Практичне застосування ArcGIS Survey123 на планшетах дебриферів підтвердило високу стійкість системи до навантажень та зручність для персоналу. Використання ГІС-модуля дозволило скоротити невизначеність даних за рахунок інформаційного виграшу, зменшуючи ентропію при класифікації подій ізоляції.

Запропонована інформаційна модель забезпечує перехід від фрагментованого збору даних до цілісної інтелектуальної системи. Впровадження моделі дозволяє:

1. Двократно підвищити швидкість опрацювання інформації.
2. Сформувати потужну доказову базу щодо воєнних злочинів агресора.
3. Забезпечити когнітивну безпеку звільнених захисників через моніторинг загроз.

За рахунок технологічного оновлення може бути створено проактивну державну систему, де кожен захисник відчуває реальну підтримку, а держава отримує інструменти для ефективної відсічі в інформаційній та правовій площинах для притягнення рф до відповідальності за воєнні злочини.

Джерела та література

1. Герман Дж. Психологічна травма та шлях до видужання. Наслідки насильства – від знущань у сім'ї до політичного терору. Львів: Видавництво Старого Лева, 2015. 416 с.

2. Ukrinform. Як Росія використовує акції родичів військовополонених в інформаційній війні. *Укрінформ - актуальні новини України та світу*. URL: https://www.ukrinform.ua/rubric-ato/3925824-ak-rosia-vikoristovue-akcii-rodiciv-vijskovopolonenih-v-informacijnij-vijni.html (дата звернення: 03.09.2025).

3. Allied Joint Publication. AJP-3(C). Allied Joint Doctrine for the Conduct of Operations. – Brussels: NATO Standardization Office, 2019. – 240 p.

4. Vitalii Fedoriienko, Oleksandr Koshlan, Serhii Kravchenko, Andrii Shyshatskyi, Nataliia Vasiukova, Oleksandr Trotsko, Oksana Havryliuk, Oleksandr Sovik, Oleksandr Alieinik, & Yurii Svyryda. (2021). Development of a methodological approach for processing different types of data in systems of special purpose. Technology Audit and Production Reserves, 6(2(62)), 18–24. DOI: 10.15587/2706-5448.2021.243950.

УДК 355.4:004.8:007.5

Гаврилечко Ю., канд. наук з держ. упр., доц.
Заклад вищої освіти «Університет трансформації майбутнього», Україна

РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ СКЛАДОВІЙ СУЧАСНИХ ВОЄННИХ КОНФЛІКТІВ

Анотація. *Тези присвячено аналізу ризиків застосування штучного інтелекту в інформаційній складовій сучасних воєнних конфліктів. Ідентифіковано п'ять категорій загроз: генерація дипфейків, автоматизована дезінформація, кібератаки на критичну інфраструктуру, алгоритмічна упередженість та підрив суспільної стійкості. Окреслено нормативну відповідь ЄС і запропоновано три напрями протидії для України.*

Ключові слова: *штучний інтелект, воєнний конфлікт, державна інформаційна політика, публічне управління, дезінформація, кібербезпека, кібератака.*

Gavrilechko Yu., Ph.D. (Publ. Adm.), Assoc. Prof.
Higher Education Institution "University of Future Transformation", Ukraine

RISKS OF ARTIFICIAL INTELLIGENCE USE IN THE INFORMATION COMPONENT OF MODERN MILITARY CONFLICTS

Abstract. *The theses examine the risks of artificial intelligence (AI) application in the information component of modern armed conflicts. Five categories of threats are identified: deepfake generation and synthetic content production, automated disinformation campaigns, cyberattacks on critical digital infrastructure, algorithmic bias of AI systems, and erosion of societal resilience. The EU regulatory response through the AI Act, NIS2 Directive and Cyber*

Resilience Act is characterized. Three directions for Ukraine's countermeasures are proposed: legislative-normative, institutional, and public awareness.

Keywords: *artificial intelligence, armed conflict, state information policy, public administration, disinformation, cybersecurity, cyberattack.*

Збройне протистояння сьогодні розгортається одночасно у фізичному і цифровому просторах. Технології штучного інтелекту (ШІ) трансформували обидва виміри: вони знизили собівартість виробництва дезінформації до мінімуму, надали їй промисловий масштаб і зробили практично невиявною для пересічного споживача. Цифровий фронт перетворився на повноцінний театр воєнних дій, де ШІ-інструменти застосовуються для деморалізації населення, підриву довіри до владних структур і дестабілізації суспільства [1; 6]. Брак адекватної правової й інституційної відповіді на ці загрози формує системну вразливість держав, залучених до збройного протистояння.

*Основні категорії ризиків***.** На підставі аналізу джерел виокремлено п'ять взаємопов'язаних категорій ризиків.

Перша – генерація дипфейків і синтетичного контенту. Сучасні генеративні моделі здатні відтворювати зовнішність і голос реальних людей із фотографічною точністю, що уможливлює масштабне виробництво підроблених відеозвернень посадових осіб, фальшивих воєнних наказів і сфабрикованих доказів злочинів. EU AI Act кваліфікує маніпулятивний ШІ-контент як «неприйнятний ризик» і зобов'язує маркувати синтетичні матеріали [7], проте верифікаційні технології принципово відстають від інструментів генерації.

