ECONOMIC SECURITY OF THE STATE AND ECONOMIC ENTITIES

УДК 351:004.056.5(477)
JEL H11, K24, O33
DOI: 10.26906/EiR.2026.2(101).4661

ПУБЛІЧНО-УПРАВЛІНСЬКІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

Казанська Олена Олександрівна*, кандидат наук з державного управління, доцент, доцент кафедри маркетингу
Хороших Вікторія Валеріївна, кандидат наук з державного управління, доцент, доцент кафедри маркетингу**
Національний університет «Київський авіаційний університет»
Аракелова Інна Олександрівна*, кандидат економічних наук, доцент, доцент кафедри маркетингу та туризму**
Маріупольський державний університет

**ORCID 0000-0002-8100-5350*
***ORCID 0000-0001-8373-180X*
****ORCID 0000-0001-9582-793X*

Дата надходження статті: 30.03.2026
Дата прийняття статті: 20.04.2026
Дата публікації статті: 29.05.2026

Вступ. Цифровий суверенітет держави, особливо у воєнний час, означає не просто контроль над власною цифровою інфраструктурою, а є фактичною умовою інституційного виживання держави. Україна за період 2022–2025 років довела свою здатність працювати онлайн під час кібератак, руйнування або знищення фізичної інфраструктури та окупації територій. Саме це стає вже не просто питанням ефективності, а питанням збереження державності.

Не дивлячись на підвищену увагу влади до питання захисту інформаційного простору України, у системі публічного управління досі відсутня комплексна модель механізмів забезпечення цифрового суверенітету. Інституційні, правові, організаційні та міжнародні складові цього процесу функціонують розрізнено: повноваження розподілені між Міністерством цифрової трансформації України (Мінцифри), Державної служби спеціального зв'язку та захисту інформації (Держспецзв'язку) та Радою національної безпеки і оборони України (РНБО). В той же час, нормативно-правова база містить суттєві недоліки, а міжнародне партнерство у цифровій сфері не має чіткого управлінського оформлення. Все це свідчить про відсутність комплексного публічно-управлінського механізму або моделі публічного управління цифровим суверенітетом.

Огляд останніх джерел досліджень і публікацій. Питання цифрового суверенітету та механізмів публічного управління у цифровій сфері досліджується багатьма українськими і закордонними науковцями з різних позицій. Так, Єфремова К.В. [1] визначає цифровий суверенітет через здатність держави створити автономну цифрову інфраструктуру та самостійно здійснювати її керування. У свою чергу, Ярема О.Г. [2] розглядає інформаційно-правовий механізм забезпечення державного суверенітету як систему організаційних, нормативних та інструментально-процесуальних елементів, виділяючи юрис-

дикційний і технологічний підходи. Солодка О. [3] обґрунтовує необхідність комплексної нормативно-правової регламентації інформаційного суверенітету та чіткого визначення повноважень відповідних органів і їх координації. Милосердна І.М. [4] аналізує досвід формування цифрового суверенітету в ЄС, де акцент робиться на технологічній незалежності та захисті індивідуальних прав.

У сфері механізмів публічного управління Мохова Ю.Л. [5] сформувала інституційно-правовий механізм електронного урядування, Польовий П.В. [6] дослідив нормативно-правовий механізм цифрових трансформацій органів влади, Коваленко С.В. [7] розробила механізми державного управління цифровою трансформацією територіальних громад. Волошин Ю.О. та Шаповал А.О. [8] обґрунтовують, що реалізація цифрового суверенітету особливо загострюється в умовах збройних конфліктів, коли держави розширюють межі втручання у цифровий простір. У міжнародній науці Pohle J. та Thiel T. [9] виокремлюють чотири моделі національного цифрового суверенітету, а Larsen B.C. [10] пов'язує його з контролем над повним ланцюжком постачань у сфері штучного інтелекту.

