DOI: https://doi.org/10.32782/2524-0072/2024-65-60

УДК 004.9: 351.861

ЦИФРОВА ТРАНСФОРМАЦІЯ В КОНТЕКСТІ ГІБРИДНИХ ЗАГРОЗ[1]

DIGITAL TRANSFORMATION IN THE CONTEXT OF HYBRID THREATS

Карпенко Оксана Олександрівна
доктор економічних наук, професор, професор кафедри,
Заклад вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая»
ORCID: https://orcid.org/0000-0003-2943-1982

Осипова Євгенія Леонідівна
кандидат економічних наук, доцент, доцент кафедри,
Державний університет інфраструктури та технологій
ORCID: https://orcid.org/0000-0003-3266-1164

Матвійчук Євгеній Ігорович
здобувач третього (освітньо-наукового) рівня вищої освіти,
Державний університет інфраструктури та технологій
ORCID: https://orcid.org/0009-0007-4650-9936

Karpenko Oksana
Higher Educational Institution «Academician Yuriy Bugay International Scientific and Technical University»

Osypova Yevheniia, Matviichuk Yevhenii
State University of Infrastructure and Technologies

Цифрова трансформація є однією з ключових тенденцій сучасного світу, яка суттєво впливає на всі сфери життя: економіку, суспільство, державне управління, оборону і безпеку. У статті виявлено основні ризики суспільству, які несе цифрова трансформація. Визначено, що інформаційні технології стали одним з основних інструментів гібридних загроз. Охарактеризовано етапи розвитку технологій ШІ та сфери потенційного впливу ШІ на розвиток обороноздатності країн світу протягом наступних 20 років. Цифрова трансформація значно посилює ризики гібридних загроз. Завдяки швидкому розвитку інформаційних технологій, гібридні загрози можуть завдати значної шкоди на національному та міжнародному рівнях. Для успішної протидії гібридним загрозам, що викликані процесом цифрової трансформації, необхідно розробляти і впроваджувати комплексні стратегії, що поєднують кібербезпеку, боротьбу з дезінформацією, зміцнення національної стійкості та міжнародне співробітництво.

Ключові слова: цифрова трансформація, гібридні загрози, новітні та проривні технології – EDTs, штучний інтелект, блокчейн, квантові обчислення, 5G/6G, Big Data, інтернет речей, підроблення, deepfake, створення аватару.

Digital transformation is one of the key trends in the modern world, which has a significant impact on all spheres of life: economy, society, public administration, defense and security. The United Nations recognizes digitalization as one of the main dangers facing humanity. In the article the main risks to society posed by digital transformation are identified. The threats of economic, political, social, technological, and control nature are characterized. The development of Emerging and Disruptive Technologies – EDTs, such as artificial intelligence, blockchain, quantum computing, 5G/6G, Big Data, the Internet of Things, and others, should be assessed from both a positive and negative perspective in terms of their impact on society and the economy. It is determined that information

[1] Стаття підготовлена на основі матеріалів проєкту WARN «Академічна протидія гібридним загрозам» (610133-EPP-1-2019-1-FI-EPPKA2-CBHE-JP), що співфінансується програмою Erasmus+ Європейського Союзу. Підтримка Європейською Комісією у створення матеріалів, розміщених в статті, не є схваленням змісту, який відображає погляди лише авторів, і Комісія не несе відповідальності за будь-яке використання інформації, що міститься в ній.

technologies have become one of the main tools of hybrid threats. Artificial intelligence (AI) is a rapidly developing area of technologies with potentially significant implications for national security. The stages of development of AI technologies and the areas of potential impact of AI on the development of defense capabilities of countries over the next 20 years are characterized. Digital transformation significantly increases the risks of hybrid threats. Due to the rapid development of information technology, hybrid threats can cause significant damage at the national and international levels. For example, cyber attacks on critical infrastructure can lead to serious disruptions in the functioning of the state, disinformation can provoke social conflicts, and economic pressure can undermine the resilience of economies. All these factors create new challenges for national security and require new approaches to neutralize them. To successfully counter hybrid threats caused by the digital transformation process, it is necessary to develop and implement comprehensive strategies that combine cybersecurity, countering disinformation, strengthening national resilience and international cooperation. This is the only way to ensure security and stability in the digital age.

