УДК 351:004.9:[351.86:004.056]
DOI: https://doi.org/10.17721/3041-1912.2025/4-9/10

Олександр ЯКУНІН, асп.
ORCID ID: 0009-0001-6554-2033
e-mail: Oleksandr_Yakunin@proton.me
Київський національний університет імені Тараса Шевченка, Київ, Україна

КОНЦЕПТУАЛІЗАЦІЯ МОДЕЛІ "Е-ПОСЛУГ 4.0" ЯК ЧИННИКА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: ЄВРОПЕЙСЬКИЙ ДИСКУРС

Вступ. ***Обґрунтовано, що за умов ескалації гібридних загроз й інтенсифікації євроінтеграційних процесів переосмислення моделей надання державних послуг постає не лише сервісним завданням, а й критичним чинником забезпечення цифрового суверенітету та інституційної стійкості національної системи публічного управління. Метою пропонованого дослідження є концептуалізація моделі "Е-послуг 4.0" у парадигмі національної безпеки, виявлення її стратегічних характеристик у європейському дискурсі й обґрунтування ролі захищених мобільних екосистем у забезпеченні превентивності та стійкості державних інституцій.***

Методи. ***Застосовано комплексний методологічний підхід, що базується на системному аналізі еволюції моделей урядування крізь призму безпекових парадигм. Використано методи порівняльно-управлінського аналізу для зіставлення вітчизняної нормативної бази з безпековими положеннями Берлінської декларації та стандартів eIDAS 2.0. Особливу роль відведено прогностично-аналітичному методу для оцінки архітектури Mobile-First як базису забезпечення цифрової стійкості (resilience) держави в умовах воєнного стану та кібератак.***

Результати. ***Засвідчено, що вітчизняна модель публічного управління потребує зміни філософії — від "реактивної держави" до "предиктивного цифрового врядування", де автоматизація нівелює людський чинник у критичних точках взаємодії. Виявлено, що ключовими атрибутами "Е-послуг 4.0" у безпековому вимірі є алгоритмічне прийняття, транскордонна сумісність за замовчуванням (cross-border by design) і проактивність, яка допомагає випереджати соціальні та безпекові кризи. Встановлено, що інтелектуалізація сервісів є фундаментом для створення "невидимого уряду" (invisible government), спроможного функціонувати в умовах фізичного пошкодження традиційної адміністративної інфраструктури.***

Висновки. ***На підставі аналізу доведено необхідність модернізації системи публічного адміністрування на засадах архітектурної інтероперабельності та принципу одноразовості (Once-only), що мінімізує вразливість державних реєстрів. Уперше здійснено концептуалізацію "Е-послуг 4.0" як управлінської та безпекової категорії, що інтегрує технологічний інструментарій Industry 4.0 у систему захисту національних інтересів у межах європейського адміністративного простору. Практична значущість результатів полягає в можливості їхнього використання суб'єктами сектору безпеки й оборони, а також органами влади для розроблення стратегій цифрової стійкості й автоматизації антикризових управлінських процесів.***

Ключові слова: ***е-послуги 4.0, національна безпека, публічне управління, цифрова стійкість (resilience), кіберстійкість, інтероперабельність, предиктивне врядування, невидимий уряд (invisible government), мобільна екосистема, цифрова ідентичність, алгоритмічне адміністрування, європейська інтеграція.***

Вступ

Актуальність дослідження. Глобальна парадигма публічного управління в умовах гібридних викликів XXI ст. зазнає фундаментальної трансформації, що зумовлена необхідністю пошуку нових механізмів забезпечення інституційної безпеки держави. Традиційні моделі електронного урядування (e-Government), орієнтовані на просту диджиталізацію паперових форм, поступово вичерпують свій потенціал у протидії сучасним загрозам (Margetts, & Dunleavy, 2013; Lindgren et al., 2019). Попередні етапи цифровізації, фокусуючись на переведенні адміністративних процесів у цифровий формат, не вирішували критичних проблем бюрократичної інерції, корупційних ризиків і вразливості централізованих систем перед кіберзагрозами (Clarke, 2020; Атаманова, & Луняченко, 2024). У контексті національної безпеки дискреція службовців і фізичне прив'язування до адміністративної інфраструктури постають як чинники ризику, що можуть бути використані для дестабілізації врядування.

