

*Буров О.Ю.*

*доктор технічних наук, старший дослідник  
Інститут інформаційних технологій і засобів навчання, м. Київ*

## **КІБЕР-РИЗИКИ ТА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕРЕЖНІЙ ДІЯЛЬНОСТІ**

Реформування освіти, що охопило весь світ, відбувається шляхом стрімкого впровадження інформаційно-комунікаційних технологій (ІКТ), розширеного застосування синтетичного навчального середовища та штучного інтелекту (ШІ) як в навчальному процесі, так і в усіх інших сферах життя та діяльності людини [1], враховуючи системний характер навчання [2]. Україна також намагається не відставати від міжнародних трендів [3], розуміючи гострі питання, що виникають при цьому [4]. Про це свідчить і тривожна статистика зростання кіберзлочинності [5]. Враховуючи інтенсивне та екстенсивне використання ІКТ і ШІ в різних галузях критичної сфери країни [6], де людина стає все більш вразливою ланкою людино-машинної системи [7], ІКТ надають можливість ефективного використання більш складних і більш точних моделей прогнозування надійності людини та системи в цілому [8], а також впливу зовнішніх чинників.

Проте слід відзначити, що одночасно з великими очікуваннями від ШІ, зростає і його кримінальне використання, насамперед із переходом праці та освіти в дистанційну форму. Аналіз злочинних дій, проведений авторами [9], дозволив визначити найбільш вагомі ризики, пов'язані із застосуванням ШІ.

Злочини оцінювались за чотирима аспектами, які були визначені як важливі для розуміння різних аспектів тяжкості загрози, наступним чином: шкода, злочинна вигода, досяжність, витрати.

Авторами визначені 20 найбільш поширених типів злочинів із використанням ШІ (за даними наукових статей, новин і поточних подій, а також з художньої та популярної культури). Експертами виступили представники академічних кіл, приватного сектора, поліції, уряду і органів державної безпеки. Кібер-небезпеки від застосування ШІ були згруповані у відповідності до трьох рівнів – високий, середній і низький.

*Високий* рівень: аудіо/відео персоніфікація, безпілотні транспортні засоби як зброя, цільовий фішинг, пошкодження систем, керованих ШІ, масштабний шантаж, створені ШІ фейкові новини.

*Середній* рівень: воєнні роботи, «зміїні олія», отруєні дані, кібератаки на основі навчання, автономні ударні дрони, онлайн позбавлення звичних комфортних умов, обман з розпізнаванням облич, бомбардування ринку.

*Низький* рівень: використання упередженості, боти-грабіжники, ухилення від виявлення ШІ, створені ШІ фейкові огляди, переслідування за допомогою ШІ, підробка.

Певна частина із зазначених загроз можуть зустрітися під час навчання та професійної підготовки.

### **Список використаних джерел**

- [1] White Paper On Artificial Intelligence - A European approach to excellence and trust // European Commission, Brussels. - 19.2.2020 COM(2020) 65 final.- 27 pp.
- [2] Pinchuk O., Burov O., Lytvynova S. Learning as a Systemic Activity // Karwowski W., Ahram T., Nazir S. (eds) / Advances in Human Factors in Training, Education, and Learning Sciences. AHFE 2019. Advances in Intelligent Systems and Computing. Springer, Cham. – 2019. – Vol 963. – Pp. 335-342. DOI : [https://doi.org/10.1007/978-3-030-20135-7\\_33](https://doi.org/10.1007/978-3-030-20135-7_33) (2019).
- [3] Розпорядження Кабінету Міністрів України від 02 грудня 2020 р. N 1556-р Про схвалення Концепції розвитку штучного інтелекту в Україні. URL: [http://search.ligazakon.ua/l\\_doc2.nsf/link1/KR201556.html](http://search.ligazakon.ua/l_doc2.nsf/link1/KR201556.html) (дата звернення: 03.02.2021).
- [4] This alliance aims to accelerate the adoption of inclusive, trusted and transparent AI worldwide. URL: <https://www.weforum.org/agenda/2021/01/global-ai-action-alliance/> (дата звернення: 26.02.2021).
- [5] НКЦК: у 2021 році в Україні зафіксовано вже майже 14 мільйонів інцидентів у сфері кібербезпеки. URL: <https://www.rnbo.gov.ua/ua/Diialnist/4797.html> (дата звернення: 09.02.2021).
- [6] Burov O. Y. ICT for performance assessment of emergent technologies operators // Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer Kyiv, Ukraine, May 15-18, 2017. – CEUR-WS, 2017. – Т. 1844. – С. 127-138.
- [7] Буров А. Ю. Психофизиологическое обеспечение труда операторов / А. Ю. Буров // Информационно-управляющие системы на железнодорожном транспорте. – 1999. – №. 6. – С. 32-34.
- [8] Spirin O., Burov O. Models and applied tools for prediction of student ability to effective learning. 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. – CEUR-WS, 2018. – Т. 2104. – Pp. 404-411.
- [9] Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. Crime Sci 9, 14 (2020). URL: <https://doi.org/10.1186/s40163-020-00123-8> (дата звернення: 26.02.2021)