

DOI 10.34132/mspc2025.01.13.41

Марія Тимченко

ЦИФРОВА СТІЙКІСТЬ ДЕРЖАВИ У ПЕРІОД ВІЙНИ: РОЛЬ ПЛАТФОРМИ ДІЯ У ЗАБЕЗПЕЧЕННІ БЕЗПЕРЕРВНОСТІ ПУБЛІЧНИХ ПОСЛУГ

Матеріали представляють теоретичний аналіз особливостей публічного управління в умовах війни. Окреслено необхідність формування та реалізації цифрової стійкості держави за умов війни. Виявлено потреби створення цифрових платформ для забезпечення безперервності публічних послуг. Проаналізовано особливості впровадження платформи Дія в умовах війни.

Ключові слова: цифровізація, цифрова стійкість, публічні послуги, платформа Дія, безперервність.

В умовах воєнного стану в Україні створення платформ розвитку інфраструктури є важливим кроком до сприяння економічній стабільності та розвитку країни. Технології допомагають краще використовувати національні ресурси, створювати нові сектори економіки, зміцнювати національний потенціал та будувати національну економіку. Уряд відіграє одну з ключових ролей під час кризи, оскільки саме уряд повинен забезпечити надання основних послуг та широкого спектру державних послуг для підтримки стабільності. Впровадження публічного управління у період дії воєнного стану є унікальним тим, що воно вимагає швидкого реагування, вирішення конфліктів та координації різних гілок влади. Використання воєнного стану в контексті правової бази для зміцнення безпеки та підтримки національної безпеки є серйозним викликом легітимності та ефективності уряду.

Країни, що постраждали від конфліктів, стикаються зі значними проблемами управління. До них належать порушення роботи комунікаційних мереж, зміни в політичному середовищі, економічна невизначеність та необхідність швидко приймати рішення в часи невизначеності. Деякі з ключових функцій уряду під час кризових ситуацій – це управління державними ресурсами, координація безпеки, забезпечення зв'язку між державними органами та підтримка державних послуг.

Увага науковців часто спрямована на вивчення показників належного державного управління в умовах воєнного стану. Дослідники (В. Борщевський, О. Василюк, С. Єгоричева, М. Їжа, Л. Курносенко, Є. Матвеев, А. Мисишин, М. Лахижа, Дж. Немек та ін.) вивчають механізми адаптації до криз в публічному управлінні в умовах воєнного стану.

Цифрова стійкість – це здатність організації чи уряду виконувати критично важливі функції, відновлюватися та адаптуватися до нових можливостей під час та після кіберпорушень. Це визначення відображає комплексний підхід, що включає кібербезпеку, управління ризиками ІКТ та забезпечення безперервності публічних процесів [4].

Рівні цифрової безпеки включають такі структурні елементи як: законодавство, інституції, політики; технічні елементи серед яких: мережі, платформи державних послуг, системи моніторингу; та соціальні елементи: підвищення обізнаності, навчання персоналу, взаємодія зі суспільством. З метою забезпечення цифрової стійкості держави в умовах сучасних викликів важливим орієнтиром виступають міжнародні рамки та стандарти, що визначають підходи до захисту критичної цифрової інфраструктури, управління ризиками та забезпечення безперервності публічних послуг (табл. 1).

Державне регулювання використання цифрових технологій та правова основа регулювання цифрових технологій є критично важливим для утвердження верховенства права у кризових умовах.

Таблиця 1.