Стрімкий розвиток технологій четвертої промислової революції (Industry 4.0) − штучного інтелекту, великих даних і децентралізованих систем ідентифікації − вимагає переосмислення природи взаємодії між державою та громадянином через призму цифрового суверенітету (Misuraca, & Viscusi, 2020; Hammerschmid et al., 2023). Постає стратегічна необхідність впровадження концепції "Е-послуг 4.0", яка базується на принципах проактивності, безшовності (seamlessness) та повної алгоритмізації процедур (Tangi et al., 2021; Wilson, & Mergel, 2022). З погляду безпеки, перехід до алгоритмічного адміністрування дає змогу вилучити людський чинник із критичних вузлів ухвалення рішень, забезпечуючи надійність й оперативність функціонування держави в екстремальних умовах.

Актуальність теми посилюється потребою теоретико-методологічного обґрунтування безпекового виміру інтеграції України до Єдиного цифрового ринку ЄС (Digital Single Market) (European Commission, 2022). Реалізація цілей "Цифрового десятиліття 2030" (Digital Decade 2030) та виконання вимог Interoperable Europe Act (Regulation (EU) 2024/903, 2024) вимагають від вітчизняної науки публічного управління формування архітектури цифрової стійкості (resilience). Державне управління має розглядатися не як сукупність вразливих фізичних установ, а як гнучка, розосереджена цифрова платформа, спроможна зберігати керованість соціально-економічними процесами незалежно від зовнішнього тиску (Schou, & Hjelholt, 2018). Для України в умовах воєнної агресії та подальшого повоєнного відновлення розроблення моделі "Е-послуг 4.0" стає критичним складником національної стійкості, гарантуючи безперервність надання публічних сервісів і захист цифрової ідентичності громадян як фундаментального активу держави (Громова, 2025; Маркович, 2021).

Питання трансформації державного управління у цифрову епоху в безпековому вимірі перебувають у фокусі уваги провідних учених. Г. Маргеттс та П. Данліві, зок-

© Якунін Олександр, 2025

ISSN 3041-1912 (Print), ISSN 3041-1920 (Online)

рема, обґрунтували модель "Digital Era Governance", яку в сучасних умовах розглядають як спосіб реінтеграції державних функцій для підвищення їхньої стійкості до зовнішніх впливів (Margetts, & Dunleavy, 2013). Проблеми інтероперабельності як чинника транскордонної безпеки та сумісності адміністрацій досліджено в роботі (Tangi et al., 2021). Безпекові аспекти алгоритмічного врядування та використання ШІ в публічному секторі як засоби автоматизації антикризових рішень представлені у праці (Misuraca, & Viscusi, 2020). Критичний аналіз цифрової держави як інструменту забезпечення суверенітету та нової форми публічної влади надано у дослідженнях Дж. Шоу та М. Хьєльхольта (Schou, & Hjelholt, 2018).

Попри значну кількість праць, концептуалізація саме четвертого покоління е-послуг як категорії національної безпеки в українському науковому дискурсі залишається фрагментарною. Поза увагою дослідників часто залишається потенціал моделі 4.0 у нейтралізації гібридних загроз і забезпеченні цифрового суверенітету, що й визначає напрям пропонованої статті (Дворніченко, 2024; Громова, 2025; Рачинський, & Титаренко, 2024; Кожина та ін., 2026; Ситник, 2025).

Мета дослідження – теоретичне обґрунтування та концептуалізація моделі "Е-послуг 4.0" як стратегічного інструменту забезпечення національної безпеки й інституційної стійкості публічного управління, що базується на алгоритмізації процесів, захисті цифрового суверенітету й імплементації європейських стандартів безпекової інтероперабельності.

Для досягнення поставленої мети визначено такі завдання:

- проаналізувати еволюцію моделей врядування у контексті зміни безпекових парадигм – від централізованого бюрократичного апарату до децентралізованої моделі "Ера цифрового уряду 4.0" ("Digital Era Governance 4.0"), що забезпечує безперервність управління (continuity of government) у кризових умовах;
- розкрити сутність "Е-послуг 4.0" крізь призму мінімізації управлінських вразливостей, виокремивши такі атрибути, як предиктивність, транскордонна захищеність та алгоритмічна нейтральність, що дають змогу вилучити людський чинник із критичних вузлів адміністрування;
- обґрунтувати роль захищеної мобільної екосистеми як пріоритетної та найбільш стійкої платформи для реалізації сервісів четвертого покоління, що гарантує інклюзивність і безпеку доступу громадян до державних ресурсів незалежно від фізичного розташування;
- визначити вектори адаптації безпекових стандартів цифрового врядування ЄС (зокрема положень Берлінської та Талліннської декларацій, Interoperable Europe Act) у вітчизняну практику публічного управління з метою синхронізації архітектури національної безпеки з європейським цифровим простором.

Методи

У дослідженні застосовано комплексний методологічний підхід, що базується на синтезі класичних методів теорії публічного управління та спеціальних підходів до аналізу безпеки цифрових трансформацій.

