або суто адміністративними діями, а формуються на перетині нормотворчості, управлінських процесів, координації діяльності різних суб'єктів і застосування спеціалізованих технологій. Таким чином, механізми виконують роль інтегрованих засобів, що з одного боку забезпечують стабільне функціонування державних електронних послуг, а з іншого – створюють умови для своєчасного виявлення, запобігання та нейтралізації загроз інформаційній. поняття «електронні послуги».

Щодо електронних послуг, то в науковій літературі воно розглядаються як інтердисциплінарний феномен, що поєднує технологічні, організаційні,

соціальні та публічно-управлінські виміри. Категорія «електронні послуги» у межах дослідження має подвійний зміст: з одного боку, це інструмент цифрової трансформації публічного сектору, а з іншого – вразлива інфраструктура, що потребує особливих заходів управління ризиками, захисту персональних даних та забезпечення довіри користувачів. Це означає, що понятійний апарат неможливо будувати без урахування категорій «довіра», «надійність», «стійкість» і «сталість», що набувають особливого значення в умовах цифровізації державного управління. 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. Узгодженість цих складових відображає комплексність управління: воно не обмежується технічними чи правовими заходами, а передбачає інтегровану взаємодію різних рівнів управління і суспільних практик. Саме така багатовимірність дозволяє говорити про механізми як про системоутворюючий чинник, що забезпечує не лише функціональну безпеку електронних послуг, але й стабільність цифрової взаємодії між державою та громадянами.

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. Технічний вимір стосується вразливості державних ІТ-систем, які здебільшого проєктувалися у мирний час без урахування масштабних кризових сценаріїв, що зумовлює залежність від зовнішніх постачальників і підвищує ризик комбінованих атак. Організаційно-адміністративні бар'єри проявляються у фрагментації відповідальності між різними суб'єктами, нестачі фахівців у державному секторі та необхідності інтеграції приватних і волонтерських структур у систему реагування, що створює ризики управлінської неузгодженості. Правове поле перебуває у стані постійної напруги, оскільки держава змушена балансувати між обмежувальними заходами задля захисту національної безпеки та зобов'язаннями щодо дотримання прав людини і прозорих процедур оскарження. Особливу гостроту мають проблеми доступу та цифрової рівності,

адже перебої в електро- й телекомунікаційних мережах ставлять під загрозу реалізацію базових прав громадян через неможливість отримання електронних послуг.

Для вироблення концептуальної моделі публічного управління інформаційною безпекою надання електронних послуг нами 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.

Узагальнюючи світовий досвід, можна стверджувати, 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.

Враховуючи як сучасні виклики кіберсередовища, так і потреби стратегічного розвитку цифрового врядування нами 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. Здійснено класифікацію основних проблемних зон сучасної системи управління ІБ в Україні, серед яких: відсутність цілісної координаційної моделі, фрагментарність нормативно-правового регулювання, недостатня технічна готовність, обмеженість ресурсного забезпечення та низький рівень цифрової грамотності на всіх рівнях публічного управління.

Запропонована нами модель базується на ідеї взаємодії трьох рівнів управління стратегічного, тактичного та оперативного із чітким функціональним поділом відповідальностей і взаємозв'язком між ними. У межах моделі визначено п'ять ключових функціональних блоків (інституційно-координаційний, нормативно-правовий, технологічний, фінансово-ресурсний та соціокомунікаційний), кожен з яких виконує унікальну роль у формуванні кіберстійкої цифрової екосистеми публічного управління.

Узагальнено систему цільових індикаторів ефективності інформаційної безпеки, яка дає змогу кількісно оцінювати досягнення стратегічних цілей у цій сфері. Запропонована логіка взаємозв'язку між блоками управління та індикаторами забезпечує інтеграцію концептуальних засад у практичну площину, створюючи умови для розробки проєктних рішень, інструментів реалізації та механізмів моніторингу ефективності політики публічного управління ІБ.

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. Аналіз сучасних міжнародних практик свідчить, що ключовим викликом є поєднання високої швидкості впровадження інновацій та гнучкості цифрових сервісів із необхідністю забезпечення стійкості, надійності й довіри громадян та бізнесу до державних послуг. На відміну від традиційних підходів, що будуються на реактивних механізмах, інноваційне управління орієнтується на принципи «безпеки за дизайном» та «приватності за дизайном», які інтегрують вимоги безпеки у життєвий цикл електронних сервісів від моменту їхнього проєктування. Це забезпечує не лише зменшення ризиків, а й ефективніше використання ресурсів.

Управлінські закономірності вказують на те, що ефективність інформаційної безпеки залежить від балансу між централізованими й децентралізованими моделями управління ризиками, що дозволяє одночасно забезпечувати стратегічну координацію та оперативну гнучкість. Прозора система підзвітності, комунікації з громадянами і бізнесом, а також інтеграція публічно-приватних партнерств створюють передумови для зростання рівня довіри та ефективного колективного реагування.

В умовах воєнного й гібридного протистояння, як демонструє досвід України, інноваційне управління неможливе без резервних архітектур, сегментації критичних реєстрів, планів безперервності та сценаріїв відновлення. Активна міжнародна співпраця, зокрема в межах ЄС, НАТО та через спеціалізовані платформи кіберобміну, підсилює стійкість до атак та забезпечує доступ до найкращих практик. Водночас систематизація стандартів та узгоджене інституційне зміцнення органів кібербезпеки залишається необхідною умовою для підвищення ефективності захисту державних електронних послуг.

Отже, інноваційне управління інформаційною безпекою електронних послуг в умовах цифрової трансформації варто розглядати як динамічну систему, що поєднує технологічні рішення, організаційні структури, нормативно-правові механізми та культуру безпеки. Це управління повинно бути не лише інструментом зниження ризиків, а й фактором забезпечення довіри суспільства до цифрової держави, підвищення її конкурентоспроможності у глобальному середовищі та стійкості в умовах кризових ситуацій. Вибудова такої моделі є тривалим процесом, проте саме вона відповідає викликам цифрової епохи і здатна забезпечити сталий розвиток електронних сервісів як основи сучасного публічного управління.

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.

Нормативно-правовий механізм у моделі ґрунтується на гармонізації українського законодавства з міжнародними стандартами ISO/IEC 27001, ISO 27005, NIST Рамки кібербезпеки та практиками GDPR. Це дає можливість забезпечити відповідність національної системи управління інформаційною безпекою міжнародним вимогам, спростити інтеграцію до європейського кіберпростору та водночас гарантувати захист персональних даних громадян. Важливим є закріплення принципів «безпека за дизайном» і «приватність за дизайном», що дозволяє враховувати аспекти захищеності ще на етапі створення нових електронних сервісів.

