DOI: http://doi.org/10.51369/3083-5917-2024-1-8
УДК 34.01+351.86(477)+338.22

Наталя НОВІКОВА
доктор економічних наук, професор,
завідувач кафедри публічного управління та адміністрування,
Державний торговельно-економічний університет
E-mail: n.l.novikova@knute.edu.ua
ORCID: https://orcid.org/0000-0001-5219-9494

Людмила БОЙКО
аспірантка, Державний торговельно-економічного університет
E-mail: l.v.boyko@knute.edu.ua
ORCID https://orcid.org/0000-0002-6272-1298

ЦИФРОВІЗАЦІЯ ТА НАЦІОНАЛЬНА БЕЗПЕКА: ТЕНДЕНЦІЇ ТА ВИКЛИКИ

У статті проаналізовано роль цифровізації у забезпеченні національної безпеки. Визначено, що цифрова трансформація суспільних процесів позитивно впливає на розбудову взаємодії між владою та громадянами. Окреслено основні напрями діяльності та ключові тренди цифровізації у сфері GovTech. Визначено безпекові виклики, які сьогодні існують у цифровому просторі і потребують реагування з боку держави.

Авторами виявлено, що цифровізація суспільних процесів підвищує прозорість і довіру до діяльності уряду, оскільки сучасні підходи до взаємодії знижують бар'єри між урядом та громадянами, створюючи простір для продуктивного партнерства та спільнотворення. Констатовано, що координація громадських відносин, які склалися між суб'єктами з питань національної безпеки, а також створення умов для досягнення оптимального рівня безпеки в політичних, правових, інформаційних, соціально-економічних та військових сферах є основними цілями правового регулювання у сфері національної безпеки.

Аргументовано положення про те, що цифровізація державного управління у сфері національної безпеки має низку абсолютних переваг, зокрема поява нових цифрових підходів до врядування, розвиток та впровадження глобальних цифрових трендів, що підвищують прозорість та ефективність органів влади, оптимізують процеси обміну даними та створюють нові можливості для цифрового розвитку. Водночас визначено, що феномен цифровізації полягає у тому, що цифрова трансформація систем та суспільних відносин супроводжується виникненням значної кількості викликів, які потребують реагування та конкретних дій з боку держави. У сфері національної безпеки це насамперед забезпечення конфіденційності та захист даних, а з-поміж менш очевидних викликів можна виокремити інтеграцію даних в різних реєстрах, наявність цифрової нерівності та відновлення довіри громадян.

Ключові слова: *цифровізація, національна безпека, цифрова трансформація, кібербезпека, GovTech.*

Постановка проблеми. Цифровізація як динамічний процес та її вплив на різні сфери життєдіяльності суспільства вже багато років перебувають у центрі наукових дискусій і досліджень. В умовах стрімкого розвитку інноваційних технологій з'являються різноманітні цифрові рішення, необхідні для комплексної модернізації державного управління, зокрема

й в аспекті національної безпеки. Такі рішення, з одного боку, сприяють виникненню нових можливостей для розбудови системи національної безпеки у цифровому просторі. Проте, з іншого боку, процес цифрового розвитку держави зумовлює також появу численних викликів та загроз, зокрема таких, як поширення кіберзлочинності, недостатній рівень конфіденційності та захисту інформації, цифрова нерівність тощо. Тому дослідження впливу цифровізації на національну безпеку та визначення ключових тенденцій у цій сфері є важливим для розробки проектів та рішень, спрямованих на забезпечення стійкості держави до викликів сучасності.

Аналіз останніх досліджень і публікацій. Різні аспекти цифровізації державного управління у контексті національної безпеки є предметом дослідження таких науковців, як Л. Кормич, Т. Краснопольська, Ю. Завгородня, О. Мазурук, Я. Самусевич, В. Новіков та інших.

Мета статті полягає у визначенні ключових тенденцій розвитку цифровізації та викликів, з якими стикається держава у процесі забезпечення національної безпеки.

Виклад основного матеріалу. Цифрова трансформація є інструментом для забезпечення національної безпеки, оскільки цифрові технології є основним драйвером підвищення ефективності державного управління, розширення політичної участі й демократизації суспільного життя. Варто зазначити, що сам термін «цифрова трансформація» був уведений у науковий словник наприкінці XX – на початку XXI століття разом із використанням таких термінів, як «автоматизація», «комп'ютеризація», «інформатизація» та «цифрування». Під цим терміном науковці розуміють глобальний тренд застосування кібернетичних методів та інструментів управління, штучного інтелекту та інструментів аналізу великих даних, які призводять до досягнення критичної точки цифровізації. Водночас таке перетворення передбачає процес докорінної зміни форми та механізмів функціонування об'єкта чи його елементів під впливом внутрішніх або зовнішніх факторів [1].

