DOI 10.52363/2414-5866-2023-2-19
УДК 351:355:342.7

Рожко В.М., *здобувач ННВЦ НУЦЗУ, м. Харків,*
ORCID: 0009-0009-8947-7932

Rozhko V., *Ph.D. student at the National University of Civil Defense of Ukraine, Kharkiv*

ЗАКОРДОННИЙ ДОСВІД ПУБЛІЧНОГО УПРАВЛІННЯ ЦИФРОВІЗАЦІЄЮ У ВОЄННІЙ СФЕРІ

FOREIGN EXPERIENCE OF PUBLIC MANAGEMENT OF DIGITALIZATION IN THE MILITARY SPHERE

Підкреслено, що Ізраїль є піонером у сфері цифровізації, та саме цією країною було започатковано цифрові інновації в Армії оборони Ізраїлю. Показано, що Відчуття терміновості модернізації Збройних сил Німеччини випливає зі зміненої структури політики безпеки. Країни змушені просуватися вперед з інноваціями, щоб мати можливість продовжувати забезпечувати безпеку. Зазначено, що НАТО та ЄС також розпочали процес цифрової трансформації оборони. У 2022 та 2023 роках НАТО прийняла своє перше в історії бачення цифрової трансформації та стратегію реалізації цифрової трансформації, а ЄС схвалив Стратегічний план впровадження цифровізації сил ЄС. Визначено, що майже всі витрати федерального уряду США на штучний інтелект спрямовані на професійні, технічні та наукові послуги, з яких 87 відсотків вартості контракту припадає на Міністерство оборони.

Ключові слова: *цифрова трансформація, публічне управління, сфера оборони, безпека, цифровізація.*

The author emphasized that Israel is a pioneer in the field of digitalization, but it was this country that launched digital innovations in the IDF. It is shown that the sense of urgency of modernization of the German Armed Forces follows from the changed structure of security policy. Countries are being forced to move forward with innovation to be able to continue to provide security. It is noted that NATO and the EU have also begun the process of digital defense transformation. Thus, in 2022 and 2023, NATO adopted its first-ever digital transformation vision and digital transformation strategy, and the EU approved the Strategic Plan for Implementing Digitalization of EU Forces. It is determined that almost all the costs of the US federal government on artificial intelligence are aimed at professional, technical and scientific services, of which 87 percent of the contract cost comes from the Department of Defense.

Keywords: *digital transformation, public management, defense, security, digitalization.*

Постановка проблеми. У XXI столітті цифровізація відіграє все більш центральну роль у воєнних операціях. Це включає використання дронів та інших дистанційно керованих систем, а також інтеграцію цифрових систем в озброєння та інше обладнання. Крім того, військові широко використовують цифрові платформи та мережі для зв'язку, координації та обміну інформацією.

Загалом, історія цифровізації у збройних силах – це постійна еволюція та адаптація до нових технологій та зміни стратегічних потреб. У міру просування цифрових технологій роль цифровізації у військовій сфері буде продовжувати розвиватися, і саме це обумовлює актуальність обраної теми дослідження.

Аналіз останніх досліджень і публікацій. Переважна кількість вітчизняних і закордонних авторів уважають, що технологічні інновації змінюють війну і підштовхують до інновацій, до переосмислення стратегічних, оперативних і тактичних рішень, які піднімають нові питання морального і правового впливу. Технічний прогрес тільки зміцнить поліцентричну систему у воєнних технологіях. Штучний інтелект, зростаюча роль кібер- та інформаційних елементів, безпілотні системи, 3D друк та зміна сили бою – усі ці складові є вкрай необхідними для адаптації сфери оборони малих держав до нових реалій. У цьому зв’язку дослідження закордонного досвіду публічного управління у воєнній сфері слід вважати недостатньо розвиненими з тим, щоб їх можна було повноцінно імплементувати у вітчизняну практику.

Постановка завдання. Не применшуючи напрацювань та наукових досягнень зазначених вчених, відзначимо, що існує необхідність в розробці інтерактивної моделі публічного управління знаннями у соціальній групі.