Водночас аналіз наукових джерел засвідчує низку суттєвих недоліків. По-перше, цифровий суверенітет досі не концептуалізований як самостійний об'єкт публічного управління з відповідною системою механізмів реалізації, оскільки наявні дослідження зосереджені переважно на правовому або безпековому вимірах. По-друге, відсутні роботи, які б системно описували публічно-управлінські механізми забезпечення цифрового суверенітету саме в умовах збройного конфлікту. По-третє, незважаючи на те, що Україна у 2024 році посіла перше місце за Індексом цифрової залученості громадян ООН [11], питання цифрової залежності від іноземних хмарних провайдерів і відсутність власних стандартів залишаються поза увагою науки публічного управління. По-четверте, розподіл повноважень між Мінцифри, Держспецзв'язку та РНБО залишається неузгодженим і недостатньо дослідженим у науці публічного управління.

Саме тому, **метою дослідження** є концептуалізація цифрового суверенітету як об'єкта публічного управління та розробка комплексної моделі публічно-управлінських механізмів його забезпечення в умовах воєнного стану на основі аналізу українського досвіду 2022–2025 років.

Основний матеріал і результати. Аналіз наукових підходів до визначення цифрового суверенітету свідчить про відсутність єдиного розуміння цього поняття в науці публічного управління. Більшість дослідників розглядають його або крізь призму права (контроль над даними та інфраструктурою), або крізь призму безпеки (захист від кібератак та інформаційного впливу). Однак, що стосується управлінського виміру, а саме, механізми, суб'єкти та інструменти реалізації державної політики у цифровій сфері, залишається концептуально незавершеним.

З позицій публічного управління цифровий суверенітет доцільно розглядати як здатність держави через систему публічно-управлінських механізмів забезпечувати контроль над власною цифровою інфраструктурою, інформаційними потоками та технологічним середовищем, зберігаючи при цьому інституційну спроможність до прийняття самостійних управлінських рішень у цифровій сфері. Таке визначення, на відміну від наявних, акцентує увагу не на технічному чи правовому боці проблеми, а на управлінській спроможності держави як ключовій умові суверенітету.

Важливим є розмежування цифрового суверенітету від суміжних понять. Інформаційний суверенітет, закріплений у Законі України «Про Національну програму інформатизації» [12], трактується як здатність контролювати інформаційні потоки з-за меж держави. Кібербезпека, згідно зі Стратегією кібербезпеки України [13], охоплює захист кіберпростору від загроз. Цифровий суверенітет є ширшим поняттям, що поєднує обидва виміри та додає до них технологічну незалежність і управлінську автономію держави у цифровому просторі.

В умовах воєнного стану зміст цифрового суверенітету набуває специфічних характеристик. По-перше, він стає умовою безперервності державного управління, а саме, здатності органів влади функціонувати попри фізичного знищення інфраструктури. По-друге, він набуває оборонного виміру – цифрові системи стають інструментом як захисту, так і ведення бойових дій. По-третє, він виявляє внутрішнє протиріччя між потребою у швидкій цифровізації та ризиками технологічної залежності від іноземних провайдерів, адже частка американських хмарних провайдерів на українському ринку складає близько 75% [11], що ставить під сумнів реальний рівень цифрового суверенітету держави.

Повномасштабне вторгнення рф у 2022 році стало безпрецедентним випробуванням для цифрової інфраструктури України та системи публічного управління загалом. Аналіз українського досвіду 2022–2025 років дозволяє виокремити чотири ключові виклики:

1. Масштабні кібератаки на критичну інфраструктуру. З початку повномасштабного вторгнення Україна зазнає безліч кібератак на об'єкти енергетики, зв'язку, державні реєстри та фінансову систему. Це поставило під загрозу функціонування базових публічних сервісів і змусило органи влади переглянути підходи до захисту цифрової інфраструктури.

2. Проблема технологічної залежності. Евакуація державних даних у хмарне середовище іноземних провайдерів, таких як Microsoft Azure, Amazon Web Services, Google Cloud, вирішила тактичне завдання збереження даних, однак створила стратегічний виклик для цифрового суверенітету. У законодавчому полі України досі відсутнє поняття «резидентства даних» – принципу, за яким дані повинні зберігатися та оброблятися в українській юрисдикції, що є ключовим елементом цифрового суверенітету [14].