Keywords: Digital Transformation, Hybrid Threats, Emerging And Disruptive Technologies – Edts, Artificial Intelligence, Blockchain, Quantum Computing, 5G/6G, Big Data, Internet of Things, Forgery, Deepfake, Avatar Creation.

Постановка проблеми. Цифрова трансформація є однією з ключових тенденцій сучасного світу, яка суттєво впливає на всі сфери життя: економіку, суспільство, державне управління, оборону і безпеку. Водночас з розвитком цифрових технологій виникають нові виклики, серед яких особливе місце займають гібридні загрози. Тому актуальність дослідження розвитку цифрової трансформації та технологій штучного інтелекту в контексті гібридних загроз потребує особливої уваги.

Аналіз останніх досліджень і публікацій. Аналіз літературних джерел з даної тематики показав, що науковці більш розглядають питання позитивного впливу цифрової трансформації на всі сфери життя. Проте є ряд авторів, які досліджували також і негативний вплив цифровізації [1–3].

Виділення невирішених раніше частин загальної проблеми. Незважаючи на ряд відомих на сьогодні теоретичних та практичних напрацювань тематика ідентифікації великої кількості ризиків, які супроводжують процеси цифрової трансформації в контексті протидії гібридним загрозам, на наш погляд, залишається ще недостатньо дослідженою.

Метою статті є виявлення основних ризиків суспільству, що несе цифрова трансформація, зокрема з використанням штучного інтелекту, та розробка відповідних рекомендацій для забезпечення протидії гібридним загрозам.

Виклад основного матеріалу дослідження. Цифрова трансформація – це процес переходу від традиційних методів управління та виробництва до використання сучасних цифрових технологій. Найперспективнішими напрямками розвитку ІТ-сфери в найближчому майбутньому є: штучний інтелект, хмарні технології, технологія блокчейн, інформаційно-комунікаційні технології, великі дані, обчислювальна пам’ять, чат-боти, кібербезпека, розпізнавання мови, цифровий зв’язок, комп’ютерні мережі, ІТ методів управління [4]. При цьому необхідно пам'ятати про виклики та ризики, пов'язані з цифровою трансформацією.

У доповіді ОЕСР зазначено, що «цифрові технології можуть мати деструктивний характер, що в майбутньому негативно позначиться на продуктивності, зайнятості і добробуті, а також, що вони можуть посилити диспропорції в рівні їх доступності та використання, і привести до формування нового цифрового розриву й зростання нерівності» [5].

ООН також визнає цифровізацію як одну з головних небезпек, що загрожують людству [6]. «Темний» бік цифрового світу полягає в тому, що технологічні досягнення рухаються швидше, ніж здатність людства реагувати на них або навіть розуміти їх. Крім того, нові технології використовуються для вчинення злочинів, розпалювання ненависті, фальсифікації інформації, утисків і експлуатації людей і втручання у приватне життя [3].

Основні загрози в сфері цифровізації економіки можна розподілити за характером (рис. 1).

Цифровізація проявляється в докорінних перетвореннях в усіх сферах життя, при цьому її вплив на розвиток суспільства є суперечливим, про що свідчить велика кількість загроз, які вона породжує.

Розвиток новітних та проривних технологій (Emerging and Disruptive Technologies – EDTs), таких як штучний інтелект, блокчейн, квантові обчислення, 5G/6G, Big Data, інтернет речей та інші, доцільно розглядати та оцінювати їх позитивний і негативний вплив на суспільство. Цифрова трансформація супроводжується процесом посилення зв’язків між системами та збільшенням обсягів інформації, що зберігається та оброблюється. Такі процеси можуть призводити одночасно як до зміцнення економіки та збільшення ефективності

