

DOI: 10.52363/2414-5866-2022-2-37

УДК 352 (477): 322

*Примуш Р.Б., к.держ.упр., м. Київ,  
ORCID: 0000-0002-2408-6780*

*Primush R., PhD in Public Administration, Kyiv*

## **РОЛЬ ЦИФРОВІЗАЦІЇ В СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ ТА ЦИВІЛЬНОЇ БЕЗПЕКИ В УКРАЇНІ**

### **THE ROLE OF DIGITALIZATION IN THE SYSTEM OF PUBLIC ADMINISTRATION IN THE SPHERE OF NATIONAL AND CIVIL SECURITY IN UKRAINE**

*У статті визначено місце та роль цифровізації під час функціонування системи публічного управління у сфері національної безпеки України. Окреслено напрямки використання засобів цифровізації в системі публічного управління національної безпеки в Україні. Серед цих напрямків перспективну роль відведено публічно-приватному партнерству. Досліджено публічно-управлінську практику інституційної взаємодії в цій сфері. Акцентовано на впливі на неї позасистемних факторів, які доречно моніторити й оцінювати за допомогою засобів цифровізації.*

**Ключові слова:** *публічне управління, механізми, національна безпека, фактори, цифровізація.*

*The article defines the place and role of digitization during the functioning of the public administration system in the sphere of national security of Ukraine. Directions for using digitization tools in the system of public management of national security in Ukraine are outlined. Among these directions, a promising role is assigned to public-private partnership. The public-management practice of institutional interaction in this area has been studied. Emphasis is placed on the influence of non-systemic factors on it, which should be monitored and evaluated with the help of digitalization tools.*

**Keywords:** *state administration, mechanisms, national security, factors, digitization.*

**Постановка проблеми.** Аналіз Стратегії у сфері національної безпеки України «Безпека людини – безпека країни» [4] дає підстави стверджувати, що цифровізація віднесена до спектру дії саме інформаційної безпеки. Свідченням цього є те, що серед завдань у сфері нацбезпеки визначено гарантування інформаційної безпеки, але не має вказівки на результативне використання ІКТ та інших новаційних інструментів у зазначеній сфері [там само]. Власне кажучи, цифровізація є вже вимогою не тільки часу, а й суспільства, особливо в аспектах, що стосуються забезпечення нормальної життєдіяльності суспільства та системи безпеки. Крім того, усе більше відбувається зміщення акцентів і пріоритетів щодо підтримки національної безпеки, у т.ч. у бік забезпечення впровадження принципу публічності на всіх рівнях публічного управління. Зважаючи на це, потребує окремого науково обґрунтованого розгляду роль цифровізації у сфері нацбезпеки та механізмів публічного управління у цій сфері.

**Аналіз останніх досліджень і публікацій.** Різні аспекти публічного управління у сфері національної безпеки є предметом наукового дослідження вітчизняних і закондонних учених В. Бакуменка, С. Белая, О. Бондаренка, С. Домбровської, О. Євсюкова, С. Крука, О. Крюкова, С. Майстра, Н. Нижник, С. Полторака, А. Помази-Пономаренко, В. Садкового, Г. Ситника, В. Стрельцова та ін. [3; 5; 6; 7; 9]. Разом із тим потребують окремого наукового розгляду тенденції у сфері національної безпеки, які формуються з урахуванням цифровізації. Ці тенденції зумовлюють удосконалення правової бази, що, у свою чергу, потребує ґрунтовного наукового аналізу.

**Постановка завдання.** Мета дослідження – визначити роль і напрямки впровадження цифровізації в системі публічного управління у сфері національної безпеки України.