3. Інституційна невизначеність функцій. Мінцифри є головним органом щодо розвитку оборонних інновацій, однак формально до сектору безпеки і оборони не належить [15], що створює інституційні розриви в системі управління цифровим суверенітетом. Повноваження між Мінцифри, Держспецзв'язку та РНБО залишаються розмежованими без чіткого координаційного механізму.

4. Недосконалість нормативно-правової бази. Попри ухвалення Закону про хмарні послуги [16], Стратегії WINWIN [17] та оновлення Стратегії кібербезпеки [18], цілісна нормативна база щодо забезпечення цифрового суверенітету як самостійного об'єкта державної політики в Україні відсутня.

Саме тому запропонована стратегія кібербезпеки передбачає впровадження сучасних принципів, методів, підходів та механізмів публічного управління у сфері кібербезпеки [18], однак не містить комплексного бачення публічно-управлінських механізмів забезпечення цифрового суверенітету.

На основі аналізу наукових джерел, нормативно-правової бази та українського досвіду 2022–2025 років пропонується авторська комплексна модель публічно-управлінських механізмів забезпечення цифрового суверенітету держави в умовах воєнного стану (рис. 1), яка охоплює чотири взаємопов'язані механізми:

1. Інституційний механізм передбачає чітке визначення суб'єктів забезпечення цифрового суверенітету та розмежування їхніх повноважень. Ключовими суб'єктами є Міністерство цифрової трансформації України як головний орган цифрової політики, Державна служба спеціального зв'язку та захисту інформації як регулятор у сфері кібербезпеки, Рада національної безпеки і оборони як координаційний орган стратегічних рішень, а також CERT-UA як оперативний центр реагування на кіберінциденти. Проблемою залишається відсутність єдиного координаційного органу, що забезпечував би узгоджену реалізацію цифрового суверенітету як цілісної державної політики.

2. Правовий механізм охоплює нормативно-правове забезпечення цифрового суверенітету. Його основу становлять Закон України «Про основні засади забезпечення кібербезпеки України» [18], Закон «Про хмарні послуги» [16], Закон «Про критичну інфраструктуру» [19] та Стратегія цифрового розвитку інноваційної діяльності України WINWIN [17]. Водночас правовий механізм має суттєві недоліки: відсутність закону про цифровий суверенітет як самостійний об'єкт регулювання, невизначеність поняття резидентства даних, неврегульованість питання технологічного суверенітету в умовах воєнного стану.

3. Організаційний механізм включає практичні інструменти забезпечення цифрового суверенітету. Серед них – платформа «Дія» як основний канал цифрової взаємодії держави з громадянами, система електронної взаємодії «Трембіта» як захищена міжвідомча платформа обміну даними, практика хмарної евакуації державних даних як антикризовий інструмент збереження інформаційних ресурсів, а також ІТ-армія та кіберрезерв як нові організаційні форми залучення цивільних фахівців до захисту цифрового суверенітету. Кількість цифрових транзакцій у системі «Трембіта» зросла з 62,7 млн у третьому кварталі 2021 року до 541,3 млн у першому кварталі 2023 року [20], що свідчить про критичну залежність публічного управління від цієї системи та необхідність її надійного захисту.

4. Міжнародний механізм відображає зовнішній вимір забезпечення цифрового суверенітету. Він охоплює процес інтеграції України до європейського цифрового простору в рамках виконання вимог директиви NIS2, партнерство з Агентством ЄС з кібербезпеки ENISA, договірну співпрацю з глобальними технологічними компаніями Microsoft, AWS та Google щодо захисту державних даних, а також участь у міжнародній ініціативі Digital4Freedom. Цей механізм має подвійну природу: з одного боку, він зміцнює технологічний потенціал держави, а з іншого – поглиблює залежність від іноземних платформ, що само по собі є викликом для цифрового суверенітету.