Фінансовий механізм формує довгострокову та багатоканальну модель фінансування заходів кіберзахисту, яка передбачає державне бюджетування, створення цільових фондів кіберстійкості, залучення міжнародних грантів та розвиток державно-приватних партнерств. Такий підхід забезпечує стабільність і прогнозованість фінансових потоків, дозволяє здійснювати великі інфраструктурні проєкти (наприклад, впровадження SIEM, EDR, резервного копіювання) та стимулює приватний сектор до співпраці з державою у сфері кібербезпеки.

Кадровий механізм моделі передбачає створення професійного кадрового резерву шляхом формування стандартів компетенцій для ключових посад (CISO, адміністратори реєстрів, аналітики інцидентів), обов'язкових програм навчання для всіх державних службовців та спеціалізованої підготовки для фахівців. У цьому контексті важливим є впровадження системи сертифікації та безперервного підвищення кваліфікації, що відповідає міжнародним підходам, а також створення механізмів мотивації та утримання кадрів. Це дозволить знизити кадровий дефіцит та мінімізувати ризики людського фактора.

Контрольний механізм передбачає системну багаторівневу перевірку ефективності заходів із захисту інформації через внутрішні й зовнішні аудити, регулярний моніторинг, індикатори ефективності та механізми санкцій. Використання міжнародного стандарту ISO/IEC 27001 та моделі PDCA дає змогу забезпечити постійне вдосконалення системи, оперативне виявлення відхилень і підвищення рівня довіри до державних електронних послуг. Окреме значення має прозорість у звітуванні, що дозволяє громадянам і міжнародним партнерам оцінювати ефективність публічної політики.

Інформаційно-комунікативний механізм орієнтований на створення довіри до державних електронних сервісів та формування культури кібербезпеки в суспільстві. Він передбачає обов'язкову публічну звітність, інформування користувачів у випадку інцидентів, проведення освітніх та просвітницьких кампаній, а також активний обмін інформацією з міжнародними структурами, зокрема ENISA та CERT-EU. Це забезпечує прозорість, підзвітність і сприяє підвищенню стійкості до загроз.

Важливо, що 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. Це дозволяє систематизувати процеси оцінки й мінімізації ризиків, визначати пріоритети у фінансуванні та концентрувати ресурси на найбільш вразливих сегментах. Доповненням виступає механізм управління інцидентами, який ґрунтується на NIST SP 800-61

і передбачає створення CSIRT-структур, уніфіковані протоколи реагування та міжнародний обмін даними про загрози.

Узагальнюючи, можна зробити висновок, що модель механізмів публічного управління інформаційною безпекою електронних послуг формують науково обґрунтовану, практично орієнтовану й комплексну систему управління, яка враховує національні особливості України та водночас інтегрує кращий світовий досвід. Вона створює інституційну, нормативну, фінансову, кадрову, контрольну та комунікаційну основу для підвищення кіберстійкості держави, захисту прав громадян і забезпечення довіри до електронних послуг, закладаючи фундамент для інтеграції України у глобальний простір кібербезпеки.

Запропоновано розробити та прийняти Концепцію розвитку публічного управління інформаційною безпекою електронних послуг на 2026-2036 роки, де передбачається врегулювати зазначену вище модель.

За результатами дослідження, сформульовано висновки й пропозиції, що мають теоретичне та практичне значення щодо удосконалення механізмів публічного управління інформаційною безпекою надання електронних послуг. Вони представлені на слайдах, а тому дозвольте не зачитувати їх.

За результатами дослідження опубліковано 4 статті у виданнях України, які входять до фахових періодичних видань категорії Б, та тези доповідей на міжнародних науково-практичних конференціях

Дякую за увагу

3. Запитання до аспіранта по темі дисертації ставили:

1. Дерев'янко С. М. – доктор політичних наук, професор, професор кафедри політичних інститутів та процесів:

Охарактеризуйте основні проблеми та виклики до публічного управління інформаційною безпекою надання електронних послуг.

Лазарів В.О.: Дякую за запитання. Україна перебуває в умовах постійної інформаційної агресії, коли російська пропаганда та дезінформаційні кампанії створюють серйозну загрозу національній безпеці. Для протидії цим викликам необхідно вдосконалювати механізми інформаційного захисту, розвивати системи моніторингу фейків та підвищувати рівень інформаційної грамотності населення. Кібератаки на державні органи, критичну інфраструктуру, енергетичні та транспортні системи стали складовою гібридної війни. Це зумовлює потребу у посиленні кіберзахисту, модернізації ІТ-інфраструктури та створенні ефективних механізмів реагування на інциденти. Передача значної частини повноважень від центральної до місцевої влади створює нові ризики для інформаційної безпеки. Необхідно забезпечити належний рівень захисту даних громадян і цифрових ресурсів на рівні територіальних громад. Російська федерація активно використовує інформаційні та кібероперації для впливу на політичні процеси в Україні. Це потребує системного моніторингу, виявлення таких впливів і розроблення ефективних заходів їх нейтралізації. Із розвитком електронного урядування та цифрових послуг особливого значення набуває захист персональних даних громадян, безпечне зберігання та передавання інформації. Надійний рівень захисту інформації є передумовою для становлення інформаційної економіки, підвищення інвестиційної привабливості України та інтеграції у світовий цифровий простір. Україна активно взаємодіє з іноземними

партнерами та міжнародними організаціями у сфері кібер- та інформаційної безпеки, дотримуючись міжнародних стандартів і норм, що сприяє зміцненню її позицій на глобальному рівні.

2. Драбчук Н.Ю. – доктор філософії за спеціальністю 051 Економіка, асистент кафедри публічного управління та адміністрування:

Будь-ласка, надайте визначення поняття інформації, яке Ви використовуєте в роботі?

Лазарів В.О.: Дякую за запитання. У дослідженні інформація визначена, як сукупність даних, повідомлень і знань, які передаються та обмінюються з метою сприяння зрозумінню та спільному розумінню між урядовими органами, громадянами і громадськістю. Інформація включає в себе елементи комунікації, стратегії спілкування та інструменти управління справами держави, спрямовані на забезпечення відкритості, прозорості та ефективності управління.

3. Сурай І.Г. – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування:

Розкрийте зміст поняття інноваційне управління інформаційною безпекою?