Для дослідження еволюції концепцій урядування (від "e-Government" до "Digital Government 4.0") крізь призму забезпечення інституційної стійкості використано метод системного аналізу та дедукції (Margetts, & Dunleavy, 2013; Schou & Hjelholt, 2018). Це дало змогу розглянути "Е-послуги 4.0" не лише як технологічну інновацію, а і як стратегічний елемент системи національної безпеки, що трансформує роль держави від реактивного сервісного супроводу до проактивного управління ризиками та забезпечення безперервності владних функцій.

Другим етапом стало застосування порівняльно-управлінського методу. Було проведено компаративний аналіз безпекових стандартів у стратегічних документах ЄС (Берлінська та Талліннська декларації, Interoperable Europe Act) (Berlin Declaration…, 2020; Tallinn Declaration…, 2017; Regulation (EU) 2024/903, 2024) та поточної нормативно-правової бази України. Це допомогло виявити розбіжності між вітчизняною моделлю "цифровізації як технічного процесу" та європейським підходом "цифровізації як захищеної екосистеми", заснованої на принципах безпекової інтероперабельності та транскордонної стійкості даних (Tangi et al., 2021).

Також застосовано прогностично-аналітичний метод для оцінювання потенціалу мобільних екосистем у контексті національної стійкості. Аналіз звітів "eGovernment Benchmark" і кращих світових практик упровадження мобільного врядування (m-Government) допоміг обґрунтувати пріоритетність архітектури Mobile-First як найбільш життєздатної платформи для забезпечення цифрової стійкості (resilience) держави. Такий підхід розглянуто як інструмент гарантування доступу до критично важливих сервісів і збереження цифрової ідентичності громадян в умовах воєнного стану, гібридних загроз і руйнування фізичної адміністративної інфраструктури (Wilson, & Mergel, 2022; Hammerschmid et al., 2023).

Комплексне використання зазначених методів дало змогу забезпечити репрезентативність висновків і обґрунтувати когнітивну модель урядування як фундамент нової архітектури безпеки в межах європейського адміністративного простору.

Результати

Дослідження генезису управлінської філософії у ретроспективі переходу від e-Government до Digital Government 4.0 дає змогу стверджувати, що трансформація моделі надання публічних послуг безпосередньо корелює з еволюцією парадигм забезпечення інституційної стійкості держави (Margetts, & Dunleavy, 2013; Schou, & Hjelholt, 2018). Якщо традиційна бюрократія М. Вебера базувалася на жорсткій ієрархії та вразливому до фізичних загроз паперовому документообігу, то сучасний етап розвитку державного адміністрування вимагає впровадження Algorithmic Governance (алгоритмічного врядування). У межах національної безпеки цей підхід означає перетворення технологій на засадниче середовище ухвалення управлінських рішень, що мінімізує ризики суб'єктивізму та забезпечує безперервність функціонування державних інститутів (Misuraca, & Viscusi, 2020).

На основі аналізу концепцій Digital Era Governance (DEG) і вимог щодо кіберстійкості критичної інфраструктури, ми виокремлюємо чотири етапи трансформації, де рівень 4.0 постає як вища форма цифрового суверенітету (див. табл. 1).

Аналізуючи логіку переходу до когнітивного врядування, варто зауважити, що на рівнях 1.0-2.0 домінувала парадигма "Нове державне управління" ("New Public Management", NPM), де послугу розглядали як дискретний продукт, а безпека обмежувалася периметром конкретного відомства (Lindgren et al., 2019). Така модель зумовлювала збереження "силосної" структури (silo mentality), за якої кожне міністерство оперувало автономними і часто несумісними базами даних. З погляду безпеки, це створювало критичні вразливості — фрагментарність інформації уповільнювала реакцію на кризи, а громадянин, виконуючи функцію "кур'єра" між

ISSN 1728-3817

реєстрами, ставав слабкою ланкою в ланцюгу передачі державних даних (Tangi et al., 2021).

Перехід до "Цифрового уряду 3.0" ("Digital Government 3.0") допоміг ініціювати створення перших інтегрованих платформ (зокрема мобільного застосунку "Дія"), що заклали фундамент для інституційної стійкості. Проте лише модель 4.0 забезпечує перехід до "невидимого уряду" ("invisible government"), де безпека досягається через повну алгоритмізацію міжвідомчої взаємодії. У такому контурі держава не просто реагує на запит, а предиктивно моделює сценарії надання послуг й управління ризиками, що є визначальним для національної безпеки в цифровому просторі (Wilson, & Mergel, 2022).