Отже, запропонована модель відображає системний характер публічно-управлінських механізмів забезпечення цифрового суверенітету та їхню взаємозалежність. Ефективність кожного окремого механізму визначається не лише його внутрішньою спроможністю, а й узгодженістю з іншими елементами

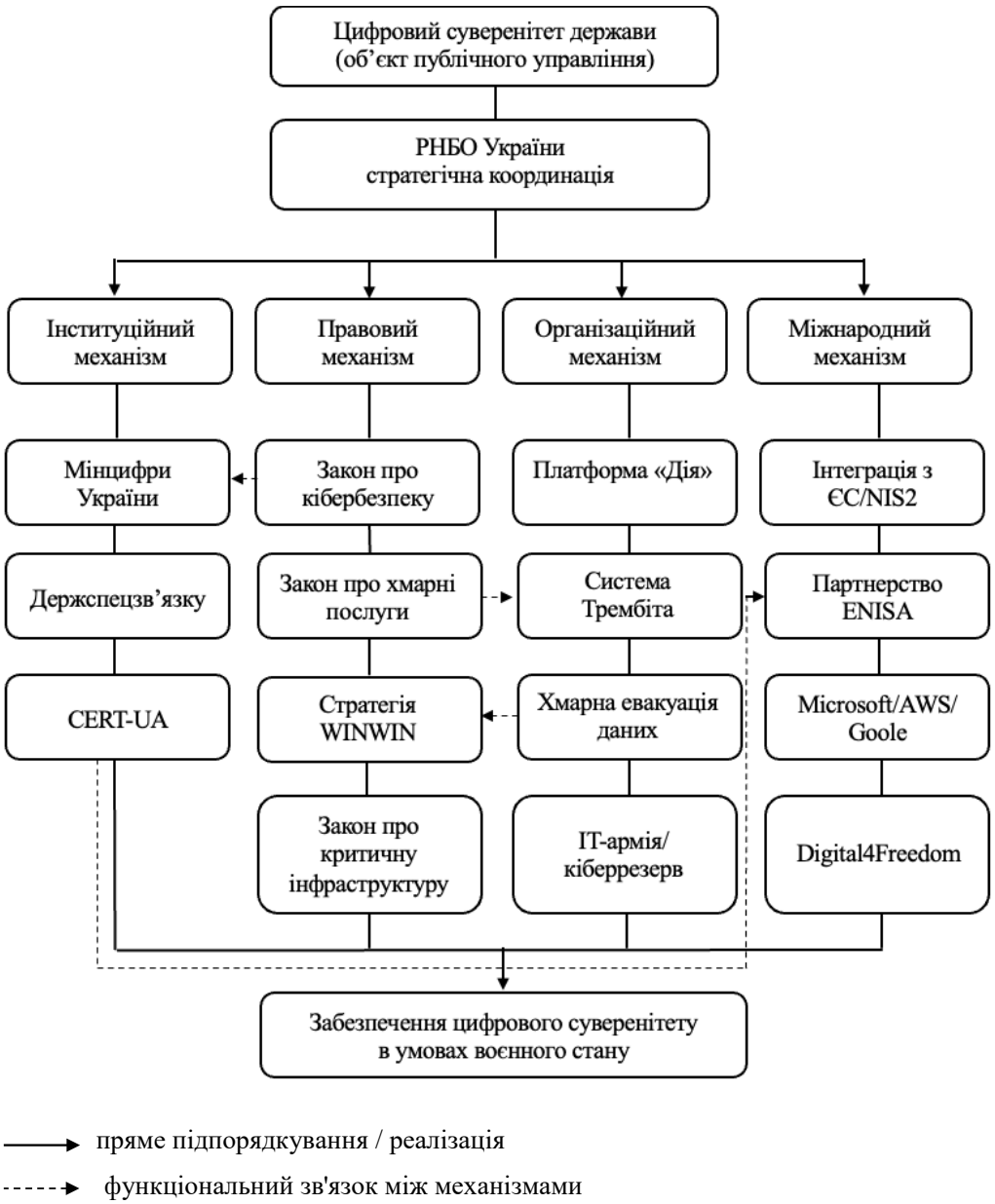

Рис. 1. Публічно-управлінські механізми забезпечення цифрового суверенітету держави в умовах воєнного стану

Джерело: складено автором на основі аналізу наукових джерел та нормативно-правової бази

системи. Саме відсутність такої узгодженості є ключовою проблемою публічного управління цифровим суверенітетом України в умовах воєнного стану.