Лазарів В.О.: Дякую за запитання. Інноваційне управління інформаційною безпекою електронних послуг в умовах цифрової трансформації варто розглядати як динамічну систему, що поєднує технологічні рішення, організаційні структури, нормативно-правові механізми та культуру безпеки. Це управління повинно бути не лише інструментом зниження ризиків, а й фактором забезпечення довіри суспільства до цифрової держави, підвищення її конкурентоспроможності у глобальному середовищі та стійкості в умовах кризових ситуацій. Вибудова такої моделі є тривалим процесом, проте саме вона відповідає викликам цифрової епохи і здатна забезпечити сталий розвиток електронних сервісів як основи сучасного публічного управлінняУ результаті проведеного дослідження було запропоновано обрати стратегічний підхід як основу для подальшого формування теоретико-методичних засад визначення інформаційної безпеки в системі публічного управління. Такий підхід передбачає розроблення та реалізацію цілісних стратегій і політик, спрямованих на ефективний захист інформації, а також забезпечення її конфіденційності, цілісності та стійкості до загроз.

4. Жук О. І. – кандидат економічних наук, доцент, завідувач кафедри публічного управління та адміністрування:

Охарактеризуйте парадигму розвитку теоретико-методичних підходів процесів інформаційного захисту?

Лазарів В.О.: Дякую за запитання. Запропонована структуризація етапів у межах парадигми розвитку теоретико-методичних підходів до визначення поняття інформаційного захисту в системі публічного управління відображає поступову еволюцію наукових досліджень у цій сфері від початкового усвідомлення проблеми до формування комплексних стратегій управління ризиками та стратегічного планування. Така парадигма акцентує увагу на необхідності цілісного, інтегрованого підходу до забезпечення інформаційної

безпеки, який охоплює технічні, організаційні, соціальні та політичні складові, що разом формують ефективну систему захисту інформації.

5. Дєгтяр О. А. – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування:

Наскільки в запропонованій Вами моделі механізмів публічного управління інформаційною безпекою електронних послуг в умовах цифрової трансформації враховані національні і міжнародні практики?

Лазарів В.О.: Дякую за запитання. 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.

6. Кафка С. М. – доктор економічних наук, професор, професор кафедри менеджменту та бізнес-адміністрування.

В чому полягає особливість фінансового механізму забезпечення кіберзахисту?

Лазарів В.О.: Фінансовий механізм формує довгострокову та багатоканальну модель фінансування заходів кіберзахисту, яка передбачає державне бюджетування, створення цільових фондів кіберстійкості, залучення міжнародних грантів та розвиток державно-приватних партнерств. Такий підхід забезпечує стабільність і прогнозованість фінансових потоків, дозволяє здійснювати великі інфраструктурні проєкти (наприклад, впровадження SIEM, EDR, резервного копіювання) та стимулює приватний сектор до співпраці з державою у сфері кібербезпеки.

7. П'ятничук І. Д. – кандидат економічних наук, доцент, декан факультету управління.

Опишіть Функціонально-ієрархічну модель публічного управління інформаційною безпекою електронних послуг, яку Ви визначили як елемент наукової новизни та представили на слайді 19?

Лазарів В.О.: Дякую за запитання. Визначення взаємозв'язків між елементами системи є вирішальним чинником для побудови системно орієнтованої, багатофакторної моделі управління, яка забезпечує як вертикальну інтеграцію рішень. Запропонована матриця зв'язків між функціональними блоками управління та відповідними індикаторами ефективності не лише

структурує внутрішню архітектуру системи публічного управління інформаційною безпекою, а й орієнтує її на досягнення конкретних, вимірюваних результатів. Такий підхід сприяє формуванню адаптивної, прогнозованої та підзвітної моделі управління, здатної відповідати викликам цифрової трансформації, виконувати євроінтеграційні зобов'язання та забезпечувати вимоги національної безпеки. Поєднання інституційної узгодженості, технологічної стійкості, нормативно-правової визначеності, належного фінансування та високого рівня соціальної залученості створює комплексну основу для ефективного функціонування національної системи кібербезпеки. Застосування індикаторного підходу у процесі моніторингу дозволяє своєчасно виявляти потенційні ризики, оцінювати результативність реалізації державної політики у сфері інформаційної безпеки та оперативно коригувати управлінські рішення на всіх рівнях управління.

8. Малишівський Т. В. – доктор філософії за спеціальністю 281 Публічне управління та адміністрування, викладач кафедри менеджменту та бізнес-адміністрування:

Опишіть структуру стратегічних та тактичних механізмів реалізації функціонально-ієрархічної моделі публічного управління інформаційною безпекою електронних послуг?

Лазарів В.О.: Дякую за запитання. Національний центр має виконувати не лише координаційну функцію, а й відігравати роль генератора державної політики, стандартів та методичних рекомендацій у сфері інформаційної безпеки. Він повинен мати відповідні повноваження для проведення моніторингу, аудиту та оперативного реагування на кризові ситуації. Діяльність Центру має ґрунтуватися на принципах прозорості, відкритості та підзвітності перед суспільством. На регіональному рівні доцільно створити обласні платформи цифрової безпеки, які можуть функціонувати на базі ЦНАПів, департаментів цифрової трансформації або органів місцевої виконавчої влади. Основними завданнями таких платформ буде координація діяльності територіальних громад у сфері інформаційної безпеки, надання консультаційної підтримки, обмін досвідом і реалізація освітніх програм для підвищення цифрової грамотності. На рівні територіальних громад пропонується запровадити посаду цифрового офіцера безпеки, відповідального за моніторинг стану інформаційної безпеки, підготовку звітності, проведення навчань для працівників та співпрацю з регіональними структурами. Така система дозволить створити багаторівневу модель управління інформаційною безпекою, здатну ефективно реагувати на сучасні виклики цифрового середовища.

До доповіді було задано 8 питань, на які здобувач дав ґрунтовні відповіді.

4. Виступи присутніх членів семінару з оцінкою дисертації.

Дерев'янко С. М. – доктор політичних наук, професор, професор кафедри політичних інститутів та процесів.

У межах дослідження здійснено ґрунтовне осмислення теоретичних основ і світових практик функціонування механізмів публічного управління інформаційною безпекою електронних послуг. З урахуванням глобального досвіду сформовано пропозиції щодо підвищення ефективності інструментів публічного управління у сфері захисту цифрових сервісів. 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.

Розкрито понятійно-категоріальну структуру, що лежить в основі аналізу механізмів публічного управління інформаційною безпекою електронних послуг. Підкреслено, що механізми публічного управління інформаційною безпекою у цій сфері становлять інтегровану систему нормативно-правових, організаційно-інституційних, технологічних та соціально-комунікативних інструментів. Через їх взаємодію органи публічної влади формують, впроваджують і здійснюють контроль за реалізацією політики захисту електронних послуг від інформаційних загроз, забезпечуючи стійкість, конфіденційність, цілісність, доступність та довіру користувачів до цифрового середовища.

