

Клеван Віолета Євгенівна,
*курсант навчально-наукового інституту
№ 1 Харківського національного
університету внутрішніх справ*

ЦИФРОВИЙ СУВЕРЕНІТЕТ ДЕРЖАВИ В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ

У ХХІ столітті держави все частіше стикаються з необхідністю переосмислення природи власного суверенітету в умовах глобальної цифрової трансформації. Впровадження технологій штучного інтелекту (ШІ), поширення великих даних і автоматизованих інформаційних систем зумовлює появу нових викликів у сфері державного управління, прав людини та інформаційної безпеки. У зв'язку з цим актуалізується поняття цифрового суверенітету, що означає здатність держави здійснювати суверенний контроль над цифровими потоками даних, інфраструктурою, платформами, а також нормотворенням у сфері цифрових технологій.

На міжнародному рівні, особливо в рамках Європейського Союзу, посилюється прагнення до цифрової автономії. Прикладом є ініціатива GAIA-X, яка передбачає створення власної безпечної хмарної інфраструктури, що відповідає вимогам Загального регламенту захисту даних (GDPR) і зменшує залежність від іноземних платформ [1]. Іншим важливим кроком стало прийняття Регламенту ЄС про штучний інтелект (AI Act), який класифікує системи ШІ за ступенем ризику, забороняє використання технологій для соціального скорингу та масового біометричного нагляду, а також передбачає правові механізми для забезпечення прозорості алгоритмів [5, с. 1].

На відміну від ЄС, Україна ще перебуває на стадії концептуального осмислення цифрового суверенітету. В умовах гібридної війни держава стикається з викликами інформаційної безпеки, маніпуляції громадською думкою, використанням бот-мереж і алгоритмів ШІ у пропагандистських кампаніях [2]. Як зазначається в дослідженні Інституту Просвіти, сучасні цифрові платформи стали основними каналами поширення фейкової інформації, що формує спотворену реальність для користувачів і підриває стабільність суспільства [2].

Додаткову загрозу становить явище цифрового колоніалізму, коли країни, що не мають власних технологій, змушені покладатися на іноземне програмне забезпечення для зберігання, обробки й захисту державних даних. Як слушно зазначає І.М. Милосердна, в умовах цифрової глобалізації така залежність є не менш небезпечною, ніж економічна чи політична, і здатна спричинити втрату цифрової автономії [3, с. 2].

Загроза цифровій безпеці також пов'язана з недостатнім рівнем цифрової грамотності населення. У ситуації, коли громадяни не володіють навичками критичного мислення, технології ШІ можуть бути використані як засіб когнітивного контролю. Це підкреслює необхідність формування не лише

техніко-правових інструментів цифрового суверенітету, а й суспільної стійкості до маніпуляцій [2].

На цьому тлі особливої ваги набуває Рекомендація ЮНЕСКО з етики ШІ (2021), яка містить принципи, орієнтовані на забезпечення прав людини, прозорість, недискримінацію, безпеку та інклюзію при використанні штучного інтелекту [4]. Її положення можуть стати основою для імплементації національного законодавства України у сфері ШІ.

Отже, формування цифрового суверенітету України потребує поєднання технічної незалежності, етичного правового регулювання, освітніх програм та міжнародної інтеграції стандартів. Без цього держава залишатиметься вразливою до зовнішніх технологічних впливів.

Список використаних джерел

1. Компанієць Ф. Контроль над хмарою – контроль над майбутнім. *Speka – онлайн-медіа про підприємництво та технології*. URL: <https://speka.media/cifrovii-suverenitet-jevropi-9qy53k>.

2. Цифрові пропагандисти та інформаційний суверенітет. Як захистити свої права в онлайн-епоху. *Інститут Просвіти*. URL: <https://iprosvita.com/tsyfrovii-propahandysty-ta-informatsijnyj-suverenitet-iaak-zalyshytysia-neoshukanym-ta-zakhystyty-svoi-prava-v-onlajn-epokhu/>

3. Милосердна І.М. Цифровий суверенітет держави: наукова риторика та реальні зміни. *Репозитарій ПНПУ ім. К. Д. Ушинського*. URL: <http://dspace.pdpu.edu.ua/bitstream/123456789/21794/1/25.pdf>.

4. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.

5. Regulation (EU) 2024/1365 of the European Parliament and of the Council of 13 March 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1365>.

Ковальова Дар'я Юріївна,

*слухач навчально-наукового інституту
поліцейської діяльності Національної
академії внутрішніх справ*

ЗАХИСТ ДІТЕЙ ТА ВРАЗЛИВИХ ГРУП У ЦИФРОВОМУ СЕРЕДОВИЩІ

Цифрове середовище стало невід'ємною частиною повсякденного життя, і воно надає безліч можливостей для дітей та молоді, зокрема в навчанні, соціалізації, культурному обміні і навіть у професійному розвитку. Однак, разом із цими можливостями виникають нові загрози для здоров'я та безпеки, особливо для дітей та вразливих груп. Цифровий простір парадоксально поєднує у собі освітні можливості й механізми впливу, які часто використовуються