Висновки. Роблячи висновок, зазначимо, що цифровий суверенітет держави в умовах воєнного стану є не лише технічною чи правовою категорією, а повноцінним об'єктом публічного управління, що потребує системного підходу до його забезпечення. Авторське визначення цифрового суверенітету як здатності держави через систему публічно-управлінських механізмів забезпечувати контроль над власною цифровою інфраструктурою, інформаційними потоками та технологічним середовищем, зберігаючи інституційну спроможність до самостійних управлінських рішень у цифровій сфері, розширює наявні підходи за рахунок управлінського виміру.

Запропонована авторська модель публічно-управлінських механізмів дозволила систематизувати основні суб'єкти забезпечення цифрового суверенітету з урахуванням їхньої ієрархії; визначити функціональні зв'язки між механізмами; врахувати специфіку воєнного стану через включення антикризових інструментів.

Перспективними напрямами подальших досліджень є розробка критеріїв оцінки ефективності публічно-управлінських механізмів забезпечення цифрового суверенітету, вироблення пропозицій щодо усунення нормативно-правових недоліків, зокрема законодавчого визначення резидентства даних, а також формування єдиного координаційного органу у сфері цифрового суверенітету.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ:

1. Єфремова К.В. Забезпечення цифрового суверенітету держави в умовах Індустрії 4.0. *Конституційні засади розвитку інноваційного суспільства:* зб. наук. пр. Харків: НДІ ПЗІР НАПрН України, 2021. С. 25–30. URL: https://openarchive.nure.ua/handle/document/17435
2. Ярема О.Г. Зміст інформаційного суверенітету у контексті державного суверенітету. *Юридичний науковий електронний журнал.* 2022. № 3. С. 191–194. DOI: https://doi.org/10.32782/2524-0374/2022-3/43
3. Солодка О. Пріоритетні напрями забезпечення інформаційного суверенітету України. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 85, ч. 3. С. 134–138. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.20
4. Милосердна І.М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Науковий журнал «Політикус».* 2024. Вип. 6. С. 154–160. DOI: https://doi.org/10.24195/2414-9616.2024-6.23
5. Мохова Ю.Л. Інституційно-правовий механізм забезпечення електронного урядування в Україні. *Інвестиції: практика та досвід*. 2021. № 13–14. С. 93–97. DOI: https://doi.org/10.32702/2306-6814.2021.13-14.93
6. Польовий П.В. Нормативно-правовий механізм цифрових трансформацій в органах публічної влади та розвитку цифрових компетентностей публічних службовців. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2022. Т. 33 (72), № 4. С. 84–93. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.4/14
7. Коваленко С.В. Механізми державного управління цифровою трансформацією територіально-економічних систем: дис. … д-ра філософії: 281. Чернігів: Національний університет «Чернігівська політехніка», 2024. 247 с.
8. Волошин Ю.О., Шаповал А.О. Цифровий суверенітет та міжнародні зобов'язання держав: межі допустимого втручання у цифровий простір. *Юридичний науковий електронний журнал.* 2026. № 2. С. 177–181. DOI: https://doi.org/10.32782/2524-0374/2026-2/38
9. Pohle J., Thiel T. Digital sovereignty. *Internet Policy Review.* 2020. Vol. 9, Issue 4. DOI: https://doi.org/10.14763/2020.4.1532
10. Larsen B.C. The Geopolitics of AI and the Rise of Digital Sovereignty. *Brookings*. 2022. URL: https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/
11. Цифровий суверенітет України: як ми ризикуємо стати цифровою колонією. *Dev.ua.* 2025. URL: https://dev.ua/news/gigacloud-one-1751973165
12. Про Національну програму інформатизації: Закон України від 04.02.1998 № 74/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/74/98-вр
13. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013
14. Хабібрахманова Т. Стратегія, якої бракує Україні: чому цифровий суверенітет має стати державним пріоритетом. *ЛІГА.Блоги.* 2024. URL: https://blog.liga.net/user/tkhabibrakhmanova/article/58460
15. Звіт Рахункової палати № 33-1/2025. URL: https://rp.gov.ua/upload-files/Activity/Collegium/2025/33-1_2025/Zvtit_33-1_2025.pdf
16. Про хмарні послуги: Закон України від 17.02.2022 № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20
17. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України (WINWIN): Розпорядження КМУ від 31.12.2024 № 1351-р. URL: https://zakon.rada.gov.ua/laws/show/1351-2024-р
18. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
19. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
20. Моніторинговий звіт Програми SIGMA: Державне управління в Україні. 2023. URL: https://mof.gov.ua/storage/files/Звіт_Програми_SIGMA_(укр).pdf