Узагальнено ключові проблеми публічного управління інформаційною безпекою надання електронних послуг. В умовах воєнного стану ці проблеми набули системного та багатовекторного характеру, оскільки поєднують технічні, адміністративно-організаційні, правові та соціальні аспекти. Технічний вимір охоплює вразливості державних інформаційних систем, що проєктувалися переважно для умов мирного часу й не передбачали функціонування у ситуаціях масштабних загроз. Це посилює залежність від зовнішніх технологічних рішень і створює підґрунтя для комбінованих атак, здатних порушувати сталість надання електронних послуг.

Дисертація аспіранта Лазаріва Владислава Олеговича на тему "Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід" на здобуття ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування повністю відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (зі змінами), вимогам до оформлення дисертації, затвердженими наказом Міністерства освіти і науки України від 12 січня 2017 р. № 40 (зі змінами), та Постанові Кабінету Міністрів України № 44 від 12.01.2022 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (зі змінами), а її автор Лазарів Владислав Олегович заслуговує на присудження за результатами публічного захисту ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування.

Сурай І. Г. – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування – гарант ОНП «Публічне управління та адміністрування»:

Розгортання інформаційного суспільства та стрімкий розвиток цифрових технологій формують нову структурну конфігурацію сучасної цивілізації, у якій інформація перетворюється на пріоритетний стратегічний ресурс для всіх сфер діяльності, включно з публічним управлінням. Перехід від аграрної моделі до індустріальної, згодом до постіндустріальної та, нарешті, до інформаційної епохи супроводжується істотним посиленням значення процесів обробки, збереження, передачі й захисту інформації як фундаментальної основи соціально-економічного поступу.

Теоретичні положення та результати дисертаційної роботи Лазаріва Владислава Олеговича виконаного на здобуття наукового ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування ефективно впроваджувалися в освітній процес Карпатського національного університету імені Василя Стефаника упродовж 2021-2025 років, зокрема в освітню програму галузі знань D Бізнес, адміністрування та право, спеціальності D4 Публічне управління та адміністрування освітнього рівня бакалавр ОК12 Інформаційні технології в управлінні, ОК 24 Діловодство та електронний документообіг та освітнього рівня магістр ОК 4 Інформаційні технології в публічному управлінні.

Дисертація аспіранта Лазаріва Владислава Олеговича на здобуття ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування повністю відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого постановою Кабінету Міністрів України від 23 березня 2016 р. № 261 (зі змінами).

Кафка С. М. – доктор економічних наук, професор, професор кафедри менеджменту та бізнес-адміністрування.

Дисертація є самостійно виконаним науковим дослідженням. Наукові розробки, висновки та пропозиції, що містяться в роботі, належать особисто автору. Наукові праці, опублікованих у співавторстві відсутні. Основні положення дисертаційного дослідження, доповідалися, обговорювалися та отримали позитивну оцінку на 6 міжнародних науково-практичних конференціях. 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. Дисертація аспіранта Лазаріва Владислава Олеговича на тему "Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід" відповідає вимогам підготовки здобувачів вищої освіти ступеня доктора філософії, а її автор Лазарів Владислав Олегович заслуговує на присудження за результатами публічного захисту ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування.

Дєгтяр О. А. – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування.

Інформаційна безпека перетворилася на системоутворювальний елемент функціонування державних інституцій, оскільки будь-які порушення роботи цифрових платформ або несанкціоноване розкриття даних здатні спричинити фінансові втрати та підважити довіру громадян до механізмів державного управління. З огляду на воєнні ризики та комплекс гібридних впливів, які безпосередньо торкаються України, результативність інструментів публічного управління у сфері забезпечення інформаційної безпеки електронних послуг набуває визначального значення, адже від неї залежить стабільність економіки та безперебійне функціонування критично важливих сервісів. Одночасно з цим інтеграція України у спільний європейський цифровий простір потребує гармонізації національних управлінських механізмів із міжнародними стандартами та провідними підходами. Такий процес передбачає не тільки технологічне зміцнення цифрової інфраструктури, а й формування відповідного правового забезпечення, посилення інституційної взаємодії та утвердження зрілої цифрової культури в суспільстві. Дисертація Лазаріва В.О. виконана відповідно до плану науково-дослідних робіт Карпатського національного університету імені Василя Стефаника на тему «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (номер державної реєстрації 0120U100494). У межах тем автором проведені дослідження, пов'язані з розробкою механізмів публічного управління забезпечення кібербезпеки надання електронних послуг. Дисертація аспіранта Лазаріва Владислава Олеговича відповідає вимогам підготовки здобувачів вищої освіти ступеня доктора філософії.

Жук О. І. – кандидат економічних наук, доцент, завідувач кафедри публічного управління та адміністрування.

Необхідність формування, впровадження та постійного вдосконалення механізмів публічного управління інформаційною безпекою у сфері електронних послуг в умовах цифрової трансформації та постійних безпекових викликів обумовлює теоретичну цінність та високу практичну значущість обраної теми дисертаційного дослідження. Системне дослідження зазначених механізмів дозволить сформувати науково обґрунтовані підходи до побудови ефективної моделі механізмів публічного управління в умовах гібридних загроз і нестабільності. Дисертаційна робота виконана відповідно до напрямів дослідження кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, науково-дослідницької роботи за темою «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (державний реєстраційний номер: 0120U100494).У межах тем автором проведені дослідження, пов'язані з розробкою механізмів публічного управління забезпечення кібербезпеки надання електронних послуг. 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. Дисертація аспіранта Лазаріва Владислава Олеговича на тему "Механізми публічного

управління інформаційною безпекою надання електронних послуг: світовий досвід" відповідає вимогам підготовки здобувачів вищої освіти ступеня доктора філософії, а її автор Лазарів Владислав Олегович заслуговує на присудження за результатами публічного захисту ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування.

5. Виступ наукового керівника доктора політичних наук, професора Нагорняка М.М., який відзначив, що аспірант Лазарів Владислав Олегович своєчасно виконував всі розділи індивідуального плану наукової роботи в установлені терміни. Своєчасність та повнота виконання індивідуального плану аспіранта підтверджена результатами піврічної проміжної, підсумкової (річної) та заключної атестації. Відповідально ставився до поставлених завдань. Зокрема, своєчасно і в повному обсязі провів усі види робіт. Пройшов педагогічну практику. Користувався повагою з боку студентів та колег-аспірантів.

Дисертація аспіранта Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» за спеціальністю 281 Публічне управління та адміністрування повністю 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 12.01.2022 № 44 (зі змінами) та Вимогам до оформлення дисертації, затвердженими наказом МОН України від 12.01.2017 № 40 (зі змінами), та може бути представлена до захисту в разовій спеціалізованій вченій раді.