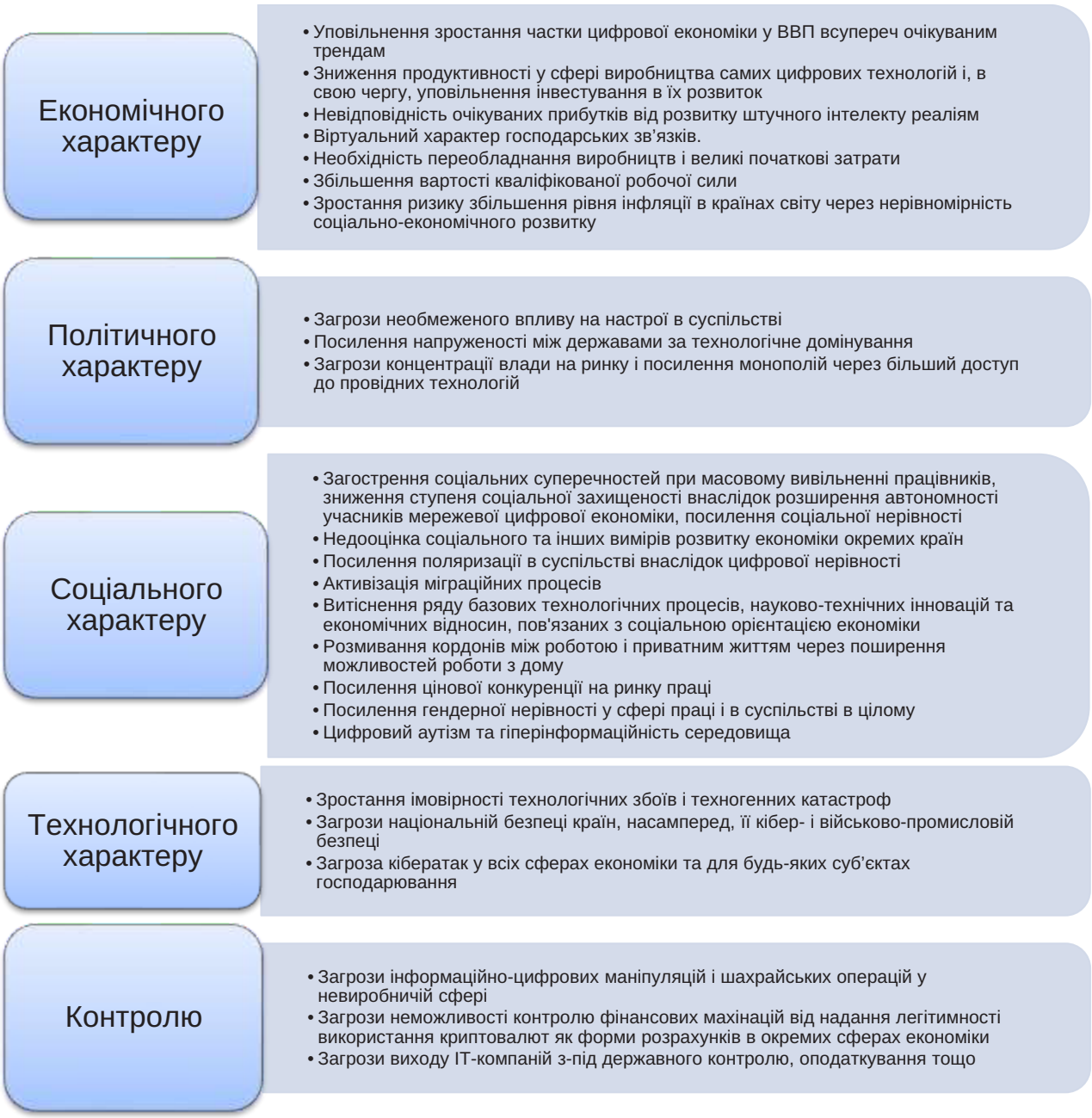

Рис. 1. Загрози та ризики суспільству, що несе цифровізація

Джерело: сформовано на основі [1]

окремих систем, так і до створення додаткових вразливостей, які можуть бути використані для різного роду атак [7].

Основними викликами, з якими стикається світ у світлі розвитку EDTs та цифрової трансформації, є забезпечення отримання суспільством вигоди від потужніших, швидших та взаємопов'язаних обчислень та процесів при одночасному відстеженні відповідального використання нових технологій та чіткому переконанні, що це не призводить до зростання вразливості безпеки.

Сьогодні, коли інформаційні технології розвиваються шаленими темпами, вони стають, нажаль, одним з основних інструментів гібридних загроз. За допомогою інформаційних технологій можна швидко розповсюджувати будь-яку інформацію. Справжня небезпека виникає, коли ця інформація не правдива. На арену створення неправдивої інформації виходить багато комп'ютерних інструментів, зокрема штучний інтелект (ШІ).