**Виклад основного матеріалу.** Дослідження Стратегії у сфері національної безпеки України «Безпека людини – безпека країни» [4] дало змогу зазначити, що в межах цього нормативно-правового документа цифровізація та діджиталізація один в один термінологічно не використовуються. Разом із тим, у межах аналізованої Стратегії можна зустріти відсилочні (бланкетні) норми або норми із синонімічним співставленням цифровізації (діджиталізації), зокрема, під час такого посилання на неї:

1) стрімко зростає роль інформаційних технологій у всіх сферах суспільного життя (п. 9);

2) зовнішня агресія передбачає гібридну війну, у межах якої *системно застосовуються* політичні, економічні, *інформаційно-психологічні*, кібер- і воєнні засоби (п. 17);

3) *відсутність цілісної інформаційної політики держави*, слабкість системи стратегічних комунікацій *ускладнюють нейтралізацію цієї загрози* (п. 20);

4) *пріоритетними завданнями правоохоронних, спеціальних, розвідувальних та інших державних органів відповідно до їх компетенції є активна й ефективна протидія зовнішнім спеціальним інформаційним операціям та кібератакам* (п. 45);

5) Україна має розвивати інклюзивний політичний діалог через *стимулювання конкуренції у сфері надання інформаційних послуг населенню* (п. 49);

6) *Україна здійснить цифрову трансформацію, забезпечить надання адміністративних послуг через безпечне «єдине вікно» з використанням сучасних інформаційних технологій, поширюватиме цифрову грамотність* (п. 51);

7) *основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації* (п. 52);

8) для гарантування достатку й безпеки громадян потрібні ресурси, які при залученні та ефективному використанні зовнішніх джерел можуть забезпечити *стале і динамічне економічне зростання*. Для цього необхідно створити сприятливі умови для запровадження новітніх технологій, зокрема у сферах безпеки та оборони, охорони здоров'я, промисловості, енергетиці, машинобудуванні, сільському господарстві, будівництві та інфраструктурі, спорті, в інформаційній та телекомунікаційній сферах (п. 53);

9) слід реалізувати Стратегію інформаційної безпеки (п. 66) [4].

Як бачимо, авторами Стратегії акцентується увага, насамперед, на ролі цифровізації в напрямку, з одного боку, підтримки інформаційної та кібербезпеки (в умовах зовнішньої агресії). А з другого – на підвищенні цифрової грамотності та пришвидшенні надання адміністративних послуг, зокрема, через безпечне «єдине вікно» (насамперед, під час мирного стану). Проте цифровізація не закінчується на цих двох основних напрямках. Свідченням цього є сфера нацбезпеки, цивільного захисту й цивільної оборони, що існують як у мирний час, так й у воєнний. Безперечно, останній стан зумовлює збільшення небезпек у сфері цивільного захисту, на які потрібно реагувати як завжди так само оперативно.

Як відомо, виникнення та поширення пандемії COVID-19 пришвидшило процеси цифровізації в усіх сферах суспільної життєдіяльності (освітній, медичній, податковій, фінансовій тощо). У той же час, зовнішня агресія проти України остаточно підкреслила (закцентувала) важливість не просто активізації цифровізації, а й необхідність її повсюдного впровадження на вітчизняних теренах.

За даними Міністерства цифрової трансформації України, пандемія COVID-19 прискорила цифровізацію в Україні настільки, що останнім часом (протягом 2020-2021 років) було впроваджено 94 проекти цифрової трансформації [1]. Крім того, за даними Мінцифри, онлайн послугами стали

користуватися у 5 разів більше українців. Діджиталізувалися останніми роками такі сфери суспільної життєдіяльності:

- 1) сфера медичного захисту;
- 2) правозахисту (створено та функціонує підрозділ Нацполіції проти домашнього насильства «ПОЛІНА»; усе більше актуалізувався «електронний суд»);
- 3) туристична сфера (діє платформа «ДРУГ»);
- 4) сфера захисту довкілля та інші сфери суспільної життєдіяльності також діджиталізуються.

На жаль, через зовнішню агресію проти України відбувся ряд вимушених змін, покликаних забезпечити більш менш нормальне життя українців. І це вже не кейси-безпеки, які доречні були при поширенні пандемії COVID-19. У відповідний період дії урядів не були обмежені через руйнування критичної чи логістичної інфраструктури, чи через пожежі, чи інші надзвичайні ситуації. Стимулом, якщо так можна наразі стверджувати, є саме військова агресія проти України. Ті засоби цифровізації, які були доречними у ковідний період не всі можуть спрацьовувати сьогодні.