Відповідно, метою даної статті є дослідження закордонного досвіду публічного управління цифровізацією у воєнній сфері. Зазначена мета передбачає вирішення низки відповідних завдань:

1) порівняти стан цифіровізації в оборонній сфері Ізраїлю та Німеччини;

2) виокремити поточні тенденції у процесах цифрової трансформації оборонного планування в ЄС та НАТО;

3) оцінити стан державного впровадження передових цифрових технологій в США для забезпечення оборонної діяльності.

Виклад основного матеріалу. Ізраїль є піонером у сфері цифровізації. Особливо це стосується сфери оборони. У 2017 році Кіберінноваційний центр Бундесверу Збройних сил Німеччини став першим цифровим інноваційним підрозділом, створеним німецьким міністерством. Він був започаткований як каталізатор і рушійна сила цифрових інновацій в Армії Оборони Ізраїлю [1; 3].

З моменту заснування Кіберінноваційного центру Бундесверу Збройних сил Німеччини у 2017 році вже було запущено понад 140 інноваційних проектів.

Такий темп відображає нові соціальні реалії 21 століття. Цифрова революція збільшила швидкість, з якою інновації виходять на ринок. Водночас, однак, швидкість, з якою повинні прийматися рішення у воєнній сфері, також зросла. У цьому відношенні країни зі структурними проблемами у впровадженні цифрових інновацій особливо змушені діяти [2; 5].

Німеччина теж стикається з такими викликами. Протягом десятиліть було накопичено величезну кількість знань про те, як керувати процесами та підтримувати їх рух. На жаль, цифрові інновації здебільшого є руйнівними та кидають виклик саме цим знанням. Нові процеси займають місце старих усталених структур, які стають зайвими і втрачають сенс [1; 5].

У більшості випадків потрібен імпульс, щоб поставити під сумнів давно сформовані структури. Такий момент стався 24 лютого 2022 року. Початок загарбницької війни Росії проти України знаменує собою "Zeitenwende", поворотний момент у часі. Відчуття терміновості модернізації Збройних сил Німеччини випливає зі зміненої структури політики безпеки. Країни змушені просуватися вперед з інноваціями, щоб мати можливість продовжувати забезпечувати безпеку.

На цьому тлі Ізраїль є хорошим прикладом, який може дати орієнтир. Десятиліттями стикаючись з відчуттям безпосередньої загрози, цифрова трансформація відбувалася там надзвичайно швидко, особливо в оборонному секторі. Однією з причин цього було те, що Ізраїль мав реагувати на нові сценарії загроз у кіберпросторі, які йдуть рука об руку з цифровою трансформацією. Сьогодні набагато менш розвинуті в промисловому відношенні країни та недержавні суб'єкти можуть завдати великої шкоди за допомогою кіберзброї. І чим менш розвинена технологія країни-мішені щодо опору потенційної кібератаки, тим більшою може бути шкода. У цьому зв'язку корисною є співпраця оборонного сектору зі стартапами [2; 6].

Зрештою, всесвітньо відомий сектор високих технологій Ізраїлю завжди був пов'язаний з оборонним сектором, не в останню чергу через жвавий обмін персоналом. Важливим поштовхом стало заснування в 1970 році Ізраїльського промислового центру досліджень і розробок командувачем Армії оборони Ізраїлю, до якого у 2016 році було додано Ізраїльське управління інновацій. Сьогодні Ізраїль має найвищу щільність стартапів на душу населення. Дослідження показують, що в цьому інноваційному середовищі як воєнний, так і цивільний сектори взаємно виграють один від одного. Саме це середовище та ці можливості також потрібні нам в Україні, щоб стимулювати цифровізацію в оборонному секторі.

НАТО та ЄС також розпочали процес цифрової трансформації оборони. У 2022 та 2023 роках НАТО прийняла своє перше в історії бачення цифрової трансформації та стратегію реалізації цифрової трансформації, а ЄС схвалив Стратегічний план впровадження цифровізації сил ЄС, інтегрованих кібер-

ефектів у воєнних операціях ЄС та визначив пріоритет цифрових можливостей у рамках четвертої основи (інвестиції) свого Стратегічного компасу. Залежно від галузевих стратегій, різні елементи цифрової трансформації, включаючи дані, хмарні застосунки та Інтернет речей, все більше пов'язані, забезпечуючи цифровізацію оборони як засіб, що сприяє багатодоменним операціям та оборонним інноваціям завдяки застосуванню нових та революційних технологій [3; 4; 7].

