

*Галушко С.П., здобувач вищої освіти НУЦЗУ, м. Харків,  
ORCID: 0009-0005-3169-1478*

*Galushko S., Postgraduate student of the Educational, Research and  
Production Center, National University of Civil Protection of Ukraine, Kharkiv*

## **ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ**

## **THEORETICAL PRINCIPLES OF PUBLIC ADMINISTRATION IN THE SPHERE OF NATIONAL SECURITY UNDER THE CONDITIONS OF DIGITALIZATION**

*Досліджено теоретичні засади публічного управління у сфері національної безпеки в умовах цифровізації. Обґрунтовано роль штучного інтелекту у сфері забезпечення у сфері національної безпеки.*

***Ключові слова:** публічне управління, сфера національної безпеки, цифровізація, технології цифровізації, цифрова трансформація, органи влади.*

*The theoretical principles of public administration in the field of national security in the conditions of digitalization have been studied. The role of artificial intelligence in the provision of national security is substantiated.*

***Keywords:** public administration, sphere of national security, digitalization, digitalization technologies, digital transformation, authorities.*

**Постановка проблеми.** Вітчизняні та закордонні дослідники слушно наголошують, намагаючись попередити ті чи інші кризові явища, що технології, пов'язані зі штучним інтелектом, змінюють звичний порядок життя, у т.ч. у внутрішній та міжнародній безпеці. Крім того, ці технології забезпечують трансформацію системи публічного управління у сфері забезпечення національної безпеки. Вони передбачають застосування інших підходів до всієї гарантування глобальної системи безпеки. Проте як саме змінюється система безпеки держави під впливом поширення «штучного інтелекту». З огляду на це можемо відзначити важливість науково-теоретичного дослідження особливостей такого впливу штучного інтелекту на зазначену сферу суспільної життєдіяльності.

**Аналіз останніх досліджень і публікацій.** Розгляду особливостей формування та реалізації державної політики у сфері забезпечення національної безпеки присвячені публікації таких науковців, як Базилюк Я., Гриценко А., Денисенко М., Карсруд А., Клют Р., Колісніченко П., Лекарь С., Орлик В., Почепцов Г, Тайер А., Чуб С. та інші [1-5; 13; 20-26].

Однак чимало питань стосовно можливостей запровадження в Україні існуючого передового світового досвіду формування та реалізації державної політики у сфері забезпечення національної безпеки залишаються недостатньо дослідженими, і ці аспекти пов'язані з використанням цифрових технологій.

**Постановка завдання.** Метою статті є аналіз сучасного стану реалізації механізмів публічного управління у сфері національної безпеки в умовах цифровізації.

**Виклад основного матеріалу.** Група вчених слушно зауважили, що прийняття урядових рішень ґрунтується на певних даних та інформації [2; 3; 15; 17]. З огляду на це набуває актуальності питання використання, обміну, аналізу даних, а також забезпечення прозорості та підзвітності державного управління. Ці питання стають усе більш важливими як для сфери політики та державного управління, так і з технологічної погляду.

У теоретичний і практичний обіг був введений термін «datafication», що означає можливість трансформувати нетрадиційні джерела інформації, такі як текст, зображення та транзакційні записи, у дані. Поява такої можливості дозволяє управлінням краще розуміти інформацію, що витягується з різноманітних даних, і забезпечує проникнення кількісного аналізу в політичний процес глибше, ніж будь-коли раніше.

Зростання здатності збирати та аналізувати дані в режимі реального часу визначає потребу у розширенні доступу до них та створює умови для прийняття рішень, що ґрунтуються на фактичних даних [2; 3; 17]. У сфері державної політики системи безпеки зазначені зміни проявляються по-різному, зокрема, з позиції національних інтересів (державних, суспільних, приватних й окремо взятих громадян), а саме:

– академічні дисципліни, які вивчають політику та управління, усе більше розвиваються у форматі data-driven та method-driven, і пропонують все більшу кількість обчислювальних (computational social/political science) та алгоритмічних підходів, які мають на увазі роботу з даними;

– громадськість приділяє все більшу увагу питанням цифрового середовища, приватності та конфіденційності в роботі з даними (звідси – явища «дата-активізму» (data-activism) та посилення дискусій про безпеку цифрового простору);

