СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ЗАСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ В УКРАЇНІ

Авдєєва Галина Костянтинівна,
кандидат юридичних наук, старший науковий співробітник, провідна наукова співробітниця Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України

Вплив РФ на населення нашої країни в інформаційному просторі є інформаційною війною, головним завданням якої є підрив морально-психологічного стану, зміна поведінкового й емоційного настрою, дезорієнтація та дезінформація, послаблення певних традицій і переконань, залякування своєю могутністю та ін. [1]. Ворог намагається зіпсувати

стосунки між Україною та країнами-партнерами, між силовими структурами України та волонтерами, між військовими і населенням, спрямовує зусилля на зрив мобілізації, тощо.

РФ в Україні та інших країнах колишнього СРСР просуває ідеї так званого «руського миру», який передбачає відновлення ідеології радянської системи управління. В цьому напрямі «працюють» всі, хто має вплив на населення: актори, режисери, співаки, вчителі, політичні діячі, журналісти, блогери та ін. Навіть вчені-історики та освітяни РФ «переписують» історію на замовлення керівництва країни-агресора, «вкладають» її у розум росіян та «нав'язують» громадянам України. М. Дмитренко справедливо зауважує, що ця «війна не за території, а за світогляд, думки і душі людей». [2, с. 240–241].

Поряд із використанням традиційних засобів (друковані та електронні засоби масової інформації) РФ використовує спеціальні засоби впливу на людину через комп'ютерні мережі: засоби інформаційно-психологічного впливу, психогенного впливу, психоаналітичного впливу, нейролінгвістичного впливу, психотронного впливу та психотропного впливу. [3, с. 46]. Спецслужбами РФ для проведення інформаційно-психологічних атак використовуються фейкові (підроблені) новини, які супроводжуються підробленими фотознімками та відеозаписами, в т.ч. – створеними за допомогою нейронних мереж, алгоритм роботи яких імітує роботу мозку людини (штучний інтелект). Останнім часом найбільш відомими продуктами, згенерованими системами штучного інтелекту, є зображення хлопчика, який вижив під час ракетного удару в Дніпрі та фейкове відео-звернення В. Зеленського про капітуляцію, яке з'явилося в інформаційному просторі у березні 2022 р. [4].

За результатами дослідження, проведеного аналітичним центром NewsGuard в січні 2023 р., встановлено, що дуже популярна та загальнодоступна в усьому світі система штучного інтелекту ChatGPT (Generative Pre-trained Transformer) здатна генерувати неправдиві тексти з елементами інформації про реальні події. [5]. Система за певним запитом може згенерувати дезінформаційне повідомлення, в т. ч. – засноване на «кремлівській» пропаганді.

В. С. Батиргарєєва справедливо зазначає, що «на теперішній час протидія дезінформації – одна з ключових проблем убезпечення національного інформаційного простору від загроз в умовах ведення так званої гібридної війни проти нашої держави, низького рівня медіаграмотності українців та неможливості ідентифікувати особу, яка масово розповсюджує ту чи іншу дезінформацію». [6, с. 111].

Інформаційний захист в Україні здійснюється шляхом проведення контрольної розвідки, збирання та перевірки інформації, зіставлення інформації про той самий факт (явище) від різних джерел з метою виявлення і блокування дезінформації. Такі завдання є дуже складними і масштабними і тому для їх швидкого і якісного виконання використовуються системи штучного інтелекту, які мають великий потенціал для створення та опрацювання великого обсягу цифрової інформації.

Вчені у галузі комп'ютерних наук під штучним інтелектом (ШІ) розуміють «властивість автоматичних систем брати на себе окремі функції інтелекту людини». [7, с. 9]. ШІ може використовуватися для автоматичного аналізу великої кількості даних з різних джерел з метою виявлення неправдивої інформації, розпізнавання змінених або підроблених зображень шляхом порівняння їх з оригінальними, встановлення схем і способів поширення дезінформації та її блокування. Зокрема, в Апараті РНБО України використовується сучасна багатофункціональна інформаційно-аналітична система з елементами ШІ «СОТА», яка слугує інструментом аналізу та управління ризиками у сфері національної безпеки і оборони України. [8].