REFERENCES:

1. Yefremova K.V. (2021) Zabezpechennia tsyfrovoho suverenitetu derzhavy v umovakh industrii 4.0 [Ensuring the digital sovereignty of the state in the conditions of industry 4.0]. *Konstytutsiini zasady rozvytku innovatsiinoho suspilstva*. Kharkiv: NDI PZIR NAPrN Ukrainy. P. 25–30. Available at: https://openarchive.nure.ua/handle/document/17435 (in Ukrainian)
2. Yarema O.H. (2022) Zmist informatsiinoho suverenitetu u konteksti derzhavnoho suverenitetu [Content of information sovereignty in the context of state sovereignty]. *Yurydychnyi naukovyi elektronnyi zhurnal*. № 3. P. 191–194. DOI: https://doi.org/10.32782/2524-0374/2022-3/43 (in Ukrainian)
3. Solodka O. (2024) Pryorytetni napriamy zabezpechennia informatsiinoho suverenitetu Ukrainy [Priority directions of securing the information sovereignty of Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo.* Vyp. 85, ch. 3. P. 134–138. DOI: https://doi.org/10.24144/2307-3322.2024.85.3.20 (in Ukrainian)

4. Myloserdna I.M. (2024) Tsyfrovyi suverenitet derzhavy: naukova rytoryka ta realni zminy [Digital sovereignty of the state: scientific rhetoric and real changes]. *Naukovyi zhurnal "Politykus"*. Vyp. 6. P. 154–160. DOI: https://doi.org/10.24195/2414-9616.2024-6.23 (in Ukrainian)

5. Mokhova Yu.L. (2021) Instytutsiino-pravovyi mekhanizm zabezpechennia elektronnoho uriaduvannia v Ukraini [Institutional and legal mechanism for e-governance in Ukraine]. *Investytsii: praktyka ta dosvid*. № 13–14. P. 93–97. DOI: https://doi.org/10.32702/2306-6814.2021.13-14.93 (in Ukrainian)

6. Polovyi P.V. (2022) Normatyvno-pravovyi mekhanizm tsyfrovykh transformatsii v orhanakh publichnoi vlady ta rozvytku tsyfrovykh kompetentnostei publichnykh sluzhbovtsiv [Regulatory and legal mechanism of digital transformations in public authorities and development of digital competencies]. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V.I. Vernadskoho*. T. 33 (72), № 4. P. 84–93. DOI: https://doi.org/10.32782/TNU-2663-6468/2022.4/14 (in Ukrainian)

7. Kovalenko S.V. (2024) Mekhanizmy derzhavnoho upravlinnia tsyfrovoiu transformatsiieiu terytorialno-ekonomichnykh system [Mechanisms of public administration of digital transformation of territorial-economic systems]: dys. … d-ra filosofii: 281. Chernihiv: Natsionalnyi universytet "Chernihivska politekhnika". 247 pp. (in Ukrainian)