Коротка характеристика етапів розвитку ШІ наведена на рис. 2.

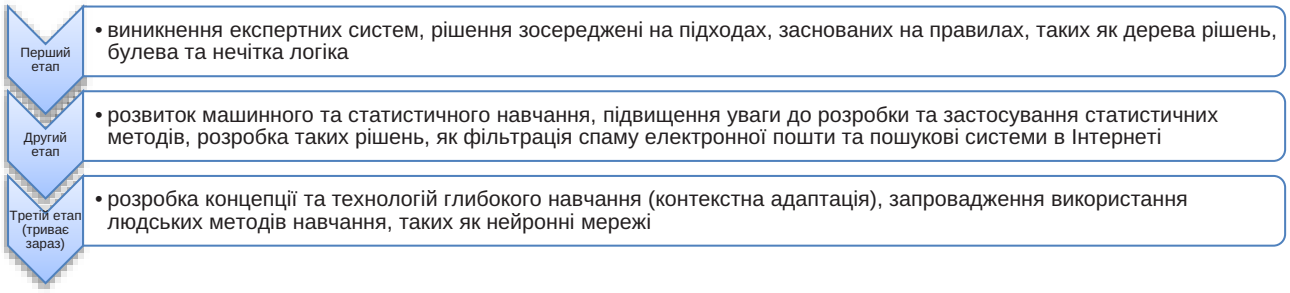

Рис. 2. Коротка характеристика етапів розвитку технологій ШІ

Джерело: сформовано на основі [2]

Штучний інтелект є перспективним інструментом в гібридній війні. І вже сьогодні він може створювати велику загрозу. Можна виділити такі можливості, які використовуються в інформаційних кампаніях: підроблення фото, підроблення звуку, підроблення відео, deepfake (комбінація попередніх пунктів) чи створення аватару. Аватар – це певне зображення чи анімація, основною метою якого є проникнення в конкретну спільноту для маніпулювання. Створення аватару (цифрового аватару) відбувається на основі аналізу великої кількості даних (характеристик) цільової аудиторії. Підроблення фото, звуку та відео самі по собі не дуже цікаві, а ось їхня комбінація, а саме deepfake, дуже цікаве явище. Deepfake, як правило, використовує образ публічної людини (адже багато вихідних даних можна легко знайти). Основною метою deepfake є створення неправдивої картинки для того, щоб людина говорила те, щоб точно ніколи не сказала або зобразити лідера жорстким/слабким/брехливим (на свою користь). Тобто основною метою deepfake є дискредитація певної особи перед його цільовою аудиторією [8].

Штучний інтелект (ШІ) – це сфера технологій, що швидко розвивається і має потенційно значні наслідки для національної безпеки. Тому Сполучені Штати та деякі інші країни розробляють програми ШІ для цілого ряду військових функцій. Дослідження ШІ ведуться в таких сферах, як збір і аналіз розвідданих, логістика, кібероперації, інформаційні кампанії, командування і управління, а також у різноманітних напівавтономних і автономних транспортних засобах. ШІ вже застосовувався у військових операціях в Іраку і Сирії. Потенційні міжнародні конкуренти на ринку ШІ тиснуть на Сполучені Штати, змушуючи їх конкурувати у сфері інноваційних військових застосувань ШІ. Провідним конкурентом у цьому відношенні є Китай, який у 2017 році оприлюднив план захоплення світового лідерства у розробці ШІ до 2030 року. Наразі Китай, насамперед, зосереджений на використанні ШІ для прийняття швидших і більш обґрунтованих рішень, а також на розробці різноманітних автономних військових транспортних засобів [9].

У роботах [2; 10] викладено інформацію про основні сфери потенційного впливу ШІ на розвиток обороноздатності країн світу протягом наступних 20 років (рис. 3).

Штучний інтелект на сьогоднішній день хоч й не може мислити, але все ж таки завдяки складним евристичним алгоритмам може вирішувати складноформалізовані задачі. Цих можливостей штучного інтелекту достатньо, щоб працювати не на користь людям та бути потужнім інструментом для гібридної загрози.