Таблиця 1

Матриця еволюції публічного врядування та безпеки сервісів

Рівень	Концептуальна модель	Пріоритетна технологія	Роль держави у безпековому контурі	Стратегія стійкості
1.0	Digitization	Web 1.0 (Статичні сайти)	Інформатор	Оцифрування даних
2.0	E-Government	Web 2.0 (Портали, форми)	Надавач послуг (реактивний)	Автоматизація запитів
3.0	Digital Government	Хмарні обчислення, Mobile	Платформа взаємодії	Сервісна інтеграція
4.0	Digital Government 4.0	ШІ, Big Data, Blockchain	Захищена когнітивна екосистема	Предиктивна стійкість

Джерело. Розроблено автором.

Справжня трансформація управлінської парадигми відбувається на рівні 4.0, що ознаменовує перехід до нової онтології публічної влади, де цифрові технології постають гарантом інституційної безпеки. "Е-послуги 4.0" базуються на принципі одноразовості подання даних (Once-only), закріпленому в Талліннській декларації (Tallinn Declaration…, 2017). У безпековому контексті цей принцип означає відмову держави від надлишкового й інвазивного збору інформації на користь захищеного оперування верифікованими даними в розподілених реєстрах (Regulation (EU) 2024/903, 2024). Це мінімізує ризики витоку персональних даних та запобігає створенню вразливих "інформаційних накопичувачів", що можуть стати ціллю кібератак.

Як засвідчують дані, наведені на рис. 1, перехід до когнітивного врядування супроводжується делегуванням рутинних повноважень алгоритмічним системам. У вимірі національної безпеки це означає докорінну зміну архітектури публічної влади − перехід від ієрархічної бюрократії до алгоритмічного суверенітету (Misuraca, & Viscusi, 2020). На рис. 1 показано поетапний розвиток моделей − від базової цифровізації до формування когнітивного врядування, спроможного підтримувати життєдіяльність держави за умов критичного пошкодження фізичної інфраструктури (Schou, & Hjelholt, 2018).

Як ілюструє рис. 1, розвиток цифрового врядування відбувається шляхом поступового нарощування когнітивних спроможностей держави. На рівні 4.0 ми бачимо перехід від інвазивної моделі збору даних до алгоритмічного оперування верифікованою інформацією. Це дає змогу реалізувати модель "невидимого уряду", де державний інтерфейс стає безшовним і стійким до зовнішніх гібридних впливів внаслідок вилучення людського чинника з процесу обробки інформації.



Рис. 1. Еволюційна модель переходу до алгоритмічного врядування та предиктивної стійкості (Resilience)
Джерело. Розроблено автором.

Логічним завершенням трансформації публічного управління в межах концепції 4.0 постає модель "невидимого уряду" ("Invisible Government"). З позицій національної стійкості (resilience), ключовою перевагою цього рівня є автономне ініціювання адміністративних процедур у разі настання юридично значущого факту або життєвої ситуації (Life Event) (Tangi et al., 2021). У безпековому вимірі це забезпечує безперервність надання критичних сервісів. Наприклад, автоматичне нарахування соціальних виплат чи коригування статусів осіб у зонах конфлікту відбувається без необхідності їхнього фізичного звернення до установ, що в умовах загрози життю є життєво важливим чинником.

Застосування такої моделі радикально трансформує роль державного апарату. Алгоритмічні системи, перебираючи на себе функцію прийняття рутинних рішень, фактично здійснюють автоматизовану антикорупційну селекцію, усуваючи надмірну адміністративну дискрецію, яка в умовах кризи може стати джерелом дестабілізації (Hammerschmid et al., 2023). Отже, реалізується концепція безшовних послуг (Seamless Services), де інституційні бар'єри між органами влади нівелюються, утворюючи єдиний, інтегрований і захищений "державний інтерфейс", стійкий до зовнішніх маніпуляцій та гібридного впливу (Tangi et al., 2021).

У межах формування моделі "Е-послуг 4.0" особливого значення набуває архітектурний принцип Mobile-First, який ми пропонуємо розглядати як фундамент інклюзивної безпеки. Аналіз поточної ситуації в Україні доводить, що мобільна екосистема (на прикладі застосунку "Дія") виявилася найбільш стійкою платформою публічного управління в умовах масштабних криз і воєнних загроз. На відміну від стаціонарних порталів, мобільні екосистеми забезпечують безперервний доступ до державних сервісів та цифрової ідентичності навіть за умови часткового руйнування наземної зв'язної інфраструктури, завдяки використанню децентралізованих мереж і мобільного інтернету.