Цифрова трансформація тягне за собою глибокі соціально-технологічні та організаційні зміни. Ініціативи цифрової трансформації в НАТО та ЄС мають позитивний вплив, оскільки європейські уряди йдуть шляхом поступової оптимізації цифрових можливостей до 2030-х років. Європейська безпека виграє від обміну найкращими практиками щодо цифрової трансформації, встановлення спільних технічних стандартів і політики обміну даними, а також координації вимог до цифрових можливостей і цілей у оборонному плануванні.

Масштаби цифрової трансформації є амбітними як в НАТО, так і в ЄС. Вони включають технологічну, організаційно-процесуальну та людську основи трансформації та визначають пріоритети даних та хмарні оновлені підходи до кібербезпеки. Однак реалізації перешкоджають довгі часові рамки для цифрової трансформації (до 2030-х років), відсутність прогресу в ключових процедурних компонентах (зокрема, закупівлі та узгодження бюджету), проблеми, пов'язані з суверенітетом даних і доступністю, а також постійні недостатні інвестиції в цифрові можливості для оборони по всій Європі. Якщо в усіх цих сферах не відбудуться серйозні зміни в короткостроковій перспективі, і НАТО, і ЄС навряд чи досягнуть своїх віх цифрової трансформації до 2030 року [1; 5].

Сучасні політики в США готові усунути розрив між приватним і державним впровадженням передових технологій, перш за все заради захисту нації та її людей – найвищого обов'язку уряду.

Інтерес до передових технологій найбільший у міністерствах оборони, енергетики, внутрішньої безпеки та фінансів, а також у розвідувальній спільноті та NASA. Бюджет Міністерства оборони на дослідження та розробки збільшується на 10 відсотків на рік і зріс на колосальні 20 мільярдів доларів США до 137 мільярдів доларів з 2022 по 2023 рік. Заявлена мета цих інвестицій полягає в забезпеченні переваги в морі, повітрі та космосі Збройних сил США.

У той же час безпека комп'ютерних систем, мереж і пристроїв від кібератак державних і недержавних хакерів, іноземних і вітчизняних, також набуває все більшого значення для громадськості, а отже і для уряду, який зараз витрачає 10 мільярдів доларів на кібербезпеку. Забезпечення цілісності соціальних медіа від маніпуляцій з боку ворожих акторів також стало питанням національної безпеки. Відстеження та передбачення переміщень людей, нар-

котиків і екстремальних погодних умов є як ніколи важливими для громадської безпеки [2; 6; 7].

Перед обличчям цих небезпек особливо важливі три «постцифрові» технології: звичайно, штучний інтелект; квантові обчислення та комунікації; і мережеві супутникові системи. Кожен із них за своєю суттю має подвійне призначення, має високу комерційну цінність і потенціал для посилення національної безпеки.

Тим не менш, у звіті Брукінгса за 2022 рік було виявлено, що державний ринок штучного інтелекту залишається незрілим, але, швидше за все, буде швидке зростання. Майже всі витрати федерального уряду на штучний інтелект спрямовані на професійні, технічні та наукові послуги, з яких 87 відсотків вартості контракту припадає на Міністерство оборони.