Організація Науки та Технологій при НАТО висловила думку, що EDTs важливі для безпеки у майбутньому з наступних причин [7; 10]:

– використання штучного інтелекту може забезпечити більш повну та глибоку аналітичну картину поля бою;

– взаємозв’язок – мережі датчиків і зв’язок між ними можуть забезпечити ефективне підключення на полі бою;

– розподіл – перехід до децентралізованого збору та аналізу даних може надати підрозділам більшу автономію на полі бою;

– оцифрування – більш зручний та швидкий доступ до інформації допомагає швидше реагувати на поточну ситуацію.

Швидкі темпи цифрової трансформації, розвиток EDTs потребують реагування таких організацій, як ЄС та НАТО, та їх країн-партнерів [7; 8]:

– особи, які приймають рішення, не повинні зосереджуватися виключно на траєкторії окремих EDTs. Необхідно, щоб будь-яка

Рис. 3. Сфери потенційного впливу ШІ на розвиток обороноздатності країн світу протягом наступних 20 років та їх характеристика

Джерело: сформовано на основі [2; 10]

оцінка EDTs проводилась в ширшому контексті цифровізації, основними ознаками якої є взаємозв'язок систем, централізація даних та децентралізація використання даних;

– ЄС і НАТО мають продовжувати зосереджуватися на підтримці та забезпеченні цифрової трансформації й комунікувати щодо загроз і викликів, які можуть з'являтись на горизонті;

– один із головних методів підготовки до протидії вразливостям безпеки, викликаним цифровізацією, є планування низки спільних навчань і підвищення обізнаності про ситуацію;

– існує нагальна потреба подолати велику прірву між швидким технологічним розвитком і ресурсною базою збройних сил, оновити доктрини та процеси операцій впливу та протидії впливу в інформаційній сфері, підготувати спеціальний персонал для отримання необхідних знань, щоб протидіяти сучасній інформаційній війні.

Для ефективної протидії гібридним загрозам у цифрову епоху необхідно впроваджувати комплексні заходи, що включають наступні елементи:

– розвиток кібербезпеки шляхом створення ефективних систем захисту від кібератак, навчання персоналу та впровадження сучасних технологій захисту даних;

– протидія дезінформації шляхом використання методів медіаграмотності, проведення інформаційних кампаній для підвищення обізнаності громадян про загрози дезінформації, а також розробка механізмів швидкого реагування на інформаційні атаки;

– зміцнення національної стійкості шляхом впровадження стратегій, спрямованих на підвищення стійкості суспільства до гібридних загроз, зокрема економічних і соціальних;

– міжнародне співробітництво шляхом координації зусиль з іншими державами та міжнародними організаціями для протидії транснаціональним гібридним загрозам, обмін досвідом і кращими практиками.

Висновки. Цифрова трансформація значно посилює ризики гібридних загроз. Завдяки швидкому розвитку інформаційних технологій, гібридні загрози можуть завдати значної шкоди на національному та міжнародному рівнях. Наприклад, кібератаки на критичну інфраструктуру можуть призвести до серйозних порушень у функціонуванні держави, дезінформація може спровокувати соціальні конфлікти, а економічний тиск може підривати стійкість економік. Всі ці фактори створюють нові виклики для національної безпеки та вимагають нових підходів до їх нейтралізації.

Цифрова трансформація відкриває нові горизонти для розвитку, але одночасно створює виклики у вигляді гібридних загроз. Для успішної протидії цим загрозам необхідно розробляти і впроваджувати комплексні стратегії, що поєднують кібербезпеку, боротьбу з дезінформацією, зміцнення національної стійкості та міжнародне співробітництво. Тільки таким чином можна забезпечити безпеку та стабільність у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Хаустов М., Бондаренко Д. Цифровізація: здобутки та загрози для суспільства. *InterConf,* 2021. № 51. С 49–58. URL: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/11577 (дата звернення: 21.07.2024)

2. Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *Бізнес Інформ*. 2022. № 3. С. 17–26. DOI: https://doi.org/10.32983/2222-4459-2022-3-17-26 (дата звернення: 26.06.2024)

3. Цифрова економіка: тренди, ризики та соціальні детермінанти / Центр Разумкова. Київ : Видавництво “Заповіт”, 2020. 274 с. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf (дата звернення: 05.08.2024)