– державні органи покликані створювати умови та (або) безпосередньо розвивають цифрові (електронні) технології, таким чином, підвищуючи результативність державної політики та публічного управління

(electronic/digital democracy, electronic/digital government, GovTech, electronic participation та ін.). При цьому все більш впливовим підходом стає «державна політика, заснована на даних, як різновид та прояв доказової політики (evidence based policy);

– бізнес комерціалізує дані, використовуючи їх (наприклад, дані користувачів) для отримання прибутку, збільшення власної вартості тощо. (виражається в розхожому виразі «дані – це нова нафта»);

– у наднаціональному плані мають вирішуватися питання, пов'язані з даними та цифровими технологіями на міжнародному рівні

Отже, дані та цифрові технології сприймаються як драйвер розвитку держав, населення, приватного сектору та громадян в цілому («Digital Transformation Initiative») [25]. При цьому спостерігається трансформаційний ефект цифрових технологій в останні десятиліття, що став основним фокусом розвитку конкурентоспроможності держав та формування сталого та гнучкого суспільства, на думку експертів ООН, а цифрова конкурентоспроможність сприймається як основний виклик соціально-економічного розвитку (IMD World Competitiveness Center) [22] та ін. У той же час, будь-який виклик - це певною мірою джерело загроз.

Збільшення джерел даних, їх варіативність, поширеність й обсяги нарівні з підвищенням обчислювальних потужностей зумовлюють стрімкий розвиток різних технологічних концепцій, де метадані є базисом. Це призводить до появи нової соціально-політичної моделі «цифровізації», що, з одного боку, забезпечує модернізацію приватного й державного секторів, а з іншого – ці сектори стають мішенню, площадкою для апробації цифрових технологій з метою дестабілізації нормальної роботи цих секторів.

Останнім часом цифровізація та цифрова трансформація привертають величезну увагу як з боку представників держав, так і з боку міжнародних організацій (державних та недержавних). Здебільшого дослідники розглядають цифровізацію як «рятувальне коло», що є цілком виправданим. Згідно з різними розробками, ефективна цифрова адаптація відіграє ключову роль у досягненні зростання доходів та підвищенні задоволеності користувачів [11], тобто громадян. Цифрові технології можуть принести користь суспільству, полегшуючи доступ до державних послуг, підвищити зайнятість населення та темпи економічного зростання, що може сприяти підвищенню рівня благополуччя громадян [12]. Цифровізація доповнює та компенсує традиційні та формальні механізми взаємодії громадян та уряду, створюючи додаткові та/або доповнюючі традиційні інститути. Більше того, цифровізація значно змінила відносини між державою та суспільством, поступово підвищуючи частоту й якість взаємодії між громадянами та урядом [24].

Зазначені процеси змінюють структуру та зміст державної політики та державного управління [6; 8]. Слід зазначити, що через комплексний

характер феномену цифровізації відбувається термінологічна плутанина. З однією сторони, такі терміни, як оцифрування (завантаження форм в Інтернеті), цифровізація (заповнення форм в Інтернеті) та цифрова трансформація (надання повного обслуговування в режимі онлайн), використовуються в літературі як взаємозамінні та часто зосереджені лише на перших двох функціях [15]. З іншого – в основі безпосередньо цифровізації лежить взаємозв'язок різних типів цифрових технологій, а також система трьох елементів, що включає: інфраструктуру технології, програмне забезпечення, а також користувачів та програмне забезпечення, що зв'язує як технологію та користувача, і користувачів між собою. У зв'язку з цим для цілей даного дослідження застосовується концептуалізація, запропонована Мергелем, Едельманном та Хаугом [15], сфокусована на концепті цифровізації:

– оцифрування, що передбачає перехід від аналогових до цифрових послуг зі зміною «один до одному» у «доставці» контенту/інформації та з додаванням технологічного канал зв'язку;

– цифровізація, що зосередження уваги на потенційних змінах процесах (як соціальних, економічних, так і політичних), крім звичайного оцифрування існуючих процесів і форм;

– цифрова трансформація, що охоплює реалізацію процесів у цифровому середовищі з урахуванням культурних, соціальних й організаційних особливостей із застосуванням цілісного підходу та отриманням різних результатів.