Власне кажучи, сучасні публічно-управлінські зміни відбулися за допомогою повноцінного використання засобів цифровізації, а саме в таких напрямках (рис. 1):

- 1) українські програмісти за підтримки Міністерства цифрової трансформації України створили додаток, який сповіщає про повітряну та ще 5 типів тривоги — для людей, у яких немає або не працюють сирени та тих, хто знаходиться в укриттях;

- 2) спрощену процедуру звернення до органів державної влади за допомогою у разі втрати працездатності або житла чи іншого майна через зовнішню агресію проти України (через мобільний додаток «Дія»);

- 3) в окремих регіонах (у м. Харків, наприклад, створено чат-бот у месенджері, яким можна скористатися для повідомлення про знайдені снаряди [8];

- 4) в Україні створено додаток для розмінування територій (Державна служба України з надзвичайних ситуацій спільно з державною ІТ-компанією «Інфотех» запустили додаток «Розмінування України») [2] тощо. Варто зазначити, що застосунок «Розмінування України» дозволяє:

- повідомляти рятувальників про знайдені вибухонебезпечні та підозрілі предмети;

- переглянути мапу територій, які потенційно можуть бути забруднені вибухонебезпечними предметами;

- повідомити про знайдені на території України нездетоновані снаряди, міни, вибухонебезпечні та підозрілі предмети, залишити про них мітки на карті, додати фото та опис. Цю інформацію опрацьовує потім ДСНС України [там само].