6. В обговоренні дисертаційної роботи взяли участь: Дерев'янко Сергій Миронович – доктор політичних наук, професор, професор кафедри політичних інститутів та процесів; Сурай Інна Геннадіївна – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування – гарант ОНП «Публічне управління та адміністрування»; Дєгтяр Олег Андрійович – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування; Кафка Софія Михайлівна – доктор економічних наук, професор, професор кафедри менеджменту та бізнес-адміністрування; Жук Ольга Іванівна – кандидат економічних наук, доцент, завідувач кафедри публічного управління та адміністрування.

Заслухавши публічну презентацію наукових результатів дисертації Лазаріва Владислава Олеговича та обговоривши її на фаховому семінарі факультету управління, прийнято наступні висновки щодо дисертації: рекомендувати для подання до розгляду та захисту в разовій спеціалізованій вченій раді.

7. Висновок про перевірку дисертацій та наукових публікацій здобувача на виявлення порушення академічної доброчесності з наданням (до витягу додається).

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертації.

Висновок
наукового фахового семінару факультету управління
Карпатського національного університету імені Василя Стефаника
про наукову новизну, теоретичне та практичне значення результатів дисертації «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» здобувача ступеня доктора філософії за спеціальністю 281 Публічне управління та адміністрування з галузі знань 28 Публічне управління та адміністрування

1. Актуальність теми

Розвиток інформаційного суспільства та цифрових технологій формує нову архітектоніку сучасної цивілізації, у якій інформація набуває статусу ключового стратегічного ресурсу для всіх секторів, зокрема і для публічного управління. Трансформація від аграрної до індустріальної, далі до постіндустріальної моделі та, зрештою, до інформаційного суспільства зумовлює зростання ролі обробки, збереження, передачі та захисту інформації як основної цінності соціально-економічного розвитку.

У розвинутих країнах цифрова трансформація охоплює економічну, соціальну сфери та систему надання електронних публічних послуг. У цьому контексті формування та впровадження ефективних механізмів публічного управління інформаційною безпекою стає визначальним чинником стабільності цифрового розвитку держави. Саме механізми публічного управління забезпечують скоординовану дію інституцій, регламентацію процесів, моніторинг ризиків та реалізацію адаптивних управлінських рішень для гарантування безпеки в інформаційному просторі.

Здатність держави розробляти, впроваджувати та оновлювати механізми публічного управління інформаційною безпекою надання електронних послуг визначає рівень її цифрової спроможності, легітимності та довіри з боку громадян. У сучасних умовах ці механізми охоплюють нормативно-правові, організаційно-інституційні, технологічні, кадрові та комунікаційні складові, які взаємодіють у рамках єдиної управлінської системи, спрямованої на протидію загрозам та зміцнення цифрової стійкості.

Інформаційна безпека електронних публічних сервісів є невід'ємною частиною внутрішньої та зовнішньої політики держави, що зумовлює необхідність створення дієвих та адаптивних механізмів публічного управління, здатних ефективно реагувати на комплекс загроз: від цілеспрямованих кібератак до витоку персональних даних, від дезінформації до зниження довіри до державних цифрових сервісів.

Для України, яка декларує інтеграцію до Європейського Союзу та орієнтується на принципи прозорості, відкритості, підзвітності та безпеки в публічному управлінні, формування надійних механізмів публічного управління інформаційною безпекою є технологічним, правовим завданням та виявом інституційної відповідальності, елементом демократичного врядування в цифрову епоху.

Особливої актуальності проблематика забезпечення інформаційної безпеки набула в умовах повномасштабної військової агресії російської федерації проти України. На передній план вийшли ризики, пов'язані з

деструктивними впливами на інформаційний простір: поширенням дезінформації та фейків, хакерськими атаками на державні ресурси, маніпуляцією громадською думкою, незаконним збором та використанням персональних даних. У таких умовах захист інформаційної інфраструктури, що забезпечує функціонування електронних публічних послуг, стає критичним завданням публічного управління.

Вирішення цього завдання потребує системного розгортання ефективних механізмів публічного управління інформаційною безпекою, які ґрунтуються на принципах кіберстійкості, правової визначеності, технологічної спроможності та інституційної взаємодії між органами влади, приватним сектором і громадянським суспільством. Такі механізми мають забезпечувати безперервність управлінських процесів, оперативне реагування на загрози, прозорість і підзвітність дій органів публічного управління у сфері інформаційної безпеки.

Отже, необхідність формування, впровадження та постійного вдосконалення механізмів публічного управління інформаційною безпекою у сфері електронних послуг в умовах цифрової трансформації та постійних безпекових викликів обумовлює теоретичну цінність та високу практичну значущість обраної теми дисертаційного дослідження. Системне дослідження зазначених механізмів дозволить сформувати науково обґрунтовані підходи до побудови ефективної моделі механізмів публічного управління в умовах гібридних загроз і нестабільності.

Вирішення цього завдання потребує системного розгортання ефективних механізмів публічного управління інформаційною безпекою, які ґрунтуються на принципах кіберстійкості, правової визначеності, технологічної спроможності та інституційної взаємодії між органами влади, приватним сектором і громадянським суспільством. Такі механізми мають забезпечувати безперервність управлінських процесів, оперативне реагування на загрози, прозорість і підзвітність дій органів публічного управління у сфері інформаційної безпеки.

2. Зв'язок з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до напрямів дослідження кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника, науково-дослідницької роботи за темою «Теоретико-методологічні та прикладні засади розроблення і функціонування інноваційних механізмів публічного управління та адміністрування» (державний реєстраційний номер: 0120U100494).У межах тем автором проведені дослідження, пов'язані з розробкою механізмів публічного управління забезпечення кібербезпеки надання електронних послуг.

3. Особистий внесок здобувача в отриманні наукових результатів. Дисертація є самостійно виконаним науковим дослідженням. Наукові розробки, висновки та пропозиції, що містяться в роботі, належать особисто автору. Наукові праці, опублікованих у співавторстві відсутні.

4. Теоретичне та практичне значення результатів дисертації Лазаріва Владислава Олеговича на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» виконаного на здобуття наукового ступеня доктора філософії за спеціальністю

281 Публічне управління та адміністрування ефективно впроваджувалися в освітній процес Карпатського національного університету імені Василя Стефаника упродовж 2021-2025 років, зокрема в освітню програму галузі знань D Бізнес, адміністрування та право, спеціальності D4 Публічне управління та адміністрування освітнього рівня бакалавра ОК12 Інформаційні технології в управлінні, ОК 24 Діловодство та електронний документообіг та освітнього рівня магістр ОК 4 Інформаційні технології в публічному управлінні.

5. Ступінь новизни основних результатів дисертації зумовлена поставленими завданнями та результатами їх розв'язання.

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 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.

Використання (апробація) результатів роботи.