На наше переконання, слушною в цьому контексті є позиція вчених Кастеллса та Почепцова, за якої цифровізація охоплює технологічні досягнення й інституційні зміни такі, як надійне з'єднання та стандарти якості, мережа Інтернет і безпека даних, фінансові та правові основи, а також науковий, інноваційний та людський капітал [1; 9].

Поширення цифрових технологій у політичному житті є хоч і щодо недавнім, але визнаним об'єктом дослідження (наприклад, дослідження глобальних політичних комунікацій та глобального політичного управління [9], впливу цифрового розриву на політичну участь [21], впливу використання Інтернету та онлайн-діяльності на політичну участь [18], впливу інформаційних та цифрових технологій на електоральну поведінку [23]; дослідження інституційних та неінституційних форм політичної участі з застосуванням інформаційних та цифрових технологій [14], «цифрових аборигенів» та «мережевого покоління» [6], негативного впливу Інтернету та онлайн середовища на політичну замученість [7], електронної участі [19], електронного уряду та ін.).

Таким чином, забезпечення безпеки впливає на ефективність держави як усередині її кордонів, і поза ними. В останні роки все більше уваги вчені приділяють дослідженню формування, регламентації та безпосередньому

забезпеченню національної безпеки з позиції посилення процесів цифровізації. У цьому контексті набувають важливості питання, пов'язані з підтримкою інформаційної безпеки та кібербезпеки. Результат – це сфера забезпечення нацбезпеки, що розширюється та наповнюється новими елементами такими, як кібербезпека, безпека комп'ютерних мереж, інформаційна безпека тощо. Відповідно, за рахунок використання цифрових технологій збільшується арсенал засобів забезпечення національної безпеки (технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються в системі забезпечення нацбезпеки для збору, формування, обробки, передачі або прийому інформації про стан такої безпеки та заходи щодо її зміцнення).

**Висновки.** Отже, спостерігаючи підвищення статусу та свого роду відокремлення галузі соціальних наук (включаючи і політичну), що фокусується на цифровій тематиці, можна констатувати, що відсутня єдність оцінок та підходів до осмислення соціально-політичних ефектів цифровізації.

Залишається безліч проблем, пов'язаних з таким: 1) обробкою, зберіганням та обігом даних [26]; 2) з наслідками впровадження різних технологічних рішень, за яких потенційно можливе зниження національного контролю не лише над даними, але й над тим, що ці дані описують (як приклад можна взяти хмарні обчислення в іноземній юрисдикції та пов'язані ризики «цифрової вразливості») [13]; 3) з використанням персональних даних, особливо медичних [20]; 4) формуванням та адмініструванням державних реєстрів [14] та ін.

Цифрові технології викликають зміни у сфері забезпечення безпеки. Однією з основних функцій сучасної держави, незалежно від типу політичного режиму, залишається забезпечення безпеки громадян (певних груп громадян) і себе в цілому. Якість реалізації такої функції впливає на сприйняття громадянами легітимності уряду, політичних інститутів та акторів.

#### **Список використаних джерел:**

1. Почепцов Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Харків : Віват, 2022. 384 с.
2. Помаза-Пономаренко А.Л., Тарадуда Д.В. Закордонний досвід забезпечення соціальної безпеки шляхом стійкого функціонування об'єктів критичної інфраструктури та підвищеної небезпеки // Наука і техніка сьогодні. 2024. № 4 (32). С. 371-384.
3. Помаза-Пономаренко А.Л., Тарадуда Д.В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). <https://www.inter-nauka.com/issues/administration2024/3/9732>.
4. Тайер А.А. Вплив комунікативних технологій на ефективність

публічного управління в Україні в умовах воєнного стану. URL: <https://maup.com.ua/assets/files/dis/25-00-05/tajer-disertaciya.pdf/>.

5. Чуб С.В. Механізми прийняття державно-управлінських рішень у сфері національної безпеки в сучасній Україні. URL: <https://maup.com.ua/assets/files/dis/25-00-05/chub-disertaciya.pdf>.

6. Bennett S., Maton K., Kervin L. The digital natives debate: A critical review of the evidence // *British Journal of Educational Technology*. 2008. Vol. 39, no. 5. P. 775–786.

7. Boulianne S. Does internet use affect engagement?: A meta-analysis of research // *Political Communication*. 2009. Vol. 26, no. 2. P. 193–211.