Цифровізація суспільних процесів підвищує прозорість і довіру до діяльності уряду, оскільки сучасні підходи до взаємодії знижують бар'єри між урядом та громадянами, створюючи простір для продуктивного партнерства та спільнотворення. Власне, координація громадських відносин, які склалися між суб'єктами з питань національної безпеки, а також створення умов для досягнення оптимального рівня безпеки в політичних, правових, інформаційних, соціально-економічних та військових сферах є основними цілями правового регулювання у сфері національної безпеки. Досягнення даних цілей є передумовою для реалізації конституційних норм, виконання яких неможливе без застосування інформаційно-комунікаційних технологій. Ми погоджуємося з думкою Л. Домбровського, котрий стверджує, що національна безпека є певним громадським благом, цінність якого нестримно підвищується за умови узгодженої взаємодії органів публічної влади і громадянського суспільства [2].

Взаємодія громадян, державних та приватних структур, науковців і розпорядників венчурного капіталу, які беруть участь у розробці технологічних рішень для вирішення суспільних проблем держави, породжує появу екосистеми GovTech [3] – це абревіатура від Government Technology і нова концепція, яка набуває популярності в Україні та світі. GovTech передбачає вдосконалення розробки та постачання орієнтованих на людину держав-

них послуг та процесів, створених на основі керованих даних за допомогою цифрових технологій. Цей сектор представлений компаніями, які розробляють соціально-технічні рішення для урядів тих країн, які прагнуть впроваджувати сучасні цифрові продукти.

В умовах цифровізації уряди країн зосереджуються на IT-послугах і відповідному програмному забезпеченні, про що свідчить структура їхніх витрат на рішення GovTech. Переважна більшість компаній GovTech у всьому світі працюють у підсекторах електронного урядування та охорони здоров'я, оскільки ці сфери користуються найбільшим попитом. Серед інших популярних підгалузей GovTech компаній можемо також виділити кібербезпеку та громадську безпеку (рис. 1).

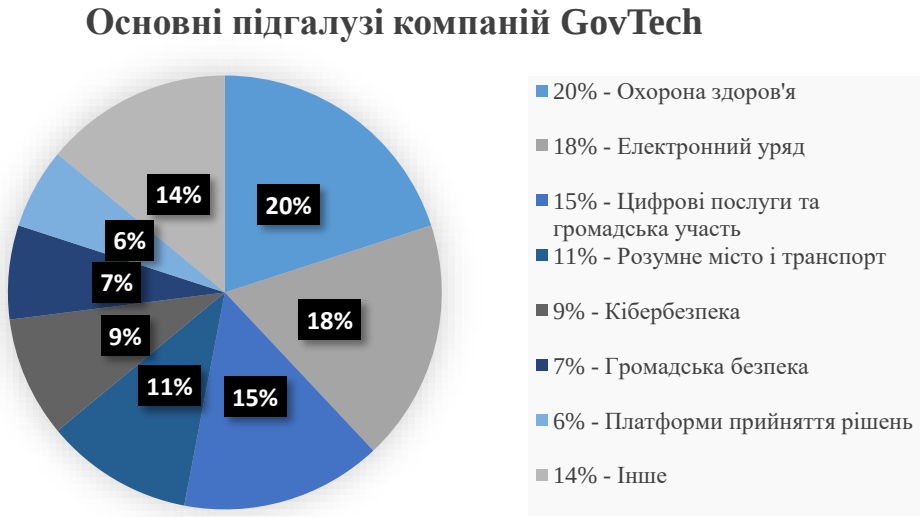

Рисунок 1 – Основні підгалузі компаній GovTech у світі (джерело: сформовано за [4])

За результатами дослідження «The global market of Govtech solutions» [5], що було проведено аудиторською компанією Kreston Ukraine за підтримки Міністерства цифрової трансформації України, Міністерства економіки України, Офісу реформ Кабінету Міністрів України та ISE Corporate Accelerator у 2023 році поряд із штучним інтелектом, цифровою ідентифікацію, гіпертавтоматизацією, цифровими валютами та загальною модернізацією сектору IT ключовим трендом GovTech індустрії є кібербезпека держави.