Основні положення дисертаційного дослідження, доповідалися, обговорювалися та отримали позитивну оцінку на 6 міжнародних науково-практичних конференціях: 2 Міжнародна науково-практична конференція. From Ideas to Solutions: Innovations in Science and Technology. Лондон. Великобританія (2025); 1 Міжнародна науково-практична конференція. Modern Scientific

Research: Theoretical and Practical Aspects. Рига. Латвія; International Scientific Internet Conference (issue 95). Тернопіль – Ополе. 16-17 січня 2025 року; Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (December 23-25, 2024. San Francisco, USA). European Open Science Space, 2024; IV Міжнародна мультидисциплінарна науково-практична конференція (Луцьк, 20 червня 2023 р.); Modern Aspects of Modernization of Science: Status, Problems, Development Trends. Materials of the 26th International Scientific and Practical Conference. November 7, 2022, Загреб (Хорватія).

Публікації. За результатами дослідження опубліковано 10 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, 6 тез доповідей та матеріалів міжнародних науково-практичних конференцій.

7. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі.

Дисертаційна робота виконана на кафедрі публічного управління та адміністрування, науковий керівник Нагорняк Михайло Миколайович – доктор політичних наук, професор, професор кафедри міжнародних відносин

Робота є результатом самостійних досліджень Лазаріва Владислава Олеговича.

8. Перелік публікацій за темою дисертації. За результатами досліджень опубліковано 10 наукових праць, з яких:

Статті у наукових фахових виданнях України (категорії Б):

1. Лазарів О.В. Порівняльний аналіз моделей публічного управління інформаційною безпекою: світовий досвід. Успіхи і досягнення у науці: № 4 (14) (2025) / серія «Управління та адміністрування»

URL: http://perspectives.pp.ua/index.php/sas/article/view/22944

DOI: https://doi.org/10.52058/3041-1254-2025-4(14)-606-615

2. Лазарів В.О. Кібербезпека та публічне управління: виклики та можливості для електронних послуг. Актуальні питання у сучасній науці № 1(31) (2025): Серія «Публічне управління» 26.01.2025.

URL: http://perspectives.pp.ua/index.php/sn/article/view/18787

DOI: https://doi.org/10.52058/2786-6300-2025-1(31)-281-291

3. Лазарів В.О. Моделювання процесів публічного управління інформаційними технологіями надання електронних послуг на публічному рівні. Актуальні питання у сучасній науці № 1(29) (2024): Серія «Публічне управління» 28.11.2024.

URL: http://perspectives.pp.ua/index.php/sn/article/view/16517

DOI: https://doi.org/10.52058/2786-6300-2024-11(29)-378-388

4. Лазарів О.В. Концептуальні засади публічного управління інформаційною безпекою електронних послуг: теорія та виклики. Наукові перспективи (Серія «Публічне управління»). Випуск No 6(36) 2023. 01.07.2023.

URL: http://perspectives.pp.ua/index.php/np/issue/view/156

DOI: https://doi.org/10.52058/2708-7530-2023-6(36)-143-150

Матеріали і тези наукових конференцій:

1. Лазарів В.О. Інформаційна безпека як складова цифрової трансформації публічних послуг: механізми інтеграції у практику публічного управління. 2

Міжнародна науково-практична конференція. From Ideas to Solutions: Innovations in Science and Technology. Лондон. Великобританія.

URL: https://www.eoss-conf.com/arkhiv/from-ideas-to-solutions-innovations-in-science-and-technology-21-04-25/

2. Лазарів В.О. Механізми забезпечення кіберстійкості в системі публічного управління електронними послугами: міжнародні та українські реалії. 1 Міжнародна науково-практична конференція. Modern Scientific Research: Theoretical and Practical Aspects. Рига. Латвія.

URL: https://www.eoss-conf.com/arkhiv/modern-scientific-research-theoretical-and-practical-aspects/

3. Лазарів В.О. Політики захисту даних у публічному секторі: кращі світові практики для безпеки електронних послуг. International Scientific Internet Conference (issue 95). Тернопіль – Ополе. 16-17 січня 2025 року.

URL:http://www.konferenciaonline.org.ua/data/downloads/file_1736632243.pdf

4. Лазарів В.О. Цифрові технології як основа для побудови ефективних систем інформаційної безпеки в публічному управлінні. Collection of Scientific Papers with the Proceedings of the 2nd International Scientific and Practical Conference «Innovative Solutions in Science: Balancing Theory and Practice» (December 23-25, 2024. San Francisco, USA). European Open Science Space, 2024. 297 p. 181-183

URL:https://www.eoss-conf.com/wp-content/uploads/2024/12/San_Francisco_USA_23.12.2024.pdf

5. Лазарів В.О. Публічне управління інформаційною безпекою: сучасні виклики та перспективи розвитку. Наукова інтеграція в умовах глобальних викликів: збірник тез доповідей IV Міжнародної мультидисциплінарної науково-практичної конференції (Луцьк, 20 червня 2023 р.). / За заг. ред. Павліхи Н. В. – Луцьк : Вежа-Друк, 2023.

URL:https://www.researchgate.net/publication/372438666_NAUKOVA_INTEGRACIA_V_UMOVAH_GLOBALNIH_VIKLIKIV_Zbirnik_tez_dopovidej_IV_MIZNARODNOI_MULTIDISCIPLINARNOI_NAUKOVO-PRAKTICNOI_KONFERENCII

6. Лазарів В.О. Публічне управління інформаційною безпекою: сучасні виклики та перспективи розвитку. Modern Aspects of Modernization of Science: Status, Problems, Development Trends. Materials of the 26th International Scientific and Practical Conference. November 7, 2022, Zagreb (Croatia) remotely.

URL: http://perspectives.pp.ua/public/site/conferency/conf-26.pdf

1. Наукове значення виконаного дослідження із зазначенням можливих наукових галузей та розділів програм навчальних курсів, де можуть бути застосовані отримані результати.

Отримані результати можуть бути застосовані в галузях знань вищої освіти «Публічне управління та адміністрування» та «Бізнес, адміністрування та право». Зокрема, в освітній процес Карпатського національного університету імені Василя Стефаника упродовж 2021-2025 років, зокрема в освітню програму галузі знань D Бізнес, адміністрування та право, спеціальності D4 Публічне управління та адміністрування освітнього рівня бакалавр ОК12 Інформаційні

технології в управлінні, ОК 24 Діловодство та електронний документообіг та освітнього рівня магістр ОК 4 Інформаційні технології в публічному управлінні.

Матеріали дисертації можна використовувати у проведенні навчання із підвищення кваліфікації державних службовців і посадових осіб місцевого самоврядування, представників громадських організацій.

2. Практична цінність результатів дослідження із зазначенням конкретного підприємства або галузі народного господарства, де вони можуть бути застосовані.