8. Bretschneider, Mergel. Technology and Public Management Information Systems: Where we have been and where we are going // *The state of public administration: issues, challenges, and opportunities*. 1st ed. London:Routledge Taylor Francis Group, 2015. P. 187–203.

9. Castells. The new public sphere: Global civil society, communication networks, and global governance // *The Annals of the American Academy of Political and Social Science*. 2008. Vol. 616, no. 1. P. 78–93.

10. Data science meets public policy. URL: <https://mag.uchicago.edu/university-news/data-science-meets-public-policy>.

11. Dong Q.J. Moving a Mountain with a Teaspoon: Toward a Theory of Digital Entrepreneurship in the Regulatory Environment // *Technological Forecasting and Social Change*. 2019. Sept. Vol. 146. P. 923–930.

12. Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // *Journal of Business Research*. 2019. Vol. 101(C), no. 146. P. 522–527.

13. Hagen J., Lysne O. Protecting the digitized society—the challenge of balancing surveillance and privacy // *The Cyber Defense Review*. 2016. Vol. 1, no. 1. P. 75–90.

14. Hooghe M., Marien S., Quintelier E. Inequalities in non-institutionalized forms of political participation: A multi-level analysis of 25 countries // *Political Studies*. 2010. Vol. 58, no. 1. P. 87–213.

15. Mergel, Edelmann, Haug. Defining digital transformation: Results from expert interviews // *Government Information Quarterly*. 2019. Oct. Vol. 36, no. 4. P. 101385.

16. Office of the Provost, The University of Chicago. URL:<https://provost.uchicago.edu/directory/daniel-diermeier>.

17. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // *AD ALTA: Journal of Interdisciplinary Research*. 2024. Volume 14. Issue 1. Pp. 216–220. URL: [https://www.magnanimitas.cz/ADALTA/140139/papers/K\\_10.pdf](https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf).

18. Quintelier E., Vissers S. The effect of Internet use on political participation: An analysis of survey results for 16-year-olds in Belgium // *Social Science Computer Review*. 2008. Vol. 26, no. 4. P. 411–427.

19. Saebo O., Rose J., Skiftenes Flak L. The shape of e-Participation: Characterizing an emerging research area // *Government Information Quarterly*. 2008. Vol. 25, no. 3. P. 400–428.

20. Sun T., Medaglia R. Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare // *Government Information Quarterly*. 2019. Vol. 36, no. 2. P. 368–383.

21. Sylvester D., McGlynn A. The digital divide, political participation, and place // *Social Science Computer Review*. 2010. Vol. 28, no. 1. P. 64–74.

22. The IMD World Digital Competitiveness Ranking 2018 by Arturo Bris, Jose Caballero, Christo Cabolis and Marco Pistis. IMD World Competitiveness Center.

23. Tolbert C., McNeal R. Unraveling the effects of the Internet on political participation? // *Political Research Quarterly*. 2003. Vol. 56, no. 2. P. 175–185.

24. Wong, Chu. Digital Governance as Institutional Adaptation and Development: Social Media Strategies between Hong Kong and Shenzhen // *China Review*. 2020. Aug. Vol. 20, no. 3. P. 43–70.

25. World Economic Forum. Digital Transformation Initiative. URL: <http://reports.weforum.org/digital-transformation>.

26. Wright D., Raab C. D. Constructing a surveillance impact assessment // *Computer Law and Security Review*. 2012. Vol. 28, no. 6. P. 613–626.

### References:

1. Pocheptsov G. Toxic infospace. How to maintain clarity of thinking and freedom of action. Kharkiv: Vivat, 2022. 384 p.

2. Pomaza-Ponomarenko A.L., Taraduda D.V. Foreign experience of ensuring social security through the sustainable functioning of critical infrastructure objects and increased danger // *Science and technology today*. 2024. No. 4 (32). P. 371-384.

3. Pomaza-Ponomarenko A.L., Taraduda D.V. Mechanisms for ensuring civil security of Ukraine: aspects of emergency prevention at the facilities of the military-industrial complex // *Public administration and national security*. 2024. No. 3 (44). <https://www.inter-nauka.com/issues/administration2024/3/9732>.

4. Thayer A.A. The impact of communication technologies on the effectiveness of public administration in Ukraine under martial law. URL: <https://maup.com.ua/assets/files/dis/25-00-05/tajer-disertaciya.pdf/>.

