ЕВОЛЮЦІЙНА ТРАНСФОРМАЦІЯ ПРОЦЕСІВ ЦИФРОВІЗАЦІЇ ЯК ІНСТРУМЕНТУ ЦИВІЛЬНОГО ЗАХИСТУ[1]

EVOLUTIONARY TRANSFORMATION OF DIGITALIZATION PROCESSES AS AN INSTRUMENT OF CIVIL PROTECTION

У статті здійснено аналіз фундаментальної трансформації процесів цифровізації в Україні, спричиненої повномасштабним вторгненням 2022-го року. Досліджується зсув від сервіс-орієнтованої моделі «держави у смартфоні», що фокусувалася на зручності та антикорупційному ефекті, до безпекової моделі, де цифрові інструменти стали невід'ємною частиною системи цивільного захисту. На прикладах еволюції екосистеми «Дія» та створення спеціалізованих інструментів, як-от «єВорог», «єППО» та «єВідновлення», проаналізовано процес інтеграції цифрових технологій у завдання оповіщення, контррозвідки, протиповітряної оборони та ліквідації наслідків. Обґрунтовано тезу про те, що зазначена трансформація призвела до суб'єктивізації громадян, перетворивши їх із об'єктів захисту на активних учасників національної оборони, та сформувала нову, унікальну модель цифрової стійкості держави.
Ключові слова: *цифровізація, цивільний захист, воєнний стан, Дія, держава у смартфоні, цифрова стійкість, трансформація, управління в кризових умовах.*

The article analyzes the fundamental transformation of digitalization processes in Ukraine caused by the full-scale invasion of 2022. It examines the shift from a service-oriented "state in a smartphone" model, which focused on convenience and anti-corruption effects, to a security-oriented model in which digital tools have become an integral part of the civil protection system. Using examples such as the evolution of the Diia ecosystem and the development of specialized tools including eVorog, ePPO, and eVidnovlennia, the study explores the integration of digital technologies into tasks of public alerting, counterintelligence, air-defense coordination, and recovery operations. The article substantiates the argument that this transformation has led to the subjectivization of citizens, turning them from passive objects of protection into active participants in national defense, and has shaped a new, unique model of the state's digital resilience.
Key words: *digitalization, civil protection, martial law, Diia, state in a smartphone, digital resilience, transformation, crisis management.*

УДК 004.9:351.86
DOI: https://doi.org/10.32782/dees.20-28

Щебетун Р.В.[2,3]
здобувач освітнього ступеня «бакалавр»,
Сумський державний університет

Shchebetun Ruslan
Sumy State University

Постановка проблеми. Україна увійшла у 2022-й рік одним зі світових лідерів у галузі державних цифрових інновацій. Це не було перебільшенням. Концепція «держави у смартфоні» перетворилася з амбітного політичного гасла на відчутну щоденну реальність для мільйонів. Флагманський проєкт «Дія» став справжнім помічником, акумулювавши високий рівень суспільної довіри. Він був не просто гаманцем для цифрових документів, а цілісною екосистемою, що дозволяла зареєструвати бізнес за десять хвилин, сплатити податки без черг, ідентифікувати особу чи підтвердити вакцинацію [1, 2]. «Дія» стала символом прозорості та демонтажу старої бюрократичної машини.

Паралельно з державним проєктом, приватний сектор та комунальні сервіси формували власні потужні екосистеми. Медична платформа «Helsi» привчила мільйони до електронних рецептів та онлайн-запису до лікаря. Вибуховий розвиток фінтеху, зокрема Monobank та оновлений Privat24, встановив світовий стандарт якості мобільного банкінгу. Ці процеси разом сформували унікальне середовище: високу цифрову грамотність населення [3] і, що найважливіше, масове звикання до якісних, миттєвих та зручних онлайн-сервісів.

Таким чином, до лютого 2022 року Україна володіла потужною цифровою інфраструктурою, захищеними реєстрами та величезним кредитом довіри громадян до цифрових інструментів. Проте вся ця складна система була спроєктована та оптимізована виключно для завдань мирного часу. Вона будувалася для комфорту, сервісу та економічного розвитку. У її архітектуру не закладалися ризики повномасштабної конвенційної війни.