Результати дослідження мають значну практичну цінність для діяльності регіонального відділення ВАОМС «Асоціація міст України», Департаменту інфраструктури, житлової иа комунальної власності Івано-Франківської міської ради, ТОВ « Н-ІКС ДЕЛІВЕРІ»

Матеріали дослідження можуть використовуватись в практичній діяльності, зокрема, концептуальну модель механізмів публічного управління інформаційною безпекою електронних послуг, яка охоплює взаємопов'язані компоненти: нормативно-правовий, інституційно-організаційний, функціонально-комунікаційний і технологічний, що функціонують як єдина система публічного управлінського впливу, спрямована на забезпечення цифрової стійкості публічних сервісів. Практичне впровадження розроблених автором рекомендацій дозволяє забезпечити підвищення показників ефективності й якості публічного управління.

3. Оцінка структури дисертації, її мови та стилю викладення. Дисертація за структурою, мовою та стилем викладення відповідає вимогам МОН України.

ВВАЖАТИ:

1. Що дисертаційна робота Лазаріва В.О. на тему «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід» є завершеною науковою працею, у якій розв'язано конкретне наукове завдання з розробки науково-обгрунтованих пропозицій щодо публічного управління інформаційною безпекою надання електронних послуг, що має важливе значення для галузі знань 28 Публічне управління та адміністрування.

2. За темою дисертації опубліковано 10 наукових публікацій, де повністю відображені основні результати дисертації, з яких: 4 статті надруковано в наукових фахових України (категорії Б) у виданнях з державного управління; 6 тез – у матеріалах науково-практичних конференцій.

3. Дисертація відповідає вимогам, встановленим Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії постанова Кабінету Міністрів України від 12.01.2022 р. № 44 (зі змінами) та Вимогами до оформлення дисертації наказ Міністерства освіти і науки України від 12.01.2017 № 40 (зі змінами).

РЕКОМЕНДУВАТИ дисертаційну роботу «Механізми публічного управління інформаційною безпекою надання електронних послуг: світовий досвід», подану Лазарівим Владиславом Олеговичем на здобуття ступеня доктора філософії. Рекомендується для подання до розгляду та захисту у

спеціалізованій вченій раді Карпатського національного університету імені Василя Стефаника.

Розглянувши заяви і документи голови СВР, рецензентів і опонентів та встановивши, що подані документи відповідають вимогам до членів спеціалізованої вченої ради згідно Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії Постанова Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами).

Пропонувати вченій раді Університету призначити наступний склад разової ради:

Головою разової спеціалізованої вченої ради

1. Сурай Інна Геннадіївна – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника (м. Івано-Франківськ).

Докторська дисертація: диплом 31.10.2014 р., спеціальність 25.00.03 – державна служба.

ORCID: https://orcid.org/0000-0003-4377-2724

1. Goncharuk, N., Pyrohova, Y., Suray, I., Prokopenko, L and Prudius, L. (2023). Reformation Public Administration in Ukraine in the Context of European Integration: Current State, Problems and Priorities. Economic Affairs, Vol. 68, No. 03, pp. 1613-1627, September 2023 .

DOI: http://dx.doi.org/10.46852/0424-2513.3.2023.27

URL:https://www.scopus.com/pages/publications/85177025883?origin=resultslist

ISSN : 0424-2513 *(SCOPUS, Q3)*

Keywords: Public management, European integration, public administration, public service, government service, digitalization, sustainable development, innovative approaches, innovative development, administrative service

2. Сурай І. Г. Цифрова трансформація публічного управління: семантичний аналіз поняття. Державне управління: удосконалення та розвиток. 2024. № 1. (електронне фахове видання, категорія Б)

DOI: http://doi.org/10.32702/2307-2156.2024.1.2

URL: https://nayka.com.ua/index.php/dy/article/view/2828/2864

Ключові слова: цифровізація (диджиталізація), цифрова трансформація, державне управління, публічне управління, парадигмальні зміни, цифрова трансформація публічного управління, цифрова трансформація в публічному управлінні, цифрові технології, цифрова трансформація регіонів, цифрова трансформація освіти

3. Сурай І. Тенденції щодо надання публічних адміністративних послуг в Україні. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2024. Вип.8. С.116–125. фах. видання, категорія Б)

DOI: https://doi.org/10.31470/2786-6246-2024-8-116-125

URL: https://pa.journal.in.ua/index.php/pa/article/view/145/147 (

Ключові слова: публічне/державне управління, публічні послуги, адміністративні послуги, електронні послуги, цифрові технології, цифровізація,

цифровізація публічних послуг, цифрова трансформація, європейська інтеграція, інформаційна безпека

Рецензенти:

1. Дєгтяр Олег Андрійович – доктор наук з державного управління, професор, професор кафедри публічного управління та адміністрування Карпатського національного університету імені Василя Стефаника (м. Івано-Франківськ).

Докторська дисертація: диплом 28.04.2015 р. спеціальність 25.00.02 – механізми державного управління

ORCID: https://orcid.org/0000-0001-6413-3580

1. Радзівілов Г. Д., Остапчук В. М., Дєгтяр О. А. Міжнародний досвід цифровізації державних послуг в Україні. Національні інтереси України. 2025. № 6(11) 2025. С. 996-1006. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-996-1006

URL: http://perspectives.pp.ua/index.php/niu/article/view/25312

Ключові слова: цифровізація державних послуг, імплементація електронні послуги, зарубіжний досвід, органи державної влади держава

2. Радзівілов Г., Дєгтяр О. Вплив цифровізації на ефективність державних сервісів в умовах війни. Національні інтереси України. 2025. №5(10) 2025. С. 1234-1242.(фах. видання, категорія Б)

DOI: https://doi.org/10.52058/3041-1793-2025-5(10)-1234-1242

URL: http://perspectives.pp.ua/index.php/niu/article/view/23790/23761

Ключові слова: цифрові платформи, державні послуги, взаємодія з громадянами, війна, кібербезпека, захист персональних даних, цифрова трансформація, гуманітарна допомога

3. Дєгтяр О. А. Цифрові технології як інструмент зміцнення інформаційної безпеки в системах публічного управління. Актуальні питання у сучасній науці. Серія Державне управління. 2025. № 4(34) 2025. С. 194-206. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/2786-6300-2025-4(34)-194-206

URL: http://perspectives.pp.ua/index.php/sn/article/view/22523/22493

Ключові слова: публічне управління, механізми публічного управління Інформація, інформаційна безпека, електронні послуги, публічні послуги цифрові технології, цифровізація публічних послуг європейська

4. Дєгтяр О. А. Використання технологій штучного інтелекту у публічному управлінні інформаційною безпекою // Електронне наукове видання. Публічне адміністрування та національна безпека. - 2024. - №3. С. 73-80.(фах. видання, категорія Б)

DOI: https://doi.org/10.25313/2617-572X-2024-3-9785

URL: https://www.inter-nauka.com/issues/administration2024/3/9785

Ключові слова: публічне управління, механізми публічного управління, інформація, інформаційна безпека, публічне управління інформаційною безпекою, цифрові технології, цифровізація, цифрова трансформація

2. П'ятничук Ірина Дмитрівна – кандидат економічних наук, доцент, декан факультету управління Карпатського національного університету імені Василя Стефаника (м. Івано-Франківськ).