З позицій національної безпеки, роль мобільної екосистеми в парадигмі 4.0 реалізується через три стратегічні вектори, а саме:

- гарантування цифрової ідентичності (Digital Identity Resilience),
- предиктивна комунікація та антикризовий менедмент,
- інтероперабельність як захист інформаційного суверенітету.

Щодо першого – упровадження стандартів eIDAS 2.0 і перспективного European Digital Identity Wallet (EUDI) у мобільну архітектуру дає громадянину можливість володіти захищеним цифровим гаманцем, що визнається на транскордонному рівні (Regulation (EU) 2024/1183, 2024). Для національної безпеки це означає захист персональних даних від несанкціонованого доступу та можливість ідентифікації особи за будь-яких умов, що є критичним для забезпечення правопорядку та надання соціального захисту в зонах ризику. По-друге, мобільна платформа 4.0 функціонує як сенсорний вузол, що допомагає державі здійснювати превентивне інформування та автоматизовану координацію дій населення. Алгоритмізація сповіщень про безпекові загрози або зміни в адміністративних статусах перетворює смартфон на інструмент оперативного управління безпекою, де швидкість доведення інформації стає критичним чинником мінімізації втрат. І третє, мобільна екосистема, побудована за стандартами ЄС, забезпечує безшовний обмін даними за принципом Once-only. Це усуває потребу у створенні дублюючих, а отже, − вразливих точок входу до державних реєстрів. Використання єдиного, високонадійного мобільного інтерфейсу зменшує "поверхню атаки" для кіберзлочинців і гібридних впливів, спрямованих на дискредитацію державних інституцій.

Отже, мобільна екосистема в контексті "Е-послуг 4.0" постає не просто зручним засобом взаємодії, а автономним модулем врядування, що забезпечує стабільність зв'язку "держава − людина" у глобальному безпековому просторі.

Аналіз характеристик "Е-послуг 4.0" у межах європейського дискурсу дає змогу простежити фундаментальну трансформацію акцентів − від суто технологічних рішень до глибинних безпекових і ціннісних орієнтирів (Berlin Declaration…, 2020; European Commission, 2022). Сучасна парадигма публічного управління визначає цифрові сервіси нового покоління як фундаментальну основу цифрового суверенітету та стійкості демократичних інститутів (Tallinn Declaration…, 2017). У цьому контексті ми виокремлюємо три засадничі характеристики моделі 4.0, що формують її безпекове ядро.

По-перше, визначальною рисою є проактивність (Proactivity), заснована на концепції життєвих ситуацій (Life Events). Якщо традиційна адміністративна парадигма спиралася на заявницький принцип (що є вразливим у ситуаціях кризи або втрати громадянином доступу до зв'язку), то рівень 4.0 змінює цю логіку на користь випереджального антикризового врядування. Згідно з Берлінською декларацією (Berlin Declaration…, 2020), цифрова трансформація має стати піонером у захисті прав громадян. У межах національної безпеки це означає делегування державі відповідальності за моніторинг життєвих обставин особи. Така проактивність, що реалізується через Data-driven governance, допомагає підтримувати життєдіяльність соціуму в автоматичному режимі, нівелюючи потребу у фізичній присутності в установах, що є критичним для мінімізації ризиків у зонах конфліктів і надзвичайних ситуацій (Wilson, & Mergel, 2022).

Другою характеристикою є транскордонна безпека за замовчуванням (Cross-border by design). У парадигмі 4.0 державні кордони перестають бути бар'єрами для захисту прав громадян. Послуга, ініційована в Україні, має бути функціонально зрозумілою та технічно захищеною у всьому європейському середовищі. Згідно з Талліннською декларацією (Tallinn Declaration…, 2017), інтероперабельність – наріжний камінь безпечного Єдиного цифрового ринку. Важливо наголосити, що інтероперабельність (Interoperability) тут розглянуто як інституційну спроможність до оперативної транскордонної співпраці органів влади без створення додаткових вразливостей у внутрішніх процедурах (Regulation (EU) 2024/903, 2024).

Третій складник – алгоритмічне врядування (Algorithmic Governance) та впровадження етичного штучного інтелекту для автоматизації критичних управлінських рішень. Цей перехід до моделі, де алгоритмічний код мінімізує простір для суб'єктивізму, вимагає суворого дотримання принципу антропоцентричності. Як зазначено в Interoperable Europe Act (Regulation (EU) 2024/903, 2024), інтероперабельність має працювати на користь людей. У моделі 4.0 алгоритмічне управління постає вагомою безпековою категорією, яка гарантує прозорість та невідворотність надання публічних благ, повністю усуваючи "людський чинник" як потенційне джерело корупції, зловживань або ворожого впливу на чиновників (Hammerschmid et al., 2023).