5. Chub S.V. Mechanisms of state-management decision-making in the field of national security in modern Ukraine. URL: <https://maup.com.ua/assets/files/dis/25-00-05/chub-disertaciya.pdf>.

6. Bennett S., Maton K., Kervin L. The digital natives debate: A critical review of the evidence // *British Journal of Educational Technology*. 2008. Vol. 39, no. 5. P. 775–786.

7. Boulianne S. Does internet use affect engagement?: A meta-analysis of research // *Political Communication*. 2009. Vol. 26, no. 2. P. 193–211.

8. Bretschneider, Mergel. Technology and Public Management Information Systems: Where we have been and where we are going // *The state of public administration: issues, challenges, and opportunities*. 1st ed. London:Routledge Taylor Francis Group, 2015. P. 187–203.

9. Castells. The new public sphere: Global civil society, communication networks, and global governance // *The Annals of the American Academy of Political and Social Science*. 2008. Vol. 616, no. 1. P. 78–93.

10. Data science meets public policy. URL: <https://mag.uchicago.edu/university->

news/data-science-meets-public-policy.

11. Dong Q.J. Moving a Mountain with a Teaspoon: Toward a Theory of Digital Entrepreneurship in the Regulatory Environment // *Technological Forecasting and Social Change*. 2019. Sept. Vol. 146. P. 923–930.

12. Galindo-Martin M.-A., Castano-Martinez M.-S., Mendez-Picazo M.-T. Digital Transformation, Digital Dividends and Entrepreneurship: A Quantitative Analysis // *Journal of Business Research*. 2019. Vol. 101(C), no. 146. P. 522–527.

13. Hagen J., Lysne O. Protecting the digitized society—the challenge of balancing surveillance and privacy // *The Cyber Defense Review*. 2016. Vol. 1, no. 1. P. 75–90.

14. Hooghe M., Marien S., Quintelier E. Inequalities in non-institutionalized forms of political participation: A multi-level analysis of 25 countries // *Political Studies*. 2010. Vol. 58, no. 1. P. 87–213.

15. Mergel, Edelmann, Haug. Defining digital transformation: Results from expert interviews // *Government Information Quarterly*. 2019. Oct. Vol. 36, no. 4. P. 101385.

16. Office of the Provost, The University of Chicago. URL:<https://provost.uchicago.edu/directory/daniel-diermeier>.

17. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // *AD ALTA: Journal of Interdisciplinary Research*. 2024. Volume 14. Issue 1. Pp. 216–220. URL: [https://www.magnanimitas.cz/ADALTA/140139/papers/K\\_10.pdf](https://www.magnanimitas.cz/ADALTA/140139/papers/K_10.pdf).

18. Quintelier E., Vissers S. The effect of Internet use on political participation: An analysis of survey results for 16-year-olds in Belgium // *Social Science Computer Review*. 2008. Vol. 26, no. 4. P. 411–427.

19. Saebo O., Rose J., Skiftenes Flak L. The shape of e-Participation: Characterizing an emerging research area // *Government Information Quarterly*. 2008. Vol. 25, no. 3. P. 400–428.

20. Sun T., Medaglia R. Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare // *Government Information Quarterly*. 2019. Vol. 36, no. 2. P. 368–383.

21. Sylvester D., McGlynn A. The digital divide, political participation, and place // *Social Science Computer Review*. 2010. Vol. 28, no. 1. P. 64–74.

22. The IMD World Digital Competitiveness Ranking 2018 by Arturo Bris, Jose Caballero, Christo Cabolis and Marco Pistis. IMD World Competitiveness Center.

23. Tolbert C., McNeal R. Unraveling the effects of the Internet on political participation? // *Political Research Quarterly*. 2003. Vol. 56, no. 2. P. 175–185.

24. Wong, Chu. Digital Governance as Institutional Adaptation and Development: Social Media Strategies between Hong Kong and Shenzhen // *China Review*. 2020. Aug. Vol. 20, no. 3. P. 43–70.

25. World Economic Forum. Digital Transformation Initiative. URL: <http://reports.weforum.org/digital-transformation>.

26. Wright D., Raab C. D. Constructing a surveillance impact assessment // *Computer Law and Security Review*. 2012. Vol. 28, no. 6. P. 613–626.