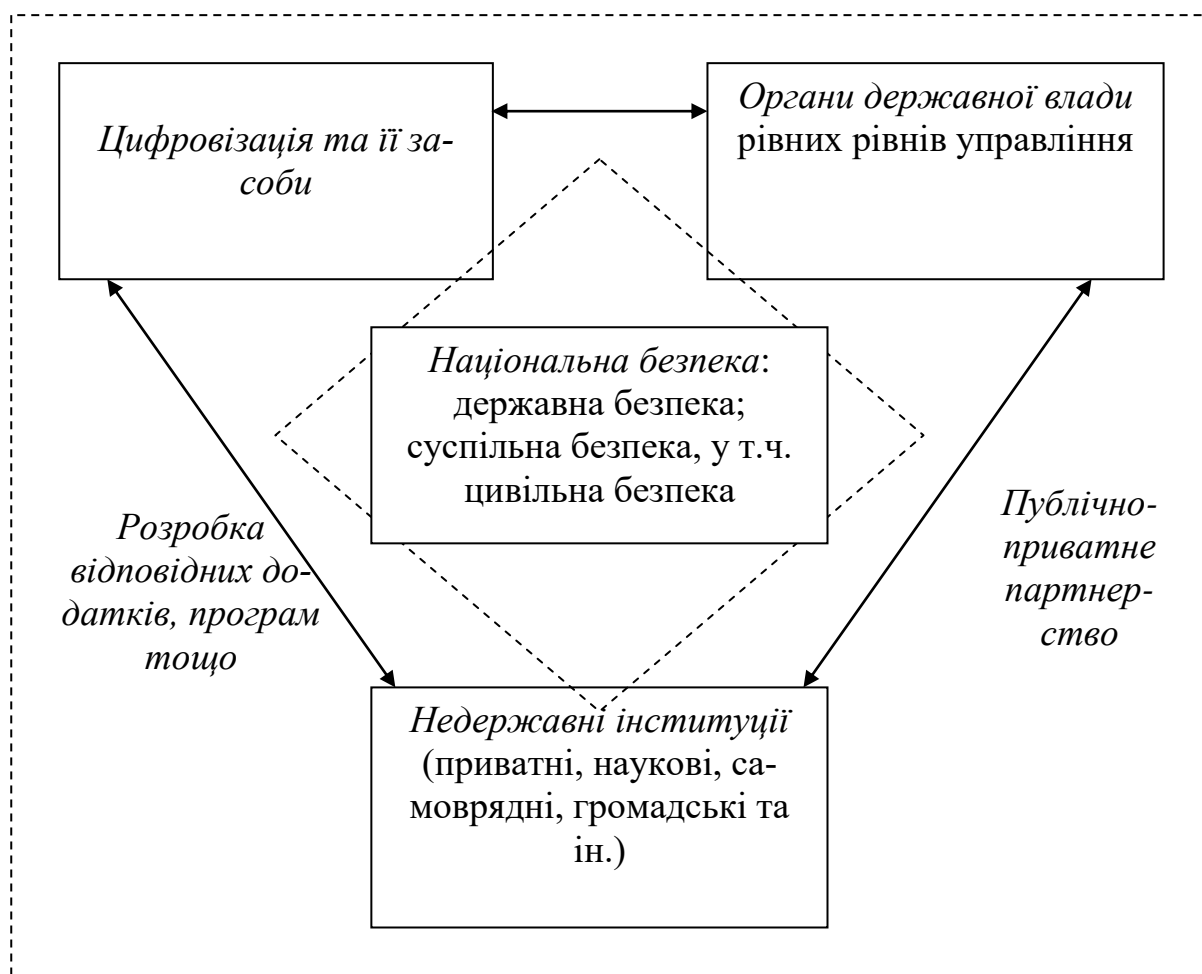


Рис. 1. Напрями використання цифровізації в державному та недержавному секторі в контексті забезпечення національної безпеки  
 Джерело: авторська розробка

Очевидно, можемо зауважити, що спостерігаються значні результати від державно-приватного партнерства у сфері цифровізації. Так, Мінцифри співпрацює з програмістами, які працюють на фрілансі або в приватних компаніях, ДСНС України – з ІТ-компанією та ін., і конкретний результат, спрямований на підтримку системи безпеки загалом і цивільної зокрема.

Отже, усі ці заходи, що реалізуються із використанням засобів цифровізації мають публічно-владний характер, оскільки передбачають як участь органів державної влади, так і недержавних інституцій. Ці заходи покликані забезпечити вчасне, комплексне й оперативне реагування на події, які убезпечують нормальну життєдіяльність суспільства. Власне кажучи, вживаються зазначені заходи та застосовуються новітні технології одночасно; і вони необхідні для максимально системного забезпечення функціонування сфери нацбезпеки, цивільного захисту й цивільної оборони. Крім того, актуальність оптимізації будови системи державного управління в зазна-

ченій сфері давно потребувала повсюдного впровадження засобів цифровізації. Проте тільки наразі це вже не викликає такого соціального спротиву та сумнівів, що унеможлиблювали вирішення наявних проблем та загроз. Сьогодні використання цифрових технологій – це реальність, відстані та часові межі якої можуть скорочуватися до нуля.

**Висновки.** Таким чином, на центральному, регіональному та місцевому рівнях управління відбувається гарантування безпеки, що передбачає забезпечення громадського порядку та цивільного захисту. Доведено, що зреалізувати повсюдність, масштабність і вчасність виконання цієї функції можливо за рахунок використання засобів цифровізації. Виявлено, що вона є реальністю та вимогою не тільки часу, а самого суспільства. Такому розумінню, на жаль, сприяв вплив позасистемних факторів. Серед них визначено виникнення та поширення пандемії COVID-19, зовнішню агресію проти України тощо. З огляду на це наполягається на використанні засобів цифровізації як тактичного та стратегічного інструментарію, що наближує державу (в особі її органів) до потреб населення. З'ясовано, що важливість використання засобів цифровізації варто визначати «до» і «після» активізації впливу позасистемних факторів. З метою нейтралізації негативного впливу останніх чинників аргументована необхідність у збільшенні напрямів упровадження цифровізації за допомогою публічно-приватного партнерства.