Системи ШІ ефективно вирішують завдання щодо ідентифікації осіб за фотознімками та відеозаписами. Зокрема, за допомогою американської системи розпізнавання осіб Clearview AI, яка використовує базу даних з 10 млрд фотопортретів (в т.ч. – з соціальних мереж), встановлено особи окремих громадян РФ, які розповсюджують дезінформацію від імені громадян України.

Центр стратегічних комунікацій та інформаційної безпеки України використовує автоматизовану систему SemanticForce, яка дозволяє аналізувати певні неприйнятні або шкідливі інформаційні потоки і зображення та реакцію на них користувачів, відрізняти хибні акаунти від реальних користувачів, тощо. [9]. Систему Attack Index використовують з метою виявлення певних інформаційних операцій та їх характеристик (час, інтенсивність, масштабність, ініціатор операції, мережа розповсюдження інформації) та подальшого пропонування сценаріїв протидії інформаційним загрозам. [10].

Поряд з ефективністю роботи з великими масивами інформації системи ШІ мають певні недоліки і викликають занепокоєння в усьому світі. Зокрема, через недосконаліть біометричних систем, велику кількість помилок в їх роботі та можливі порушення прав людини парламент

ЄС нещодавно запропонував заборонити збирання фотозображень осіб до приватних систем розпізнавання (в т.ч. Clearview). [11].

Члени міжнародної асоціації юристів попереджають про можливі помилкові результати роботи систем ШІ через помилки людини під час формування баз даних і формулювання варіантів підсумкових рішень, які аналізує ШІ, а також через помилки у програмному коді ШІ, який також створюється людиною. [12].

З метою запобігання дискримінації і порушення основних прав і свобод під час використання систем ШІ в правоохоронних органах до парламенту ЄС поданий проєкт «Закону про штучний інтелект», в якому запропоновано при використанні таких систем застосовувати високі рівні підзвітності, справедливості та прозорості. В документі наголошено на тому, що системи ШІ мають бути юридично, етично та технічно надійними, повинні відповідати демократичним цінностям, правам людини та верховенству закону. [13].

Завдання розвитку технологій ШІ в Україні є одним з пріоритетних напрямів у сфері науково-технологічних досліджень. В «Концепції розвитку штучного інтелекту в Україні» основою державної політики у сфері правового регулювання галузі штучного інтелекту проголошено захист прав та свобод учасників відносин у галузі штучного інтелекту, розроблення та використання технологій штучного інтелекту з дотриманням етичних стандартів. [14]. На жаль, в «Плані заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки» [15] не містяться конкретні заходи щодо законодавчого регулювання процесів використання ШІ у боротьбі зі злочинністю, а заплановано лише «запровадження правового регулювання з питань формування державної політики у галузі штучного інтелекту» та «впровадження технологій штучного інтелекту в національну систему кібербезпеки». [16, с. 39]. При цьому на сьогодні питання законодавчого врегулювання процесів використання систем ШІ у боротьбі зі злочинністю є вкрай актуальними.

Стрімкий розвиток і широке розповсюдження систем ШІ випереджають процеси створення умов і засобів ефективної протидії недобросовісному і зловмисному їх використанню. Для вирішення цього питання на засіданні групи семи розвинутих країн (G7), яке відбулося в Японії 29 квітня 2023 р, міністри цифрових технологій узгодили п’ять таких принципів розвитку ШІ: верховенство права, дотримання законної процедури, демократія, повага до прав людини і використання можливостей для інновацій. На майбутніх засіданнях групи G7 планується розглянути

питання щодо управління системами ШІ, захисту авторського права та боротьби з дезінформацією. [17].