Основні міжнародні рамки та стандарти

Організація	Рамка / Документ	Ключовий внесок	Рік
OECD	Digital Government Policy Framework (DGPF) [7]	Шість вимірів: стратегія, організація, сервіс, технології, дані, безпечність	2020
ЄС	NIS2 Directive; Digital Operational Resilience Act (DORA) [5]	Підвищення стійкості ІКТ-інфраструктури та фінсектору; кіберсертифікація	2022-2025
NATO	Resilience Reference Curriculum NATO [9]	Освітні модулі та вініетки, whole-of-government/society	2025
ООН / ITU	Global Cyber security Index	Оцінка спроможностей країн у кібербезпеці; рекомендації	2021
CERRE	Digital Supply Chains Resilience CERRE [10]	Моніторинг резильєнтності в цифрових ланцюгах постачання; міжнародна координація	2024

Органи публічного управління повинні забезпечити, щоб довіра до електронних послуг і цифрової інфраструктури була ключовим елементом взаємодії між громадянами та урядом, а також підтримкою реформи управління й ефективного надання державних послуг [3]. Платформа Дія [1] в Україні відіграє важливу роль у забезпеченні стабільності, оптимізації та сталого відновлення держави, використання та розповсюдження електронних систем для співпраці між установами та громадськістю.

Платформа Дія забезпечує:

- надійність та високу доступність через хмарну архітектуру та мультизонне резервування даних;
- безперервність послуг завдяки автоматизованим механізмам масштабування;
- захист від кіберзагроз шляхом багаторівневої автентифікації, шифрування та проведення пентестів;
- управління кризовими ситуаціями з використанням стійких бекапів і планів DRP;
- прозорість та гнучкість через відкритий код окремих компонентів і щомісячні звіти з SLI/SLO.

Платформа Дія – це хмарне рішення, яке дозволяє розподіляти робочі навантаження між кількома центрами обробки даних та аварійним відновленням. Авторизація в «Дії» здійснюється через BankID і MobileID із двофакторною перевіркою, за рахунок чого знижується ризик несанкціонованого доступу. Усі дані користувача шифруються як під час передачі TLS, так і в ключі клієнта AES-256. Крім того, проводиться постійний моніторинг «чутливих» мереж для виявлення шкідливої активності [6].

З 2021 року Міністерство цифрової трансформації України проводить зовнішні та внутрішні навчання, а також навчання «RedTeam» для вирішення складних ситуацій. «RedTeam» – це група експертів з кібербезпеки, які моделюють реальні ворожі атаки на інформаційні системи організації або держави, щоб виявити вразливості, оцінити ефективність оборонних заходів і навчити «BlueTeam» (команду захисту) оперативному реагуванню. На відміну від класичного пентесту, який має вузьке технічне завдання та обмежений час, «RedTeam» операції часто тривають тижні чи місяці й включають безперервні, цілеспрямовані багатоетапні атаки з мінімальними обмеженнями з боку замовника [8].

Під час дії воєнного стану платформа Дія стала ключем до зміцнення управління, трансформації відносин між державою і громадянами, побудови довіри та підвищення якості, прозорості та підзвітності державних послуг. З початку повномасштабного вторгнення у застосунок Дія з'явилися нові документи та послуги, серед них: електронне пенсійне посвідчення, посвідка на проживання, документи англійською мовою, а також сервіс шерингу автомобіля.

Міністерство цифрової трансформації наголошує, що виклики, з якими стикаються громадяни, спричинені воєнними діями, не є перешкодою для реалізації стратегії цифрової трансформації. Екосистема Дія ефективно використовується як інструмент для створення ефективної інфраструктурної системи, що допомагає зменшити бюрократію без шкоди для якості державних послуг. Розробка цієї платформи спрямована на надання документів та послуг, що відповідають потребам сучасних користувачів [2].

Таким чином, зважаючи на збройну агресію проти України, питання цифрової стабільності стало актуальним, адже задля добре продуманої економічної системи та для забезпечення безперервного надання державних послуг, збереження національної єдності громадян важливо підтримувати взаємозв'язки між державою і громадянами за допомогою сучасних технологій надання публічних послуг. У цьому контексті платформа Дія є важливою як інструмент для доступу громадян до державних послуг, цифрових документів та соціальних послуг. Успіх Дії під час воєнного стану відображається у високому рівні адаптивності цифрового урядування в Україні, сприяє зростанню довіри до державних інституцій і зміцненню цифрової стійкості національного масштабу.