Висновки. Таким чином, цифровізація чинить значний вплив на сучасну війну кількома способами:

1) підвищена залежність від технологій. Сучасна війна часто передбачає використання передових технологій, таких як дрони, датчики та високоточна зброя. Ці технології покладаються на цифрові системи та мережі, вразливі до кібератак або зривів;

2) кібервійна: Цифровізація також породила нову форму війни: кібервійну. Це передбачає використання кібер-атак для порушення або виведення з ладу ворожих систем, таких як мережі зв'язку або військова техніка;

3) збір розвідувальної інформації. Цифрові системи та мережі можуть збирати інформацію про сили противника, включаючи їх розташування, переміщення та можливості. Це може дати збройним силам значну перевагу в плануванні та виконанні операцій;

4) інформаційні операції. Цифрові платформи, такі як соціальні медіа, можуть бути використані для поширення пропаганди та впливу на громадську думку. Це може бути потужним інструментом для збройних сил, але це також створює потенціал для дезінформації та маніпуляцій;

5) підвищений рівень автоматизації. Цифровізація дозволила автоматизувати багато завдань, які раніше виконували люди, включаючи деякі аспекти воєнних операцій. Це може підвищити ефективність і знизити ризик для людського життя, але це також викликає занепокоєння щодо ролі людини в процесах прийняття рішень.

Список використаних джерел:

1. Єпіфанова І., Оранська Н. Сутність антикризового управління підприємством. *Економіка і суспільство*. 2016. № 2. С. 265–269.

2. Кічурчак М. Вплив сектору інформації та комунікації на просторовий розвиток і пост-воєнну відбудову креативних індустрій в економіці України. *Економічний форум*. 2023. № 1(3), С. 12-21.

3. Скалецька З. Захист прав споживачів: виклики воєнного часу та потенційні зміни в рамках євроінтеграційних процесів. *Академічні візії*. 2022. № 12. URL: https://academy-vision.org/index.php/av/article/view/230.

4. Шпарик О. Концептуальні засади цифрової трансформації освіти: європейський та американський дискурс. *Український Педагогічний журнал*. 2021. № (4). С. 65-76.

5. Abke T. Digitalization in the Armed Forces. 2023. URL: https://www.linkedin.com/pulse/digitalization-armed-forces-tom-abke.

6. Brunetti F., Matt D.T., Bonfanti A., De Longhi A., Pedrini G., Orzes G. Digital Transformation Challenges: Strategies Emerging from a Multi-Stakeholder Approach. The TQM Journal. 2020. Vol. 32. Issue 4. P. 697-724.

7. Verina N., Titko J. Digital transformation: conceptual framework. In Contemporary Issues in Business. *Management and Economics Engineering*. 2019. P. 719-727.

References:

1. Abke T. Digitalization in the Armed Forces. 2023. URL: https://www.linkedin.com/pulse/digitalization-armed-forces-tom-abke.

2. Brunetti F., Matt D.T., Bonfanti A., De Longhi A., Pedrini G., Orzes G. Digital Transformation Challenges: Strategies Emerging from a Multi-Stakeholder Approach. *The TQM Journal*. 2020. Vol. 32. Issue 4. P. 697-724.

3. Jepifanova, I., Oransjka, N. Sutnistj antykryzovogho upravlinnja pidpryjemstvom [The essence of anti-crisis management of the enterprise]. *Ekonomika i suspiljstvo*. 2016. Vol. 2, P. 265-269.

4. Kichurchak M. Vplyv sektoru informatsii ta komunikatsii na prostorovyi rozvytok i post-voiennu vidbudovu kreatyvnykh industrii v ekonomitsi Ukrainy [Impact of the information and communication sector on spatial development and post-military reconstruction of creative industries in the Ukrainian economy]. *Ekonomichnyi forum*. 2023.Vol. 1(3), P. 12-21.

5. Shparyk O. Kontseptualni zasady tsyfrovoi transformatsii osvity: yevropeiskyi ta amerykanskyi dyskurs. [Conceptual roundations of digital transformation of education: European and American discourse]. *Ukrainskyi Pedahohichnyi zhurnal*. 2021. № (4). S. 65-76.

6. Skaletska Z. Zakhyst prav spozhyvachiv: vyklyky voiennoho chasu ta potentsiini zminy v ramkakh yevrointehratsiinykh protsesiv [Consumer protection: wartime challenges and potential changes in the framework of European integration processes]. *Akademichni vizii*. 2022. № 12. URL: https://academy-vision.org/index.php/av/article/view/230.

7. Verina N., Titko J. Digital transformation: conceptual framework. In Contemporary Issues in Business. *Management and Economics Engineering*. 2019. P. 719-727.