Кандидатська дисертація: диплом 04.07.2013 р., спеціальність 08.00.09 – Бухгалтерський облік, аналіз і аудит.

ORCID: https://orcid.org/ 0000-0003-2876-6422

1. П'ятничук І.Д. Публічне управління наданням електронних послуг: аналіз ефективності та напрямки подальших покращень. *«Успіхи і досягнення у науці». (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»).* 2024. N 4(4). С. 522 – 533. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/3041-1254-2024-4(4)-522-533

URL: https://perspectives.pp.ua/index.php/sas/article/view/12607/12669

Ключові слова: публічне управління, електронні послуги, публічні послуги, публічне управління наданням електронних послуг, цифрова трансформація, цифрові технології, ефективність.

2. П'ятничук І.Д. Нормативно-правовий механізм публічного управління процесами захисту інформаційної безпеки у сфері надання електронних послуг. *Наукові перспективи.* 2024. No 4 (46). С. 361–370. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/2708-7530-2024-4(46)-361-370

URL: https://perspectives.pp.ua/index.php/np/article/view/10977/11036

Ключові слова: нормативно-правові механізми, публічне управління, захист інформаційної безпеки, електронні послуги, цифрові технології, інформаційна безпека, механізми публічного управління, інформація публічні послуги

3. П'ятничук І.Д. Інноваційні стратегії забезпечення інформаційної безпеки у сфері електронних послуг: аналіз світового досвіду. *Національні інтереси України.* 2025. 8(13). С. 1002 – 1011. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/3041-1793-2025-8(13)-1002-1011

URL http://perspectives.pp.ua/index.php/niu/article/view/27458/27423

Ключові слова: публічне управління, механізми публічного управління, інформація, інформаційна безпека, електронні послуги, публічні послуги, цифрові технології, цифровізація публічних послуг, європейська інтеграція

Офіційні опоненти:

1. Пархоменко-Куцевіл Оксана Ігорівна – доктор наук з державного управління, професор, завідувач кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі (м. Переяслав).

Докторська дисертація: диплом 25.01.2013 р., спеціальність 25.00.01 – теорія та історія державного управління.

ORCID: https://orcid.org/0000-0002-0758-346X

1. Пархоменко-Куцевіл О. І. Запровадження цифровізації у процес забезпечення якості публічних послуг. *Наукові інновації та передові технології. Серія «Управління та адміністрування».* 2024. № 2(30). С. 235-245. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/2786-5274-2024-2(30)-235-245

URL: http://perspectives.pp.ua/index.php/nauka/article/view/8998/9045

Ключові слова: публічні послуги, цифровізація, цифровізація публічних послуг, цифровізація державних послуг, цифровізація якості надання публічних

послуг, територіальні громади, місцеве самоврядування, якість публічних послуг, штучний інтелект, інформаційно-комунікативні технології

2. Пархоменко-Куцевіл О. І. Теоретичні аспекти забезпечення якості публічних послуг: світовий та національний досвід. *Наукові перспективи*. 2023. № 9. С. 168-178. (фах. видання, категорія Б)

DOI: https://doi.org/10.52058/2708-7530-2023-9(39)-168-178

URL: http://perspectives.pp.ua/index.php/np/article/view/6509/6542

Ключові слова: публічні послуги, адміністративні послуги, якість послуг на рівні громад, якість публічних послуг, цифровізація, процес забезпечення якості публічних послуг, оцінка та контроль якості публічних послуг, управління якістю публічних послуг, стандартизація публічних послуг

3. Пархоменко-Куцевіл О. І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. *Публічне управління і адміністрування в Україні*. 2022. Вип. 28. С. 177-181.

DOI: https://doi.org/10.32843/pma2663-5240-2022.28.35

URL: http://www.pag-journal.iei.od.ua/archives/2022/28-2022/35.pdf

Ключові слова: державне управління, інформація, інформаційна безпека, фейки, фейкові новини, військові дії, військові конфлікти

2. Маматова Тетяна Валеріївна – доктор наук з державного управління, професор, професор кафедри державного управління і місцевого самоврядування Національного технічного університету «Дніпровська політехніка» (м. Дніпро)

Докторська дисертація: диплом 22.04.2011 р., спеціальність 25.00.02 – механізми державного управління

ORCID: https://orcid.org/0000-0003-1844-5377

1. Маматова Т., Чикаренко І., Бородін, Є. Цифрові платформи Smart Specialisation Platform та ESPON: структура та можливості для регіонів і громад ЄС. *Аспекти публічного управління*. 2022. Т. 10, № 6. С. 37-45. (Фахове видання)

DOI: https://doi.org/10.15421/152242

URL: https://aspects.org.ua/index.php/journal/article/view/969/944

Ключові слова: стратегія, інфраструктурний проєкт, соціальний проєкт, регіон, територіальна громада, співробітництво, дижиталізація, публічне управління

2. Маматова Т., Борисенко Ю. Цифрове врядування: сучасні світові тренди та особливості розвитку в Україні. *Публічне управління та місцеве самоврядування*. 2024. № 2. С. 46-53. (фах. видання, категорія Б)

DOI: https://doi.org/10.32782/2414-4436/2024-2-6

URL: https://journals.politehnica.dp.ua/index.php/public/article/view/609

Ключові слова: публічне управління, цифровізація, цифрова трансформація, цифрове врядування, е-врядування, резільєнтність, Україна, Війна, повоєнне відновлення

3. Gustafsson, M., Matveieva, O., Wihlborg, E., ... Mamatova, T., Kvitka, S. Adaptive governance amidst the war: Overcoming challenges and strengthening collaborative digital service provision in Ukraine. *Government Information QuarterlyOpen source preview*, 2025, 42(3), 102056

ISSN: 0740-624X.

DOI: https://doi.org/10.1016/j.giq.2025.102056
URL:https://www.scopus.com/pages/publications/105009864276?origin=resultslist
Keywords: Civil society; Collaboration; Diia; Institutions; Local government; Ukraine; War

Голова фахового семінару
доктор політичних наук,
професор, професор кафедри
політичних інститутів та процесів Сергій ДЕРЕВ'ЯНКО

Секретар фахового семінару
доктор філософії (Економіка),
асистент кафедри публічного
управління та адміністрування Наталія ДРАБЧУК

21 листопада 2025 року.