24-те лютого 2022-го року стало моментом істини для цієї інфраструктури. За всіма прогнозами, вона мала б колапсувати першою. Але замість колапсу, відбулася радикальна трансформація. Система, створена для зручності, миттєво стала стратегічним активом для виживання держави.

Актуальність дослідження. Класична система цивільного захисту, яку успадкувала Україна, була продуктом іншої епохи [4, 5]. Вона оперувала поняттями фізичної інфраструктури: сирени, бомбосховища, плани евакуації, паперовий облік. Ця модель була розрахована на відносно локалізовані та прогнозовані надзвичайні ситуації.

Повномасштабне вторгнення миттєво оголило неадекватність такого підходу. Війна виявилася гібридною, тотальною та високотехнологічною. Найперше – вона вдарила по комунікаціях. Ворог

[1] Робота виконана в рамках НДР «Цифрові трансформації для забезпечення цивільного захисту та повоєнного відновлення економіки в умовах екологічних і соціальних викликів» (№ д/р 0124U000549)
[2] Науковий керівник: В.В. Койбічук, к.е.н., доцент, завідувач кафедри економічної кібернетики, Сумський державний університет, ORCID: https://orcid.org/0000-0002-3540-7922
[3] ORCID: https://orcid.org/0009-0003-2929-193X

цілеспрямовано бив по телевежах, намагаючись створити інформаційний вакуум, посіяти паніку та дезорієнтувати населення [6]. Забезпечення громадян стабільним і верифікованим каналом інформації раптом стало пріоритетним завданням цивільного захисту, до якого стара система не була готова.

Водночас кардинально змінився характер самої загрози, що вимагало нової системи оповіщення. Ворог почав застосовувати цілий арсенал озброєнь з різним часом підльоту: від балістичних ракет до повільних дронів-камікадзе. Загальна сирена «Увага всім!» втратила ефективність. Вона не давала розуміння рівня загрози, її напрямку чи орієнтовного часу, що швидко призводило до втоми від тривог [7]. Потрібна була диференційована, адресна та інформативна система, здатна донести сигнал до кожного.

Окрім цього, виникла гостра потреба в масовому та оперативному зборі розвідувальних даних з усіх регіонів країни, особливо з тимчасово окупованих територій. Традиційні методи агентурної розвідки не могли покрити такий обсяг запитів. Необхідно було створити безпечний та верифікований канал комунікації між мільйонами громадян та силами оборони [8].

Нарешті, масштаби руйнувань цивільної інфраструктури вимагали негайного рішення для фіксації збитків. Паперова бюрократія просто захлинулася б у мільйонах заяв. Був потрібен єдиний цифровий інструмент для швидкого, юридично значущого збору даних про пошкодження, який став би фундаментом для майбутнього відновлення [9]. Всі ці екзистенційні виклики і стали драйвером примусової, але надзвичайно швидкої цифрової трансформації.

Постановка завдання. Метою статті є поглиблений аналіз перетворення сервісної моделі цифровізації на життєво важливий компонент цивільного захисту та національної оборони.

Виклад основного матеріалу дослідження. Відповідь на нові виклики спиралася на ті два стовпи, що були збудовані в мирний час: величезну довіру до «Дії» та високу цифрову грамотність населення. «Дія», що вже була встановлена у переважної більшості громадян, з цифрового гаманця миттєво перетворилася на багатофункціональний інструмент виживання.

Найшвидше відреагували на інформаційну загрозу. Коли ворог вдарив по телевежах, у «Дії» за лічені дні з'явилися сервіси «Дія.Радіо» та «Дія.TV». Вони дали мільйонам людей доступ до новин навіть за умов слабкого мобільного інтернету, виконавши стратегічну функцію ЦЗ із забезпечення зв'язку [7]. Паралельно, критичну роль на себе взяли офіційні канали комунікації Повітряних Сил, ОВА та ДСНС. Вони стали новою, децентралізованою та надзвичайно оперативною системою оповіщення. Часто випереджаючи фізичні сирени, вони давали уточнення про характер загрози, дозволяючи людям ухвалювати більш адекватні рішення.