У вересні 2022 р. Європейська комісія підписала Угоду про приєднання України до програми «Цифрова Європа» та надала можливість нашій країні скористатися фінансуванням і підтримкою програми щодо розширення можливостей використання систем ШІ у різних галузях. Така можливість може бути реалізована лише за умови імплементації норм, закріплених у «Рекомендаціях щодо штучного інтелекту», що прийняті у червні 2019 року Організацією економічного співробітництва та розвитку[1] [18] у законодавство України та за умови дотримання етичних стандартів, передбачених в Рекомендаціях CM/Rec (2020)1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини, схвалених 8 квітня 2020 р. [19],. Оскільки 23 червня 2022 р. Україна набула статусу країни-кандидата на вступ до Європейського Союзу, законодавство нашої країни, в т.ч. – у частині використання систем ШІ в інформаційній війні з РФ, має бути поступово адаптовано до законодавства ЄС.

Список використаних джерел:

1. Інформаційна війна / Р. В. Пилипчук // Енциклопедія Сучасної України / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк [та ін.]. Київ : Інститут енциклопедичних досліджень НАН України, 2011. URL : https://esu.com.ua/article-12460 (дата звернення: 29.04.2023).
2. Дмитренко М. А. Проблемні питання інформаційної безпеки України. *Міжнародні відносини. Серія Політичні науки*. 2017. №17. С. 236–243.
3. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», «Кібербезпека» / В. І. Гур'єв, Д. Б. Мехед, Ю. М. Ткач, І. В. Фірсова. Ніжин: ФОП Лук'яненко В. В. ТПК «Орхідея», 2018. 166 с.
4. Штучний інтелект і дезінформація: можливості та ризики в умовах війни. Центр стратегічних комунікацій та інформаційної безпеки. Укрінформ : Мультимедійна платформа іномовлення України. 05.04.2023 . https://www.ukrinform.ua/rubric-technology/3691961-stucnij-intelekt-i-dezinformacia-mozlivosti-ta-riziki-v-umovah-vijni.html (дата звернення: 29.04.2023).
5. Misinformation Monitor: January 2023. NewsGuard. https://www.newsguardtech.com/misinformation-monitor/jan-2023/ (дата звернення: 28.04.2023).

[1] Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. (OECD/LEGAL/0449). Adopted on: 22/05/2019. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

6. Батиргареєва В. С. Концептуальна модель захисту інформаційного простору України засобами кримінального права. *Інформація і право*. № 1(32). 2020. С. 110–119.

7. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки «Комп'ютерні науки» / уклад. : А. С. Савченко, О. О. Синельніков. Київ : НАУ, 2017. 190 с.

8. В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА». РНБО: офіційний сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/5011.html (дата звернення: 27.04.2023).

9. SemanticForce media and e-commerce intelligence. URL: https://semanticforce.ai/en (дата звернення: 27.04.2023).

10. Attack index be in your guard. URL: https://attackindex.com/uk/golovna/ (дата звернення: 27.04.2023).

11. Європарламент закликав заборонити системи розпізнавання осіб. Європейська правда. 06.10.2021. URL: https://www.eurointegration.com.ua/news/2021/10/6/7128684/ (дата звернення: 28.04.2023).

12. Idder A. , Coulaux S. Artificial intelligence in criminal justice: invasion or revolution? International Bar Association. Anti-Money Laundering Forum. London. 13 December 2021. URL: https://www.ibanet.org/dec-21-ai-criminal-justice (дата звернення: 27.04.2023).

13. Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. An official website of the European Union. Brussels, 21.04.2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата звернення: 26.04.2023).

14. Концепція розвитку штучного інтелекту в Україні : схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556–2020-%D1%80#Text (дата звернення: 25.04.2023).

15. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки : затвер. розпорядженням Кабінету Міністрів України від 12 травня 2021 р. № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438–2021-%D1%80#n10 (дата звернення: 27.04.2023).

16. G7 should adopt 'risk-based' AI regulation, ministers say. Reuters. April 30, 2023. https://www.reuters.com/markets/europe/g7-should-adopt-risk-based-ai-regulation-ministers-say-2023-04-30/ (дата звернення: 30.04.2023).

17. Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. (OECD/LEGAL/0449). Adopted on: 22/05/2019. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (дата звернення: 25.04.2023).

18. Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee

of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016809e1154 (дата звернення: 25.04.2023).