Друга – автоматизовані дезінформаційні кампанії. Великі мовні моделі дозволяють автоматично формувати масиви публікацій, адаптованих під ціннісні й поведінкові патерни конкретних аудиторій. Платформні алгоритми рекомендацій органічно розповсюджують такий контент, посилюючи його охоплення без додаткових витрат. EU AI Act зараховує подібні системи до «високоризикових» у частині впливу на демократичні процеси [7].

Третя – кібератаки на цифрову інфраструктуру держави. ШІ автоматизує розвідку вразливостей, генерацію адаптивного шкідливого коду та соціальну інженерію. Атаки на інформаційні системи публічних послуг (реєстри, е-урядування, соціальні виплати) руйнують суспільну довіру до держави. Директива NIS2 та Акт про кіберстійкість ЄС встановлюють обов'язкові вимоги захисту критичної інфраструктури [3; 4].

Четверта – алгоритмічна упередженість. ШІ-системи, навчені на неякісних або маніпульованих даних, формують хибні аналітичні висновки та дискримінують окремі групи при наданні послуг (соціальні виплати ВПО, гуманітарна допомога). Ризик зростає в умовах воєнного часу, коли системи функціонують поза межами своїх тренувальних даних [6].

П'ята – підрив суспільної стійкості й довіри до інститутів. Комбінований вплив перших чотирьох категорій реалізує класичну мету гібридної агресії: розкол суспільства. ШІ є мультиплікатором ефективності такого впливу — він робить його безперервним, малозатратним і практично невід'ємним від органічного контенту.

Регуляторний контекст та виклики для України. EU AI Act (Regulation (EU) 2024/1689), чинний з серпня 2024 року, встановлює чотириступеневу ризик-орієнтовану класифікацію ШІ-систем [7]. Маніпулятивні ШІ та масова біометрична ідентифікація заборонені як «неприйнятний ризик»; ШІ у виборчих процесах і правоохоронній діяльності — «високоризиковий». В Україні як країні-кандидаті до ЄС правове регулювання залишається фрагментарним [8; 9; 10]: єдиного закону про ШІ не ухвалено, Стратегія розвитку ШІ до 2030 р. перебуває на рівні проєкту документу[2].

Протидія ШІ-ризикам в інформаційній складовій воєнного конфлікту потребує трьох взаємопов'язаних напрямів.

Нормативно-правовий: прийняття Закону України «Про штучний інтелект» із ризик-орієнтованою класифікацією, обов'язкове маркування ШІ-контенту, гармонізація з NIS2 та CRA.

Інституційний: створення Національного агентства регулювання ШІ; формування підрозділів реагування на ШІ-генеровані загрози у структурі Центру протидії дезінформації при РНБО.

Просвітньо-комунікативний: системна публічна кампанія з верифікації ШІ-контенту та розпізнавання дипфейків; навчання держслужбовців; партнерство з медіа та НГО. Комплексна реалізація цих напрямів дозволить Україні перетворитися з об'єкта ШІ-маніпуляцій на суб'єкта активної протидії їм.

Джерела та література

1. Дія.AI: Ваш персональний помічник у світі державних послуг. URL: https://diia.gov.ua/diia-ai (дата звернення: 10.04.2026).
2. Україна презентувала драфт Стратегії розвитку ШІ до 2030 року. URL: https://digitalstate.gov.ua/uk/news/govtech/ukrayina-prezentuvala-draft-stratehiyi-rozvytku-shi-do-2030-roku-fokus-na-praktychne-zastosuvannia-infrastrukturu-ta-vlasni-modeli (дата звернення: 10.04.2026).
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union.* URL: https://www.nis-2-directive.com/ (дата звернення: 10.04.2026).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Official Journal of the European Union.* URL: https://www.european-cyber-resilience-act.com/ (дата звернення: 10.04.2026).
5. Sounding the alarm: how high-profile threats influence learning behaviors. Immersive Labs. URL: https://www.immersivelabs.com/resources/blog/sounding-the-alarm-how-high-profile-threats-influence-learning-behaviors (дата звернення: 10.04.2026).
6. Штучний інтелект у правовій практиці: межі та можливості : збірник тез круглого столу (14 березня 2025 р.) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. 238 с.
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union.* URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення: 10.04.2026).
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.04.2026).
9. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.04.2026).
10. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.04.2026).

УДК 316.77:004.738.5:355.01

Горішна О., доктор філософії у галузі Освіта/Педагогіка; Зозуляк М.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СОЦІАЛЬНІ КОМУНІКАЦІЇ ТА МЕХАНІЗМИ МАНІПУЛЯЦІЇ В УМОВАХ ВОЄННИХ ДІЙ

Анотація. *У роботі проаналізовано роль соціальних комунікацій в умовах війни як критичної інфраструктури формування громадської думки, суспільної консолідації та інформаційної безпеки. Розкрито трансформацію цифрових платформ і месенджерів у ключові канали оперативної взаємодії держави й громадян, а також інструменти волонтерської самоорганізації. Окреслено основні механізми маніпулятивного впливу: дезінформацію, інформаційний оверлоад, ботоферми, дипфейки та емоційні тригери.*