«Дія» також стала інструментом економічної мобілізації. Можливість купити військові облігації чи зробити донат через United24 дозволила кожному долучитися до фінансування оборони, посилюючи економічну стійкість держави.

Але справжньою революцією стала не стільки адаптація старих сервісів, скільки створення принципово нових інструментів, що залучили громадян безпосередньо до оборони. Найяскравіший приклад – чат-бот «єВорог». Його ключовою відмінністю від стихійних ботів стала верифікація через «Дію». Цей хід миттєво забезпечив високий рівень довіри до отриманих даних, відсікаючи ворожі ІПСО. Мільйони українців на окупованих та прифронтових територіях отримали безпечний канал для передачі розвідданих, ставши очима «народної розвідки» [8].

Ще глибшою інтеграцією став застосунок «єППО». Створений у тісній співпраці з військовими, він вирішував конкретну тактичну проблему – сліпі зони радарів, які не бачать цілі на низькій висоті на кшталт крилатих ракет чи дронів [10]. «єППО» перетворив смартфон кожного громадянина на потенційний сенсор. Побачивши ціль, людина кількома натисканнями передавала її тип та геолокацію безпосередньо на командні пункти ППО, допомагаючи замкнути цикл ураження. Це унікальний у світі приклад прямої інтеграції цивільного застосунку у військову систему.

Паралельно, сервіс «єВідновлення» взяв на себе колосальне завдання менеджменту катастроф [9]. Дозволивши громадянам зафіксувати руйнування у декілька кліків, він сформував єдину верифіковану базу даних збитків. Це не лише запустило механізм компенсацій, але й дало державі та партнерам дашборд реальних масштабів трагедії для стратегічного планування відбудови.

Наочною кількісною ілюстрацією цих масштабів є дані звіту четвертої Швидкої оцінки завданої шкоди та потреб на відновлення [11], підготовленого Урядом України, Світовим банком, ООН та ЄС. Згідно з ним (табл. 1), загальні потреби на відбудову вже сягають 523,6 млрд доларів США. Аналіз у розрізі секторів чітко підсвічує ті сфери, де цифрові інструменти стали відповіддю на виклики. Найбільших збитків зазнав пункт «Житло» з 57,6 млрд дол. шкоди та 83,7 млрд потреб, що безпосередньо валідує необхідність такого інструменту, як «єВідновлення». Окрім цього, значних ударів завдано по «Енергетиці», зокрема 20,5 млрд. дол. шкоди. Показово, що звіт RDNA4 окремо виділяє потреби на відновлення пукнту «Телекомунікації, цифрові технології та

Таблиця 1

Шкода, збитки та потреби в RDNA4 в розрізі пунктів (млрд дол. США)

Сектор	Шкода	Збитки	Потреби
Соціальний сектор			
Житло	57,6	21,1	83,7
Освіта і наука	13,4	3,9	19,8
Охорона здоров'я	10,6	9,9	19,5
Соціальний захист та засоби до існування	1,5	11,6	14,9
Культура і туризм	4,1	1,9	7,0
Інфраструктурний сектор			
Енергетика та видобувні галузі	20,5	72,3	67,8
Транспорт	40,7	127,4	96,3
Телекомунікації, цифрові технології та медіа	3,6	14,7	12,8
Водопостачання та водовідведення	2,9	8,8	6,8
Муніципальні послуги	2,9	6,0	4,8
Виробничий сектор			
Сільське господарство	11,2	7,2	56,5
Торгівля та промисловість	3,5	91,7	102,9
Зрошення та водні ресурси	0,7	2,3	1,9
Фінанси та банківська діяльність	0,3	1,0	0,9
Наскрізні сектори			
Довкілля, управління природними ресурсами та лісове господарство	1,7	0,9	2,4
Реагування на надзвичайні ситуації та цивільний захист	0,6	2,5	1,8
Правосуддя та державне управління	0,4	0,3	0,9
Управління вибухонебезпечними предметами	0,4	4,2	4,0
Всього	176,1	588,8	523,6

Джерело: побудовано автором на основі [11]

медіа» та безпосередньо «Реагування на надзвичайні ситуації та цивільний захист». Таким чином, цифровізація вимушено перетворилася з сервісної функції на критично важливий інструмент менеджменту катастроф, що оперує збитками у сотні мільярдів доларів.