8. Voloshyn Yu.O., Shapoval A.O. (2026) Tsyfrovyi suverenitet ta mizhnarodni zobov'iazannia derzhav: mezhi dopustymoho vtruchannia u tsyfrovyi prostir [Digital sovereignty and international obligations of states: limits of permissible intervention in the digital space]. *Yurydychnyi naukovyi elektronnyi zhurnal.* № 2. P. 177–181. DOI: https://doi.org/10.32782/2524-0374/2026-2/38 (in Ukrainian)

9. Pohle J., Thiel T. (2020) Digital sovereignty. *Internet Policy Review*. Vol. 9, Issue 4. DOI: https://doi.org/10.14763/2020.4.1532

10. Larsen B.C. (2022) The Geopolitics of AI and the Rise of Digital Sovereignty. *Brookings.* Available at: https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

11. Tsyfrovyi suverenitet Ukrainy: yak my ryzykuiemo staty tsyfrovoiu kolonieiu [Digital sovereignty of Ukraine: how we risk becoming a digital colony]. *Dev.ua*. 2025. Available at: https://dev.ua/news/gigacloud-one-1751973165 (in Ukrainian)

12. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 04.02.1998 № 74/98-VR [On the National Informatization Program: Law of Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/74/98-вр (in Ukrainian)

13. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy "Pro Stratehiiu kiberbezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 26.08.2021 № 447/2021 [On the Cybersecurity Strategy of Ukraine: Decree of the President]. Available at: https://www.president.gov.ua/documents/4472021-40013 (in Ukrainian)

14. Khabibrakhmanova T. (2024) Stratehiia, yakoi brakuie Ukraini: chomu tsyfrovyi suverenitet maie staty derzhavnym priorytetom [The strategy Ukraine lacks: why digital sovereignty should become a state priority]. *LIHA.Blohy.* Available at: https://blog.liga.net/user/tkhabibrakhmanova/article/58460 (in Ukrainian)

15. Zvit Rakhunkovoi palaty № 33-1/2025 [Report of the Accounting Chamber]. Available at: https://rp.gov.ua/upload-files/Activity/Collegium/2025/33-1_2025/Zvtit_33-1_2025.pdf (in Ukrainian)

16. Pro khmarni posluhy: Zakon Ukrainy vid 17.02.2022 № 2075-IX [On cloud services: Law of Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/2075-20 (in Ukrainian)

17. Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy (WINWIN): Rozporiadzhennia KMU vid 31.12.2024 № 1351-r [On approval of the WINWIN Strategy: CMU Order]. Available at: https://zakon.rada.gov.ua/laws/show/1351-2024-p (in Ukrainian)

18. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII [On the basic principles of cybersecurity of Ukraine: Law of Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (in Ukrainian)

19. Pro krytychnu infrastrukturu: Zakon Ukrainy vid 16.11.2021 № 1882-IX [On critical infrastructure: Law of Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/1882-20 (in Ukrainian)

20. Monitorynh Prohramy SIGMA: Derzhavne upravlinnia v Ukraini [SIGMA Programme Monitoring Report: Public Administration in Ukraine]. 2023. Available at: https://mof.gov.ua/storage/files/Звіт_Програми_SIGMA_(укр).pdf (in Ukrainian)

УДК 351:004.056.5(477)
JEL H11, K24, O33

Казанська Олена Олександрівна, кандидат наук з державного управління, доцент, доцент кафедри маркетингу, Національний університет «Київський авіаційний університет». **Хороших Вікторія Валеріївна,** кандидат наук з державного управління, доцент, доцент кафедри маркетингу, Національний університет «Київський авіаційний університет». **Аракелова Інна Олександрівна,** кандидат економічних наук, доцент, доцент кафедри маркетингу та туризму, Маріупольський державний університет. **Публічно-управлінські механізми забезпечення цифрового суверенітету держави в умовах воєнного стану.**

У статті досліджено публічно-управлінські механізми забезпечення цифрового суверенітету держави в умовах воєнного стану на прикладі України. Обґрунтовано авторське визначення цифрового суверенітету як здатності держави через систему публічно-управлінських механізмів забезпечувати контроль над влас-