Покращення якості цифрової інфраструктури відповідно до потреб громадян має велике значення для зміцнення верховенства права, розвитку ефективної цифрової держави, здатної функціонувати в умовах надзвичайних викликів.

References

1. Diia [Diia]. (n.d.). *diia.gov.ua*. Retrieved from: <https://diia.gov.ua/> [in Ukrainian].
2. Tymchenko, M.S. (2022). Tsyfrova transformatsiia publicnogo upravlinnia v Ukraini [Digital transformation of public administration in Ukraine]. *Extended abstract of master's thesis*. Mykolaiv: ChNU im. Petra Mohyly [in Ukrainian].
3. Chalabiiieva, M.R. (2024). Adaptatsiia pravovoho rehuliuвання administratyvnoi reformy v umovakh voiennoho stanu: konstytutsiini aspekty tsyfrovizatsii publicnogo upravlinnia [Adaptation of legal regulation of administrative reform in conditions of martial law: constitutional aspects of digitalization of public administration]. Proceedings from RFSRCML '24: IV Mizhnarodna naukovopraktychna internet-konferentsiia z nahody vidznachennia Dnia nauky-2024 v Ukraini «Aktualnist ta osoblyvosti naukovykh doslidzhen v umovakh voiennoho stanu» – IV International scientific and practical internet conference on the occasion of Science Day 2024 in Ukraine «Relevance and peculiarities of scientific research in martial law». (pp. 234-238). Kyiv: DNDI MVS Ukrainy [in Ukrainian].
4. Bevin, L. (2024). What Is Digital Resilience? *www.zengrc.com*. Retrieved from: <https://www.zengrc.com/blog/what-is-digital-resilience/> [in English].
5. Shaping Europe's digital future. (n.d.). (2025). *digital-strategy.ec.europa.eu*. Retrieved from: <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies> [in English].
6. Digital technologies and the resilience of Ukraine's social protection system: wartime experience. (n.d.). (2024). *www.researchgate.net*. Retrieved from: <https://surl.li/xhdqbk> [in English].
7. The OECD DigitalGovernmentPolicyFramework: Sixdimensionsof a DigitalGovernment (n.d.). (2020). *www.oecd.org*. Retrieved from: <https://surl.lu/zesjwp> [in English].
8. Redteaming. (n.d.). (2023). *www.techtargget.com*. Retrieved from: <https://surl.lu/nqizch> [in English].
9. *Resilience Reference Curriculum*. (n.d.). (2025). Brussels: NATO Headquarters [in English].
10. Timmers, P. (2024). *Resilience in Digital Supply Chains: Opportunities for Global and International Governance*. Brussels: Centreon Regulation in Europe (CERRE) [in English].

DOI 10.34132/mspc2025.01.13.41

Maria Tymchenko

DIGITAL SUSTAINABILITY OF THE STATE DURING WAR: THE ROLE OF THE DIIA PLATFORM IN ENSURING THE CONTINUITY OF PUBLIC SERVICES

The materials presents a theoretical analysis of the features of public administration in wartime. The need to form and implement the digital sustainability of the state during wartime is outlined. The needs for creating digital platforms to ensure the continuity of public services are identified. The features of implementing the DYIA platform in wartime are analyzed.

Keywords: digitalization, digital sustainability, public services, DIIA platform, continuity.

Відомості про автора / Information about the Author

Марія Тимченко, аспірантка Навчально-наукового інституту публічного управління та адміністрування Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: mariatymchenko99@gmail.com, orcid: <https://orcid.org/0009-0007-6503-2029>.

Maria Tymchenko, PhD-student of the Educational and Scientific Institute of Public Management and Administration of the Black Sea National University named after Peter Mohyla, Mykolaiv, Ukraine. E-mail: mariatymchenko99@gmail.com, orcid: <https://orcid.org/0009-0007-6503-2029>.