Загалом зміни набагато глибші, ніж просто технологічне оновлення. Вони мають у собі вагомий соціально-політичний вимір. По суті, ми стали свідками перетворення громадянина з об'єкта на суб'єкта цивільного захисту.

Класична модель цивільного захисту [5] за своєю природою є патерналістською: держава виступає як суб'єкт, що володіє інформацією та ресурсами, а громадянин – як пасивний об'єкт захисту. Завдання останнього – слухати команди, чути сирену та йти в укриття. А цифрові інструменти воєнного часу докорінно зламали цю динаміку. Громадянин не просто отримує захист, натомість він бере активну участь у його створенні [3], стаючи сенсором для розвідки й елементом мережі протиповітряної оборони.

Це має відчутний психологічний вплив. Замість паніки та відчуття безпорадності, людина отримує інструмент та відчуття причетності до спільної боротьби. Це критично важливо для підтримки морального духу суспільства у тривалій війні на виснаження.

Окрім цього, ми бачимо формування нової архітектури цифрової стійкості. Надійність системи оповіщення тепер забезпечується не міцністю однієї фізичної сирени, а децентралізованою та надлишковою мережею мільйонів смартфонів, десятків моніторингових каналів та державних застосунків. Знищити таку систему фізично не можливо. Вона гнучка, миттєва і надає диференційовану інформацію, що дозволяє людям адаптувати свою поведінку і, зрештою, рятує життя.

Варто відзначити й унікальну модель гнучкого управління в державних інституціях під час кризи [6]. Швидкість, із якою розроблялися та впроваджувалися ці інструменти, стала можливою лише завдяки горизонтальній співпраці між профільними міністерствами, Генштабом та волонтерськими ІТ-спільнотами. Це вимагало миттєвих рішень: як технологічних, так і правових. Наприклад, запуск «єВідновлення» йшов паралельно з ухваленням пакету законів та постанов Кабміну, що легітимізували цей процес [9]. Ця синергія та гнучкість, коли бюрократія поступилася місцем ефективності, є окремим феноменом українського державного управління.

Висновки. Повномасштабне вторгнення стало жорстоким каталізатором для еволюції, яку ніхто не планував. Українська цифровізація була змушена здійснити миттєвий стрибок від економіки зручності до економіки виживання. Інфраструктура мирного часу, створена для комфорту та боротьби з корупцією, несподівано виявилася наріжним каменем стійкості та фундаментом для «цифрової фортеці».

Український досвід унікальний у світовій історії. Він вперше продемонстрував, як масові державні сервіси можуть бути не просто адаптовані, а глибоко інтегровані в систему цивільного захисту та навіть у безпосередні військові операції. Ця трансформація змінила філософію ЦЗ, перетворивши мільйони пасивних об'єктів захисту на активних суб'єктів національної оборони.

Досвід України доводить, що у 21-му столітті національна безпека нерозривно пов'язана з цифровою інфраструктурою, рівнем цифрової грамотності населення та інституційною гнучкістю держави. Україна де-факто пише новий світовий посібник із цифрового цивільного захисту. І в цьому посібнику стійкість – це не лише міцність бетону в укриттях, але й гнучкість коду, швидкість зв'язку та непохитна довіра громадян до своєї цифрової держави.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Ковтун О. А. «Держава у смартфоні» як нова модель взаємодії органів державної влади та громадян. *Сучасний менеджмент: моделі, стратегії, технології* : зб. тез XXIII Всеукр. наук.-практ. конф. (Одеса, 08–09 грудня 2022 р.). Одеса : Держ. ун-т «Одеська політехніка», 2022. С. 24–25. URL: https://surl.lt/pvotau

2. Холод Є. О. Цифровізація як основа розбудови інноваційної держави. *Інноваційні технології в розвитку сучасного суспільства* : матеріали III Всеукр. наук.-практ. інтернет-конф. (Суми, 17–18 травня 2023 р.). Суми : СумДУ, 2023. С. 177–179. URL: https://surl.lu/croywp

