УДК 331.108:355

Бондаренко С.А.
професор кафедри соціоекономіки
та управління персоналом
Київський національний економічний університет
імені Вадима Гетьмана

ЦИФРОВА ТРАНСФОРМАЦІЯ ПРАЦІ В СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ: ВИКЛИКИ ТА МОЖЛИВОСТІ КОНЦЕПЦІЇ ПРАЦІ 5.0

Глобальна трансформація промисловості від Індустрії 4.0 до Індустрії 5.0 знаменує перехід від повністю автоматизованих систем до людиноцентричного підходу, що поєднує когнітивні можливості штучного інтелекту (далі — ШІ) з людською креативністю та гнучкістю мислення.

Концепція Праці 5.0, що базується на принципах Суспільства 5.0, передбачає створення екосистеми, де передові технології вирішують соціальні проблеми при збереженні людини в центрі організаційних процесів та людино-орієнтованих рішень для забезпечення довгострокового успіху на індивідуальному та суспільному рівнях [1]. Сектор безпеки і оборони України потребує термінової модернізації в контексті сучасних викликів національної безпеки, оскільки воєнні конфлікти останніх років демонструють критичну необхідність впровадження цифрових технологій при одночасному збереженні людського фактору як ключового елементу оборонної спроможності. Інтеграція технологій Праці 5.0 у військову сферу дозволяє досягти синергії між автоматизацією процесів та унікальними людськими компетенціями — аналітичним мисленням, творчістю та адаптивністю [2].

Сучасні системи безпеки та оборони перебувають на етапі радикальної технологічної трансформації, де ключову роль відіграють ШІ, кібербезпека та інтелектуальні сенсорні мережі. Людино-орієнтований ШІ в Індустрії 5.0 забезпечує ефективну співпрацю людини та робота, пропонуючи інтелектуальні компоненти для точного та людиноцентричного прийняття рішень у виробничих процесах. При цьому ШІ сприяє своєчасному та точному реагуванню, реалізації концепції масової персоналізації та захисту від кіберзагроз через інтелектуальні методи кіберзахисту [2]. Системи на основі глибоких нейронних мереж здатні оброб-

ляти величезні обсяги даних, виявляючи приховані закономірності та потенційні загрози в режимі реального часу, проте вони демонструють вразливість, що вимагає розробки надійних методів захисту. Метод глибокого злиття, що поєднує множинні прогнози з моделями ерозії, підвищує стійкість моделі до ворожих атак більш ніж на 90 % [3].

У цьому контексті особливого значення набуває розвиток систем кібербезпеки критичної інфраструктури, адже традиційні периметрорієнтовані моделі безпеки виявилися неефективними проти сучасних складних кібератак, що вимагає переходу до архітектури нульової довіри. Концепція нульової довіри для промислових систем Інтернету речей демонструє ефективність комплексного підходу, що поєднує криптографічну автентифікацію з симетричною криптографією для взаємної верифікації пристроїв, при цьому впровадження цього підходу дозволяє знизити обчислювальну складність на 12,5 % та комунікаційні витрати на 14,29 % порівняно з традиційними методами [4]. Паралельно з розвитком систем кібербезпеки відбувається еволюція технологій моніторингу та управління критичною інфраструктурою, що знаходить своє відображення у створенні багатодоменних кібер-фізичних тестових платформ на базі моделі архітектури розумних мереж, які дозволяють оцінювати вразливості енергетичних систем до п’яти найпоширеніших типів кібератак, включаючи розвідку, атаки на відмову в обслуговуванні, ін’єкції пакетів та атаки типу «людина посередині» [5].

Інтеграція зазначених технологій створює основу для впровадження концепції цифрових двійників та систем екстреного реагування, що дозволяють створювати віртуальні копії фізичних об’єктів для моніторингу, прогнозування та оптимізації їх роботи в режимі реального часу. Системи управління надзвичайними ситуаціями у критичній інфраструктурі використовують дані від IoT-пристроїв, носимих датчиків та дронів для моніторингу подій, при цьому застосування технологій змішаної реальності для рятувальників та можливість анотування карти двовимірними і тривимірними об’єктами для операторів покращують ситуаційну обізнаність та координацію дій при реагуванні на інциденти [6].

Попри стрімкий розвиток технологій автоматизації, концепція Праці 5.0 наголошує на центральній ролі людини у виробничих та оборонних процесах, що знаходить своє відображення у переосмисленні стратегій управління талантами та розвитку персоналу. Концепція Суспільства 5.0 підкреслює необхідність кардинального переосмислення управління талантами у контексті цифрової трансформації, оскільки традиційні підходи до управ-

ління персоналом в оборонній сфері повинні еволюціонувати для залучення та утримання фахівців з критичними компетенціями у галузі ШІ, кібербезпеки та аналізу даних [1]. Ефективне залучення талантів вимагає гнучких стратегій, що враховують специфіку різних секторів — від оборонної промисловості до транспорту та розумних міст, створюючи єдину екосистему розвитку компетенцій, яка дозволяє формувати міждисциплінарні команди, здатні вирішувати комплексні виклики національної безпеки. Гібридний інтелект, що передбачає поєднання людської експертизи з обчислювальною потужністю машин, дозволяє досягти синергетичного ефекту у вирішенні складних завдань, що підтверджується досвідом фінансового сектору, де така інтеграція дозволила підвищити точність виявлення шахрайства на 30 % порівняно з повністю автоматизованими системами [7].