4. Хаустова В. Є., Решетняк О. І., Хаустов М. М. Перспективні напрямки розвитку IT-сфери в світі. *Проблеми економіки*. 2022. № 1. С. 3–19. DOI: https://doi.org/10.32983/2222-0712-2022-1-3-19 (дата звернення: 29.07.2024)

5. Key Issues for Digital Transformation in the G20. Report Prepared for a Joint G20 German Presidency. OECD, 12 January 2017. URL: https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (дата звернення: 22.07.2024)

6. UN chief outlines solutions to defeat ‘four horsemen’ threatening our global future. – UN News, 22 January 2020. URL: https://news.un.org/en/story/2020/01/1055791

7. Fiott D. Digitalization and hybrid threats: Assessing the vulnerabilities for European security. Hybrid CoE Paper 13. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/04/20220404-Hybrid-CoE-Paper-13-Digitalization-and-hybrid-threats-WEB.pdf (дата звернення: 25.07.2024)

8. Mazzucchi N. AI-based technologies in hybrid conflict: The future of influence operations. Hybrid CoE Paper 14. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf (дата звернення: 15.07.2024)

9. Artificial Intelligence and National Security / Congressional Research Service. November 10, 2020. URL: https://sgp.fas.org/crs/natsec/R45178.pdf (дата звернення: 29.07.2024)

10. Reding D. F., Eaton J. Science & Technology Trends 2020–2040. Exploring the S&T Edge / NATO Science & Technology Organization. Office of the Chief Scientist, Brussels, Belgium. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (дата звернення: 17.07.2024)

REFERENCES:

1. Khaustov M., Bondarenko D. (2021) Tsyfrovizatsiia: zdobutky ta zahrozy dlia suspilstva [Digitalization: achievements and threats to society]. *InterConf*. № 51. P. 49–58. URL: https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/11577 (accessed July 21, 2024)

2. Khaustova V. Ye., Reshetniak O. I., Khaustov M. M., Zinchenko V. A. (2022) Napriamky rozvytku tekhnolohii shtuchnoho intelektu v zabezpechenni oboronozdatnosti krainy [Directions of Development of Artificial Intelligence Technologies in Ensuring the Country's Defense Capability]. *Biznes Inform*. № 3. P. 17–26. DOI: https://doi.org/10.32983/2222-4459-2022-3-17-26 (accessed June 26, 2024)

3. Tsyfrova ekonomika: trendy, ryzyky ta sotsialni determinant (2020) [Digital economy: trends, risks and social determinants] / Tsentr Razumkova. Kyiv : Vydavnytstvo "Zapovit", 274 p. Available at: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf (accessed August 5, 2024)

4. Khaustova V. Ye., Reshetniak O. I., Khaustov M. M. (2022) Perspektyvni napriamky rozvytku IT-sfery v sviti [Promising Areas of IT Development in the World]. *Problemy ekonomiky*. № 1. P. 3–19. DOI: https://doi.org/10.32983/2222-0712-2022-1-3-19 (accessed July 29, 2024)

5. Key Issues for Digital Transformation in the G20. Report Prepared for a Joint G20 German Presidency. OECD, 12 January 2017. Available at: https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf (accessed July 22, 2024)

6. UN chief outlines solutions to defeat 'four horsemen' threatening our global future. UN News, 22 January 2020. Available at: https://news.un.org/en/story/2020/01/1055791

7. Fiott D. (2022) Digitalization and hybrid threats: Assessing the vulnerabilities for European security. Hybrid CoE Paper 13. Available at: https://www.hybridcoe.fi/wp-content/uploads/2022/04/20220404-Hybrid-CoE-Paper-13-Digitalization-and-hybrid-threats-WEB.pdf (accessed July 25, 2024)

8. Mazzucchi N. (2022) AI-based technologies in hybrid conflict: The future of influence operations. Hybrid CoE Paper 14. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf (accessed July 15, 2024)

9. Artificial Intelligence and National Security / Congressional Research Service. November 10, 2020. URL: https://sgp.fas.org/crs/natsec/R45178.pdf (accessed July 29, 2024)

10. Reding D. F., Eaton J. Science & Technology Trends 2020–2040. Exploring the S&T Edge / NATO Science & Technology Organization. Office of the Chief Scientist, Brussels, Belgium. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf (accessed July 17, 2024)