Оскільки кількість кібератак у всьому світі зростає, суспільство стурбоване захистом даних, які зберігаються та використовуються урядом. Необхідність підтримки безпеки та довіри громадян зумовлює те, що кібербезпека стає основним викликом для суб'єктів національної безпеки. Державні установи все частіше використовують можливості штучного інтелекту для автоматизації виявлення атак реагування на них і мають можливість передати деякі з цих функцій на аутсорсинг приватним компаніям [5].

Окрім кібербезпеки, яка вимагає системної роботи над забезпеченням надійності цифрових систем і захисту особистих даних громадян, О. Мазурук та С. Пойда відносять до основних викликів при реалізації цифрових ініціатив у публічному управлінні таке [6]:

– забезпечення цифрової включеності: цифрова трансформація має бути

доступною для всіх громадян, зокрема з обмеженим доступом до Інтернету або тих, хто не має необхідних навичок для використання цифрових інструментів, тому необхідно створювати умови для інклюзивного доступу до адміністративних послуг та навчання цифрової грамотності громадян;

– прозорість: громадяни мають розуміти, як саме працюють автоматизовані цифрові системи та штучний інтелект у владних структурах, а їх використання у прийнятті рішень мусить відповідати затвердженим нормам;

– доступність та інтеграція даних: додаткової уваги й контролю потребує здатність публічних органів до інтеграції цифрових систем, обробки та обміну даними між різними департаментами та органами влади в режимі реального часу;

– відновлення довіри: можливість маніпуляцій у нестабільному цифровому середовищі може похитнути довіру громадян до публічних інституцій, тому органам влади слід забезпечувати відповідальне використання цифрових інструментів і налагоджувати якісну взаємодію з громадянами.

Підтвердженням того, що побудова довіри має стати одним із пріоритетних завдань держави найближчим часом є дослідження «Оцінка ситуації в країні, довіра до соціальних інститутів, віра в перемогу, ставлення до виборів», проведеного у березні 2024 року. Відповідно до результатів дослідження довіри державному апарату часто висловлюють недовіру – їм не довіряють близько 76 % опитаних респондентів [7].

Важливим пріоритетом у процесі розбудови національної безпеки, передусім в інформаційній сфері, є розвиток цифрової освіти громадян. Вітчизняні дослідження, здійснені на основі економіко-математичного моделювання, підтверджують, що між національною безпекою, цифровізацією та освітою існують динамічні конвергентні зв'язки, що засвідчує необхідність подальшої інтеграції регуляторних практик у галузі цифровізаційних викликів національної безпеки, включаючи цифровізацію освіти [8].

Одним із доступних та важливих сервісів для самоосвіти українців є платформа «Дія. Цифрова освіта». Поєднання важливої інформації та розважальних освітніх форматів, своєю чергою, приваблює різні категорії людей і позитивно впливає на їх мотивацію здобувати нові цифрові навички. За даними Міністерства цифрової трансформації України понад 2 млн українців нині навчаються цифрової грамотності на платформах національного проєкту «Дія». Інноваційний безоплатний формат навчання є його унікальною особливістю. Після закінчення навчання учні мають змогу отримати сертифікати. На порталі розміщено освітні серіали на тему онлайн-безпеки та кібербезпеки [9], а також детальну інформацію про інформаційну гігієну в умовах воєнного стану з метою захисту громадян від дезінформації.

У даному контексті вважаємо за потрібне згадати, що в умовах воєнного часу якісна протидія дезінформації є ще одним викликом для сучасної України. Дезінформація – це спотворена, свідомо неправдива, провокаційно-тенденційна інформація, поширена як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо. Зростання кількості фейків та дезінформації потребує ефективного алгоритму для швидкого реагування. Протягом останніх років важливу роль у фільтруванні та перевірці фактів відіграли фактчекінгові проєкти: StopFake, По той бік новин, Вокс Чек, Без брехні, окремі медіа, що створили спеціальні рубрики, наприклад Texty.org.ua

(Деза війни, Фейкогриз), Детектор Медіа (DisinfoChronical), а також урядові ініціативи: Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури України та Центр протидії дезінформації при РНБО України [10].

Кількість дезінформації та інших згаданих вище викликів постійно зростає. Тому важливо, щоб цифровізація стала ефективним інструментом державної влади у процесі реагування на ці виклики, що сприятиме стійкості системи національної безпеки України.