ISSN 1728-3817



Рис. 2. Мобільна екосистема в парадигмі 4.0 як автономний модуль урядування (Resilience)

Джерело. Розроблено автором.

Взаємозумовленість зазначених характеристик (див. рис. 2) вказує на те, що без транскордонної інтероперабельності проактивність залишатиметься локальним інструментом, неспроможним забезпечити колективну цифрову стійкість у межах європейського безпекового простору (Tangi et al., 2021).

Запропонована концептуальна модель (рис. 2) відображає ієрархічну взаємозалежність компонентів, де кожен елемент постає необхідною умовою для функціонування всієї системи цифрової безпеки в парадигмі 4.0. Транскордонність (Cross-border) на рисунку є базовою площиною, що забезпечує інтероперабельну сумісність України з безпековим контуром ЄС. Без цього фундаменту локальні цифрові рішення залишатимуться вразливими до ізоляції в умовах глобальних кіберзагроз. Алгоритмізація (Algorithmic Governance) – інструментальна вершина, що забезпечує технічну реалізацію "невидимого врядування". Вона перетворює дані на управлінські рішення без ризику корупційного втручання або помилок, зумовлених людським чинником у критичні моменти. Проактивність (Proactivity) постає результативною складовою, що безпосередньо впливає на стійкість соціуму. Саме через проактивність держава виконує свою безпекову функцію − захист громадянина в автоматичному режимі, випереджаючи виникнення кризових ситуацій.

Отже, тріада характеристик на рис. 2 демонструє перехід від сервісного обслуговування до предиктивної системи національної стійкості, де алгоритмічний суверенітет (центрична частина моделі) гарантує стабільність демократичного врядування.

Окремої уваги у контексті парадигми публічного управління 4.0 потребує обґрунтування ролі мобільної екосистеми як базової платформи (рис. 3). У межах формування моделі "Е-послуг 4.0" архітектурний принцип Mobile-First трансформується з технологічного рішення у стратегічний фундамент забезпечення інституційної безпеки та цифрової стійкості (Digital Resilience). Досвід України 2022–2026 рр. довів, що мобільна екосистема (на прикладі архітектури застосунку "Дія") є найбільш життєздатною платформою публічного управління в умовах масштабних криз. За умови пошкодження наземної адміністративної інфраструктури саме мобільні рішення гарантують безперервність врядування (Business Continuity), функціонуючи як автономні вузли безпечної взаємодії між державою та громадянином (Кожина та ін., 2026). Пріоритетність мобільної платформи 4.0 обґрунтовується її здатністю бути носієм самоврядної ідентичності (Self-Sovereign Identity) та захищеним "цифровим гаманцем" згідно зі стандартами eIDAS 2.0 (Regulation (EU) 2024/1183, 2024). Це дає змогу реалізувати концепцію "цифрового гуманітарного коридору", де інтероперабельність досягається безпосередньо на рівні кінцевого інтерфейсу користувача, мінімізуючи "поверхню атаки" на державні реєстри та забезпечуючи високу доступність критичних сервісів незалежно від географічного розташування суб'єкта (European Commission, 2022; Hammerschmid et al., 2023).

Дискусія і висновки

На основі проведеного дослідження здійснено концептуалізацію моделі "Е-послуг 4.0" як фундаментальної складової системи національної безпеки та інституційної стійкості України в умовах євроінтеграції. За результатами аналізу доведено, що еволюція від e-Government до Digital Government 4.0 є об'єктивним процесом переходу до алгоритмічного врядування, яке в безпековому вимірі мінімізує вразливість державного апарату перед гібридними загрозами та корупційними ризиками. Визначено, що ключові атрибути моделі 4.0 − проактивність, транскордонність й алгоритмічність − утворюють єдину тріаду цифрової стійкості. Це допомагає реалізувати концепцію "невидимого уряду", спроможного забезпечувати безперервність публічного управління незалежно від фізичної цілісності адміністративної інфраструктури. Обґрунтовано пріоритетність мобільної екосистеми як найбільш захищеної та інклюзивної платформи для взаємодії "держава − громадянин". Встановлено, що впровадження європейських стандартів цифрової ідентичності (eIDAS 2.0) у мобільну архітектуру є запорукою захисту цифрового суверенітету України. Рекомендовано органам публічної влади змістити акценти у стратегіях цифрової трансформації з кількісного оцифрування послуг на побудову інтероперабельного безпекового сере-

довища за принципом Once-only. Перспективи подальших досліджень полягають у деталізації алгоритмів етичного штучного інтелекту в ухваленні адміністративних рішень і розробці методології оцінки цифрової стійкості органів місцевого самоврядування в умовах воєнного стану.