Паралельно з розвитком професійних компетенцій, критичного значення набуває комплексна підтримка здоров'я та реабілітації військовослужбовців, що є невід'ємною складовою людиноцентричного підходу Праці 5.0. Професійна реабілітація військовослужбовців з посттравматичним стресовим розладом (далі — PTSD) потребує інтегрованого підходу, що поєднує освітні програми, працевлаштування та забезпечення економічної незалежності. П'ятирічне проспективне спостереження за 462 ветеранами Сил оборони Ізраїлю з PTSD показало, що освітня реабілітація є найефективнішою, підвищуючи шанси інтеграції у робочу силу у 19,5 разів порівняно з іншими методами, при цьому регресійний аналіз підтвердив, що тривалість освітньої програми прямо корелює з успішністю професійної реінтеграції [8]. Важливо зазначити, що 87,9 % учасників дослідження мали також супутні фізичні травми, отримані під час військової служби, що підкреслює необхідність комплексного підходу до реабілітації, який враховує як психологічні, так і фізичні аспекти здоров'я [8]. Впровадження превентивних програм на базі носимих сенсорів та систем прогнозування ризиків на основі ШІ може знизити рівень травматизму через раннє втручання та персоналізовані тренувальні режими, оптимізуючи баланс між підготовкою та збереженням здоров'я, що демонструє практичне застосування принципів Індустрії 5.0 у сфері військової медицини.

Успішна імплементація концепції Праці 5.0 у секторі безпеки і оборони вимагає не лише технологічних інновацій, але й стратегічного підходу до фінансування та організаційних змін. Оптимізація військових активів, розвиток партнерств оборонної промисловості та державно-приватне партнерство представляють

життєздатні альтернативи традиційному бюджетуванню, проте впровадження цих механізмів вимагає правових реформ для відповідності існуючим рамкам, включаючи законодавство про державні фінанси та національну оборону. Концепція Індустрії 5.0 наголошує на сталому розвитку як основному принципі, що транслюється у підходи циркулярної економіки в оборонному секторі, включаючи реманіфактуринг озброєнь, переробку стратегічних матеріалів та мінімізацію відходів, при цьому технології вилучення критичних металів з промислових шлаків демонструють потенціал використання вторинних ресурсів, знижуючи залежність від імпорту стратегічних матеріалів.

Впровадження концепції Праці 5.0 у секторі безпеки і оборони України є не просто технологічним викликом, але комплексною трансформацією, що охоплює організаційні, соціальні та економічні аспекти. Людиноцентричний підхід підкреслює важливість інвестицій у людський капітал через комплексні програми реабілітації для військовослужбовців з акцентом на розвиток цифрових навичок, що забезпечують успішний перехід до цивільного ринку праці високотехнологічного сектору.

СПИСОК ЛІТЕРАТУРИ

1. Atay, S., Müftüoğlu, C. T., Gülmez, N., & Şahin, M. (2025). Society 5.0 and human-centered technology: Redefining talent management in the digital age. *Sustainable Futures*, 9, 100733. https://doi.org/10.1016/j.sftr.2025.100733.
2. Khosravy, M., Gupta, N., Pasquali, A., et al. (2024). Human-collaborative artificial intelligence along with social values in Industry 5.0: A survey of the state-of-the-art. *IEEE Transactions on Cognitive and Developmental Systems*, 16(1), 165–176. https://doi.org/10.1109/TCDS.2023.3326192.
3. Wang, Y., Tan, Y.-A., Baker, T., et al. (2023). Deep fusion: Crafting transferable adversarial examples and improving robustness of industrial artificial intelligence of things. *IEEE Transactions on Industrial Informatics*, 19(6), 7480–7488. https://doi.org/10.1109/TII.2022.3168874.
4. Verma, R., & Indra, G. (2024). ZAIA: Zero-trust authentication and identity attestation framework for AI-enabled IIoTs in smart manufacturing ecosystem. *In 2024 IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies*, 1–6. https://doi.org/10.1109/INSPECT63485.2024.10896155.
5. Mishchenko, D., Oleinikova, I., Erdodi, L., & Pokhrel, B. R. (2024). Multidomain cyber-physical testbed for power system vulnerability assess-

ment. *IEEE Access*, 12, 38135–38149. https://doi.org/10.1109/ACCESS.2024.3375401.

6. De Felice, F., Cannito, A. R., Noviello, P., & Crosta, P. S. (2026). XCOP: An integrated solution for emergency management during incidents in critical infrastructures. *Lecture Notes in Computer Science*, 15740. https://doi.org/10.1007/978-3-031-97772-5_8.

7. Hybrid AI-human models sharpen fraud response. (2025). *PYMNTS.com.* https://www.pymnts.com/news/artificial-intelligence/2025/hybrid-ai-human-models-sharpen-fraud-response.

8. Segev, D., Schiff, M., & Shelef, L. (2024). Occupational rehabilitation of Israel Defense Forces veterans with PTSD: A 5-year follow-up. *International Journal of Psychology*, 59(6), 1064–1074. https://doi.org/10.1002/ijop.13231.