Висновки. Цифровізація державного управління у сфері національної безпеки має низку абсолютних переваг, зокрема поява нових цифрових підходів до врядування, розвиток та впровадження глобальних цифрових трендів, що підвищують прозорість та ефективність органів влади, оптимізують процеси обміну даними та створюють нові можливості для цифрового розвитку. Проте феномен цифровізації полягає у тому, що цифрова трансформація систем та суспільних відносин супроводжується, що цілком логічно, виникненням значної кількості викликів, які потребують реагування та конкретних дій з боку держави. У сфері національної безпеки це насамперед забезпечення конфіденційності та захист даних, а з-поміж менш очевидних викликів можна виокремити інтеграцію даних в різних реєстрах, наявність цифрової нерівності та відновлення довіри громадян.

Список використаних джерел:

1. Kormych, L., Krasnopolska, T., & Zavhorodnia, Y. (2024). 1Digital Transformation and National Security Ensuring. *Evropský politický a právní diskurz*. № 1. С. 29–37. https://eppd13.cz/wp-content/uploads/2024/2024-11-1/06.pdf (дата звернення: 22.11.2024).

2. Домбровський Л. В. Інформаційна безпека держави у системі національної безпеки України. *Вісник національного університету цивільного захисту України.* 2024. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/20339/1/12Dombrovskyi.pdf (дата звернення: 22.11.2024).

3. Hoekstra, M., Van Veenstra, A. F., & Bharosa, N. (2023, July). Success Factors and Barriers of GovTech Ecosystems: A case study of GovTech ecosystems in the Netherlands and Lithuania. In *Proceedings of the 24th Annual International Conference on Digital Government Research*. P. 280-288.

4. Global Govtech Industry Landscape Overview Q2 2022", Deep Knowledge Analytics. https://analytics.dkv.global/govtech-teaser.pdf (дата звернення: 22.11.2024)

5. Результати дослідження «The global market of Govtech solutions». Офіс реформ. URL: https://rdo.in.ua/news/rezultaty-doslidzhennya-global-market-govtech-solutions (дата звернення: 22.11.2024)

6. Мазурук, О., & Пойда, С. (2023). Вплив цифрових інструментів на зміни в сучасному публічному управлінні : матеріали конференцій МНЛ, (15 груд. 2023 р., м. Івано-Франківськ), 109–111.

7. Результати дослідження Центру Разумкова «Оцінка ситуації в країні, довіра до соціальних інститутів, віра в перемогу, ставлення до виборів» URL: https://razumkov.org.ua/novyny/otsinka-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-vira-v-peremogu-stavlennia-do-vyboriv-berezen-2024r (дата звернення: 22.11.2024).

8. Samusevych, Y. V., Novikov, V. V., Artiukhov, A. Y., & Vasylieva, T. A. (2021). Convergence trends in the "economy-education-digitalization-national security" chain.

9. Портал «Дія. Цифрова освіта» URL: https://osvita.diia.gov.ua/catalog/topic/cybersecurity (дата звернення: 22.11.2024).

10. Скіпор, В. Е. (2023). Протидія дезінформації та фейкам в інформаційному полі України під час війни. Рекомендовано до друку Вченою радою Факультету журналістики Київського університету імені Бориса Грінченка (протокол № 4 від 9 лютого 2023 р.), 59.

Стаття надійшла до редакції 15.11.2024

N. Novikova, L. Boyko

DIGITALIZATION AND NATIONAL SECURITY: TRENDS AND CHALLENGES

The article analyzes the role of digitalization in ensuring national security. It is determined that the digital transformation of social processes has a positive impact on the development of interaction between the authorities and citizens. The main areas of activity and key trends of digitalization in the field of GovTech are outlined. The security challenges that exist today in the digital space and require a response from the state are identified.

The authors found that the digitalization of social processes increases transparency and trust in government activities, since modern approaches to interaction reduce barriers between the government and citizens, creating space for productive partnership and co-creation. It is stated that the coordination of public relations that have developed between subjects on issues of national security, as well as the creation of conditions for achieving an optimal level of security in the political, legal, information, socio-economic and military spheres are the main goals of legal regulation in the field of national security.

The position is argued that the digitalization of public administration in the field of national security has a number of absolute advantages, in particular the emergence of new digital approaches to governance, the development and implementation of global digital trends that increase the transparency and efficiency of government bodies, optimize data exchange processes and create new opportunities for digital development. At the same time, it is determined that the phenomenon of digitalization is that the digital transformation of systems and social relations is accompanied by the emergence of a significant number of challenges that require response and specific actions from the state. In the field of national security, this is primarily ensuring confidentiality and data protection, and among the less obvious challenges, one can single out the integration of data in various registers, the presence of digital inequality and the restoration of citizens' trust.

Keywords*: digitalization, national security, digital transformation, cybersecurity, GovTech.*