3. Ковальчук В. Б., Кривенко Ю. В. Адміністративно-правові засади відшкодування шкоди, завданої внаслідок збройної агресії РФ. *Юридична наука та практика в умовах воєнного стану* : матеріали III Всеукр. наук.-практ. конф. (Одеса, 26 травня 2023 р.). Одеса : НУ «ОЮА», 2023. С. 303–306. URL: https://surl.li/wjdqza

4. Овчарук В. П. Система цивільного захисту України та її складові. *Проблеми цивільного захисту населення та територій від надзвичайних ситуацій* : матеріали наук.-практ. конф. (Харків, 23–24 травня 2024 р.). Харків : НУЦЗУ, 2024. С. 366–368. URL: https://surl.li/bnftxo

5. Трансформація публічного управління цивільним захистом в умовах євроінтеграційних процесів: зарубіжний досвід і вітчизняна практика: монографія / за заг. ред. В. Д. Бабка. Харків : НУЦЗУ, 2024. 219 с. URL: https://surl.li/wxtzqd

6. Мельник О. В. Забезпечення інформаційної безпеки України в умовах воєнного стану: правовий аспект. *Правові та інституційні механізми забезпечення розвитку держави та права в умовах євроінтеграції* : зб. матеріалів VI Міжнар. наук.-практ. конф. (Одеса, 20 травня 2022 р.). Одеса : НУ «ОЮА», 2022. Вип. 6. С. 110–112. URL: https://surl.li/cjeclj

7. Новікова О. Ф., Азьмук Н. А. Цифровізація – чинник посилення резильєнтності соціально-трудової сфери та повоєнного відновлення України. *Економіка та суспільство.* 2023. № 53. DOI: https://doi.org/10.32782/2524-0072/2023-53-27

8. Маначинський О. Я., Оксюк П. Б., Федоров Є. В. Цифрові технології в системі національної безпеки. *Академічне бачення*. 2024. Вип. 21. URL: https://surl.li/kdyfbt

9. Клименко Н. В. Цифрова грамотність населення як ключовий фактор розвитку цифрової економіки України. *Економічні інновації*. 2018. Вип. 20, № 4(69). С. 104–112. URL: https://surl.lu/uambjm

10. Подобєд І. Цифровізація як сучасний тренд трансформації ресурсного механізму системи цивільного захисту. *Науковий вісник: Державне управління.* 2024. № 1 (15). С. 82–103. DOI: https://doi.org/10.33269/2618-0065-2024-1(15)-82-103

11. Україна: Четверта Швидка оцінка завданої шкоди та потреб на відновлення (RDNA4): Лютий 2022 – Грудень 2024. Уряд України, Група Світового банку, Європейська Комісія, Організація Об'єднаних Націй. 2025. 196 с. URL: https://surl.lt/rkdadt

REFERENCES:

1. Kovtun O. A. (2022). «Derzhava u smartfoni» yak nova model vzaiemodii orhaniv derzhavnoi vlady ta hromadian ["State in a smartphone" as a new model of interaction between state authorities and citizens]. *Suchasnyi menedzhment: modeli, stratehii, tekhnolohii:* zb. tez XXIII Vseukr. nauk.-prakt. konf. (Odesa, 08–09 December 2022 r.). Odesa : Derzh. un-t "Odeska politekhnika", pp. 24–25. Available at: https://surl.lt/pvotau

2. Kholod Ye. O. (2023). Tsyfrovizatsiia yak osnova rozbudovy innovatsiinoi derzhavy [Digitalization as the basis for building an innovative state]. *Innovatsiini tekhnolohii v rozvytku suchasnoho suspilstva* : materialy III Vseukr. nauk.-prakt. internet-konf. (Sumy, 17–18 May 2023 r.). Sumy : SumDU, pp. 177–179. Available at: https://surl.lu/croywp