Рис. 3. Концептуальна модель "Е-послуги 4.0". Тріада характеристик стійкості цифрового врядування

Джерело. Розроблено автором.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

Атаманова, Н. В., & Луняченко, І. В. (2024). До питання цифровізації публічного управління в Україні. *Юридичний науковий електронний журнал*, 68. https://doi.org/10.32782/2307-1745.2024.68.1

Громова, О. В. (2025). Розвиток концепції сервісної держави як стратегічний напрям трансформації публічного управління в Україні. *Вісник економіки транспорту і промисловості*, 90, 52–60. https://orcid.org/0000-0002-1332-8094

Дворніченко, А. С. (2024). Цифровізація публічної політики в системі державного управління. *Дніпровський науковий часопис публічного управління, психології, права*, 6. https://doi.org/10.51547/ppp.dp.ua/2024.6.3

Рачинський, А. П., & Титаренко, О. М. (2024). Цифрова трансформація публічного управління у напрямі сервісизації. *Державне будівництво*, 2(36). https://doi.org/10.26565/1992-2337-2024-2-38

Berlin Declaration on Digital Society and Value-based Digital Government. (2020). https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

Clarke, A. (2020). Digital government units: What are they, and what do they mean for digital era public management renewal? *International Public Management Journal, 23*(3), 358–379. https://doi.org/10.1080/10967494.2019.1686447

European Commission. (2022). *Declaration on European Digital Rights and Principles for the Digital Decade*. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

Hammerschmid, G., Palaric, E., Rackwitz, M., & Wegrich, K. (2023). A shift in paradigm? Collaborative public administration in the context of national digitalization strategies. *Governance*. https://doi.org/10.1111/gove.12778

Lindgren, I., Madsen, C. Ø., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A critical analysis of the digitalization of public services. *Government Information Quarterly, 36*(3), 427–436. https://doi.org/10.1016/j.giq.2019.03.002

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A, 371*(1987), Article 20120382. https://doi.org/10.1098/rsta.2012.0382

Misuraca, G., & Viscusi, G. (2020). AI-enabled innovation in the public sector: A framework for digital governance and resilience. In *Proceedings of the 19th International Conference on Electronic Government (EGOV 2020)* (pp. 110–120). Springer. https://doi.org/10.1007/978-3-030-57599-1_9

Regulation (EU) 2024/903. (2024). Interoperable Europe Act. https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng

Schou, J., & Hjelholt, M. (2018). *Digitalization and public sector transformations*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76291-3

Tallinn Declaration on eGovernment. (2017). https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. *International Journal of Information Management, 60*, 102356. https://doi.org/10.1016/j.ijinfomgt. 2021.102356

Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: Mapping the strategies of digital champions. *Government Information Quarterly, 39*(2), 101681. https://doi.org/10.1016/j.giq.2022.101681.

References

Atamanova, N. V., & Luniachenko, I. V. (2024). On the issue of digitalization of public administration in Ukraine. *Legal Scientific Electronic Journal*, 68 [in Ukrainian]. https://doi.org/10.32782/2307-1745.2024.68.1

Berlin Declaration on Digital Society and Value-based Digital Government. (2020). https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

Clarke, A. (2020). Digital government units: What are they, and what do they mean for digital era public management renewal? *International Public Management Journal, 23*(3), 358–379. https://doi.org/10.1080/10967494.2019.1686447

Dvornichenko, A. S. (2024). Digitalization of public policy in the system of public administration. *Dnipro Scientific Journal of Public Administration, Psychology, Law*, 6. https://doi.org/10.51547/ppp.dp.ua/2024.6.3 [in Ukrainian]

European Commission. (2022). Declaration on European Digital Rights and Principles for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

Hammerschmid, G., Palaric, E., Rackwitz, M., & Wegrich, K. (2023). A shift in paradigm? Collaborative public administration in the context of national digitalization strategies. *Governance*. https://doi.org/10.1111/gove.12778

Hromova, O. V. (2025). Development of the concept of a service state as a strategic direction of the transformation of public administration in Ukraine. *Bulletin of Transport and Industry Economics*, 90, 52–60 [in Ukrainian]. https://orcid.org/0000-0002-1332-8094

Lindgren, I., Madsen, C. Ø., Hofmann, S., & Melin, U. (2019). Close encounters of the digital kind: A critical analysis of the digitalization of public services. *Government Information Quarterly, 36*(3), 427–436. https://doi.org/10.1016/j.giq.2019.03.002

Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A, 371*(1987), Article 20120382. https://doi.org/10.1098/rsta.2012.0382

Misuraca, G., & Viscusi, G. (2020). AI-enabled innovation in the public sector: A framework for digital governance and resilience. In *Proceedings of the 19th International Conference on Electronic Government (EGOV 2020)* (pp. 110–120). Springer. https://doi.org/10.1007/978-3-030-57599-1_9

Rachynskyi, A. P., & Tytarenko, O. M. (2024). Digital transformation of public administration towards servicization. *State Building*, 2(36) [in Ukrainian]. https://doi.org/10.25565/1992-2337-2024-2-38

Regulation (EU) 2024/903 of the European Parliament and of the Council. (2024). Interoperable Europe Act. https://eur-lex.europa.eu/eli/reg/2024/903/oj/eng

Schou, J., & Hjelholt, M. (2018). *Digitalization and public sector transformations*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76291-3

Tallinn Declaration on eGovernment. (2017). https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and impeding factors. *International Journal of Information Management, 60*, 102356. https://doi.org/10.1016/j.ijinfomgt.2021.102356

Wilson, C., & Mergel, I. (2022). Overcoming barriers to digital government: Mapping the strategies of digital champions. *Government Information Quarterly, 39*(2), 101681. https://doi.org/10.1016/j.giq.2022.101681

Отримано редакцією журналу / Received: 28.10.25
Прорецензовано / Revised: 03.11.25
Схвалено до друку / Accepted:18.11.25

Oleksandr Yakunin, PhD Student
ORCID ID: 0009-0001-6554-2033
e-mail: Oleksandr_Yakunin@proton.me
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

CONCEPTUALIZATION OF THE "E-SERVICES 4.0" MODEL AS A FACTOR IN ENSURING NATIONAL SECURITY UNDER DIGITAL TRANSFORMATION: THE EUROPEAN DISCOURSE

Background. ***The article substantiates that amidst escalating hybrid threats and intensified European integration processes, the reconceptualization of public service delivery models emerges not merely as a service-oriented task but as a critical factor in ensuring digital sovereignty and institutional resilience of the national public administration system. It is emphasized that in Ukraine, this process requires a transition from traditional automation to the implementation of intelligent "E-services 4.0," which serve as a tool for guaranteeing the continuity of government and protecting citizens' digital identities. It is highlighted that the existing theoretical and methodological framework of public administration in Ukraine is characterized by inertia, which creates security risks during the implementation of the "Digital Decade 2030" strategy. The research aim is to conceptualize the "E-services 4.0" model within the national security paradigm, identify its strategic characteristics in the European discourse, and substantiate the role of secure mobile ecosystems in ensuring the preventiveness and resilience of state institutions.***

Methods. ***A comprehensive methodological approach has been applied, based on a systemic analysis of the evolution of governance models through the lens of security paradigms. Comparative managerial analysis methods were used to contrast the national regulatory framework with the security provisions of the Berlin Declaration and eIDAS 2.0 standards. Particular emphasis is placed on the prognostic-analytical method to evaluate the Mobile-First architecture as a basis for ensuring the state's digital resilience under conditions of martial law and cyberattacks.***

Results. ***It is evidenced that the Ukrainian model of public administration requires a fundamental shift in philosophy: from a "reactive state" to "predictive digital governance," where automation mitigates the human factor at critical points of interaction. It is found that the key attributes of "E-services 4.0" in the security dimension are algorithmic decision-making (reducing corruption risks as a threat to national security), cross-border by design compatibility, and proactivity, which allows for outstripping social and security crises. It is established that the intellectualization of services serves as the foundation for creating an "invisible government" capable of functioning despite physical damage to traditional administrative infrastructure.***

Conclusions. ***Based on the analysis, the necessity of modernizing the public administration system on the foundations of architectural interoperability and the Once-only principle, which minimizes the vulnerability of state registries, is proven. The development of a secure mobile ecosystem is identified as a priority direction for forming an inclusive and safe platform for implementing seamless services. For the first time, "E-services 4.0" has been conceptualized as a managerial and security category that integrates Industry 4.0 technological tools into the system for protecting national interests within the European administrative space. The practical significance of the results lies in the possibility of their utilization by stakeholders in the security and defense sector, as well as by government authorities, for developing digital resilience strategies and automating anti-crisis management processes.***

Keywords: ***e-services 4.0, national security, public administration, digital resilience, cyber resilience, interoperability, predictive governance, invisible government, mobile ecosystem, digital identity, algorithmic administration, European integration.***

Автор заявляє про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Видавничо-поліграфічний центр "Київський університет" Версія НЕ ДЛЯ ДРУКУ