#### **Список використаних джерел:**

1. 12 проєктів у сфері захисту довкілля увійшли до плану цифрової трансформації країни. URL: <https://mepr.gov.ua/news/36859.html>.
2. В Україні створили додаток для розмінування територій. URL: <https://zn.ua/ukr/TECHNOLOGIES/v-ukrajini-stvorili-dodatok-dlja-rozminuvannja-teritorij.html>.
3. Домбровська С.М., Полторак С.Т. Механізми формування безпеки держави // Теорія та практика державного управління і місцевого самоврядування. 2015. № 1. URL: [http://nbuv.gov.ua/UJRN/Ttpdu\\_2015\\_1\\_21](http://nbuv.gov.ua/UJRN/Ttpdu_2015_1_21).
4. Офіційний веб-сайт Верховної Ради України. URL: <http://rada.gov.ua/>.
5. Ситник Г.П. Державне управління національною безпекою України: монографія. К.: вид-во НАДУ, 2004. 408 с.
6. Крук С. І. Поняття та сутність механізмів державного управління у сфері забезпечення національної безпеки України// Держава та регіони, 2018. № 4. С. 87–90.
7. Помаза-Пономаренко А.Л., Микитюк Ю.М. Цифровізація державної політики vs. державна політика цифровізації у сфері правового регулювання : монографія. Х.: НУЦЗУ. 2021. 200 с.
8. Харків'ян просять скористатися ботом для повідомлення про знайдені снаряди. URL: <https://www.city.kharkov.ua/uk/news/kharkivyan->

prosyat-skoristatysya-botom-dlya-povidomlennya-pro-znaydeni-snaryadi-49920.html.

9. Akimova L., Litvinova I., Ilchenko H., Pomaza-Ponomarenko A. The negative impact of corruption on the economic security of states. Scientific journal «International Journal of Management». 2020. № 11 (5). P. 1058-1071.

### References:

1. 12 projects in the field of environmental protection were included in the plan of digital transformation of the country [12 proyektiv u sferi zakhystu dovkilliya uviyshly do planu tsyfrovoyi transformatsiyi krayiny]. URL: <https://mepr.gov.ua/news/36859.html>.

2. In Ukraine, an application was created for demining territories [V Ukrayini stvoryly dodatok dlya rozminuvannya terytoriy]. URL: <https://zn.ua/ukr/TECHNOLOGIES/v-ukrajini-stvorili-dodatok-dlja-rozminuvannja-teritorij.html>.

3. Dombrovskaya S.M., Poltorak S.T. Mechanisms of state security formation [Mekhanizmy formuvannya bezpeky derzhavy] // Theory and practice of public administration and local self-government. 2015. № 1. URL: [http://nbuv.gov.ua/UJRN/Ttpdu\\_2015\\_1\\_21](http://nbuv.gov.ua/UJRN/Ttpdu_2015_1_21).

4. Official web site of the Verkhovna Rada of Ukraine [Ofitsiynyy veb-sayt Verkhovnoyi Rady Ukrayiny]. URL: <http://rada.gov.ua/>.

5. Sitnik G.P. State management of national security of Ukraine [Derzhavne upravlinnya natsional'noyu bezpekoy u Ukrayiny]. Monograph. Kyiv: NADU, 2004. 408 p. Print.

6. Kruk S.I. "The concept and essence of mechanisms of public administration in the field of national security of Ukraine". *State and Regions [Derzhava ta rehiony]*. 4 (2018): 87-90. Print.

7. Pomaza-Ponomarenko, A.L. and Mykytyuk, Yu.M. Digitization of state policy vs. state policy of digitization in the field of legal regulation: a monograph. Kharkiv: NUCZU. 2018. 200 p. Print.

8. Akimova L., Litvinova I., Ilchenko H., Pomaza-Ponomarenko A. "The negative impact of corruption on the economic security of states". Scientific journal «International Journal of Management». 2020. № 11 (5). P. 1058-1071. Print.