3. Kovalchuk V. B., Kryvenko Yu. V. (2023). Administratyvno-pravovi zasady vidshkoduvannia shkody, zavdanoi vnaslidok zbroinoi ahresii RF [Administrative and legal principles of compensation for damage caused as a result of the armed aggression of the Russian Federation]. *Yurydychna nauka ta praktyka v umovakh voiennoho stanu* : materialy III Vseukr. nauk.-prakt. konf. (Odesa, 26 May 2023 r.). Odesa : NU "OIuA", pp. 303–306. Available at: https://surl.li/wjdqza

4. Ovcharuk V. P. (2024). Systema tsyvilnoho zakhystu Ukrainy ta yii skladovi [The Civil Protection System of Ukraine and its Components]. *Problemy tsyvilnoho zakhystu naselennia ta terytorii vid*

nadzvychainykh sytuatsii: materialy nauk.-prakt. konf. (Kharkiv, 23–24 May 2024 r.). Kharkiv : NUTsZU, pp. 366–368. Available at: https://surl.li/bnftxo

5. Transformatsiia publichnoho upravlinnia tsyvilnym zakhystom v umovakh yevrointehratsiinykh protsesiv: zarubizhnyi dosvid i vitchyzniana praktyka: monohrafiia [Transformation of Public Civil Protection Management in the Conditions of European Integration Processes: Foreign Experience and Domestic Practice: Monograph] / za zah. red. V. D. Babka. Kharkiv : NUTsZU, p. 219. Available at: https://surl.li/wxtzqd

6. Melnyk O. V. (2022). Zabezpechennia informatsiinoi bezpeky Ukrainy v umovakh voiennoho stanu: pravovyi aspect [Ensuring Information Security of Ukraine in Conditions of Martial Law: Legal Aspect]. *Pravovi ta instytutsiini mekhanizmy zabezpechennia rozvytku derzhavy ta prava v umovakh yevrointehratsii*: zb. materialiv VI Mizhnar. nauk.-prakt. konf. (Odesa, 20 May 2022 r.). Odesa : NU "OIuA", vol. 6, pp. 110–112. Available at: https://surl.li/cjeclj

7. Novikova O. F., Azmuk N. A. (2023). Tsyfrovizatsiia – chynnyk posylennia rezylientnosti sotsialno-trudovoi sfery ta povoiennoho vidnovlennia Ukrainy [Digitalization is a Factor in Strengthening the Resilience of the Social and Labor Sphere and Post-War Recovery of Ukraine]. *Ekonomika ta suspilstvo*, no. 53. DOI: https://doi.org/10.32782/2524-0072/2023-53-27

8. Manachynskyi O. Ya., Oksiuk P. B., Fedorov Ye. V. (2024). Tsyfrovi tekhnolohii v systemi natsionalnoi bezpeky [Digital technologies in the national security system]. *Akademichne bachennia*, vol. 21. Available at: https://surl.li/kdyfbt

9. Klymenko N. V. (2018). Tsyfrova hramotnist naselennia yak kliuchovyi faktor rozvytku tsyfrovoi ekonomiky Ukrainy [Digital literacy of the population as a key factor in the development of the digital economy of Ukraine]. *Ekonomichni innovatsii*, vol. 20, no. 4(69), pp. 104–112. Available at: https://surl.lu/uambjm

10. Podobied I. (2024). Tsyfrovizatsiia yak suchasnyi trend transformatsii resursnoho mekhanizmu systemy tsyvilnoho zakhystu [Digitalization as a modern trend in the transformation of the resource mechanism of the civil protection system]. *Naukovyi visnyk: Derzhavne upravlinnia*, no. 1 (15), pp. 82–103. DOI: https://doi.org/10.33269/2618-0065-2024-1(15)-82-103

11. Ukraina: Chetverta Shvydka otsinka zavdanoi shkody ta potreb na vidnovlennia (RDNA4): Liutyi 2022 – Hruden 2024. Uriad Ukrainy, Hrupa Svitovoho banku, Yevropeiska Komisiia, Orhanizatsiia Obiednanykh Natsii [Ukraine: Fourth Rapid Assessment of Damage and Recovery Needs (RDNA4): February 2022 – December 2024. Government of Ukraine, World Bank Group, European Commission, United Nations], p. 196. Available at: https://surl.lt/rkdadt