ною цифровою інфраструктурою, інформаційними потоками та технологічним середовищем, зберігаючи інституційну спроможність до самостійних управлінських рішень у цифровій сфері. Виявлено чотири ключові виклики цифровому суверенітету України в умовах воєнного стану: масштабні кібератаки на критичну інфраструктуру, технологічна залежність від іноземних хмарних провайдерів, інституційна невизначеність функцій між Мінцифри, Держспецзв'язку та РНБО, а також недосконаліть нормативно-правової бази. Запропоновано авторську комплексну модель публічно-управлінських механізмів, що охоплює чотири взаємопов'язані складові – інституційний, правовий, організаційний та міжнародний механізми – об'єднані стратегічною координацією РНБО. Встановлено, що ефективність кожного механізму визначається узгодженістю з іншими елементами системи. Визначено перспективні напрями вдосконалення публічного управління цифровим суверенітетом, зокрема законодавче закріплення резидентства даних та формування єдиного координаційного органу у цій сфері.

Ключові слова: цифровий суверенітет, публічне управління, механізми публічного управління, воєнний стан, кібербезпека, цифрова інфраструктура, національна безпека.

UDK 351:004.056.5(477)
JEL H11, K24, O33

Olena Kazanska, PhD in Public Administration, Associate Professor, Associate Professor of the Department of Marketing, National University "Kyiv Aviation University". **Viktoriia Khoroshykh,** PhD in Public Administration, Associate Professor, Associate Professor of the Department of Marketing, National University "Kyiv Aviation University". **Inna Arakelova,** PhD in Economics, Associate Professor, Associate Professor of the Department of Marketing and Tourism, Mariupol State University. **Public administration mechanisms for ensuring the digital sovereignty of the state under martial law.**

The article examines the public administration mechanisms for ensuring the digital sovereignty of the state under martial law, using Ukraine as a case study. The relevance of the study is determined by the fact that digital sovereignty in wartime conditions is not merely a technical or legal category, but a fundamental prerequisite for the institutional survival of the state. Ukraine's experience during 2022–2025 demonstrated that the ability of public authorities to function amid large-scale cyberattacks, destruction of physical infrastructure, and occupation of territories has become a matter of preserving statehood itself. The authors substantiate an original definition of digital sovereignty as the state's ability, through a system of public administration mechanisms, to maintain control over its own digital infrastructure, information flows, and technological environment, while preserving institutional capacity for independent management decisions in the digital sphere. This definition, unlike existing approaches, emphasizes the managerial dimension of sovereignty rather than its technical or legal aspects. The article also draws a clear distinction between digital sovereignty and related concepts such as information sovereignty and cybersecurity, establishing digital sovereignty as a broader category that encompasses both. Four key challenges to Ukraine's digital sovereignty under martial law are identified: large-scale cyberattacks on critical infrastructure, technological dependence on foreign cloud providers – whose share of the Ukrainian market reaches approximately 75% - institutional ambiguity of functions between the Ministry of Digital Transformation, the State Service of Special Communications, and the National Security and Defence Council, as well as significant gaps in the regulatory framework, including the absence of a legal definition of data residency. A comprehensive model of public administration mechanisms is proposed, encompassing four interrelated components – institutional, legal, organizational, and international mechanisms – unified by the strategic coordination of the National Security and Defence Council. The institutional mechanism establishes a three-tier hierarchy of subjects: strategic, operational, and technical levels. The organizational mechanism incorporates wartime-specific instruments such as cloud data evacuation, the IT Army, and the cyber reserve. The international mechanism is characterized as dual in nature, simultaneously strengthening the state's technological capacity and deepening its dependence on foreign platforms. It is established that the effectiveness of each mechanism depends on its coherence with other elements of the system, and that the absence of such coherence represents the core problem of public administration of digital sovereignty in Ukraine. Promising directions for further research include developing evaluation criteria for the proposed mechanisms, the legislative definition of data residency, and the establishment of a unified coordination body in the field of digital sovereignty.

Key words: digital sovereignty, public administration, public administration mechanisms, martial law, cybersecurity, digital infrastructure, national security.