УДК 347.121.1:004.8

Гера В.О.
аспірантка першого курсу юридичного факультету
Західноукраїнський національний університет
Науковий керівник:
Саванець Л.М.
к.ю.н., доцент, завідувач кафедри
міжнародного та європейського права,
Західноукраїнський національний університет

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ДАНИХ, ЗГЕНЕРОВАНИХ ШТУЧНИМ ІНТЕЛЕКТОМ

На сучасному етапі розвитку суспільства штучний інтелект (далі – ШІ) перестав бути виключно теоретичною концепцією та набув статусу повноцінного елемента повсякденного життя. Технології ШІ широко застосовуються у сфері освіти, професійної діяльності, а також у вирішенні повсякденних і життєвих завдань, постійно здійснюючи обробку інформаційних запитів і генеруючи нові масиви даних. Незважаючи на високу інформативну цінність таких даних та їхнє широке застосування у сфері медичного прогнозування, вирішення правових питань і забезпечення психологічної підтримки, спостерігається постійне зростання кількості викликів, насамперед у контексті забезпечення конфіденційності та захисту персональної інформації. Аналіз зазначених проблем і напрацювання ефективних правових та організаційних механізмів їх подолання мають ключове значення для захисту прав і свобод особи в умовах цифровізації суспільних відносин.

Конфіденційність даних є ключовою проблемою не лише перспективного розвитку суспільства, а й сучасних соціальних відносин. Саме вона забезпечує захист персональної інформації, підтримує рівень довіри між фізичними особами, суб’єктами господарювання та організаціями, а також створює умови для реалізації права особи на контроль доступу до власних даних. Незаконний витік персональних даних є однією з найбільш поширених загроз у сучасному цифровому середовищі. Його наслідками можуть бути не лише суттєві фінансові

втрати, а й значна шкода діловій репутації та емоційному благополуччю особи. Суб'єкти господарювання, для яких забезпечення конфіденційності персональних даних споживачів є пріоритетом, демонструють належний рівень відповідальності та відданості принципам захисту інформації, що, своєю чергою, сприяє зміцненню довіри користувачів.

Сьогодні головною проблемою вважається те, що ШІ використовує особисті дані без дозволу особи. При користуванні програмою її пам'ять наповнюється приватною інформацією, а саме імена, приватні листування, номери телефонів, адреси. Як зазначає П. Хакер, це прямо порушує правила захисту даних, оскільки особи не давали згоди на використання особистої інформації [7, с.145]. ШІ легко впізнає людину, навіть у тому випадку, коли її дані намагалися приховати. Це створює серйозні ризики для приватності користувачів [12, с. 510].

Також увагу варто приділити комерційній стороні питання конфіденційності даних. Л. Саванець та Г. Стахира наголошують, що зараз приватні дані стали товаром, який компанії збирають з метою отримання прибутку [6, с. 112; 10, с. 30]. У своїх дослідженнях науковці також піднімають питання захисту «цифрового споживача» в умовах економіки великих даних, в яких людина є вразливою перед алгоритмами [11, с. 155].

З метою запобігання виникнення даної проблеми необхідним є здійснення перевірки розробниками ШІ даних, ще до моменту початку самого навчання програми. На законодавчому рівні кожній особі необхідно гарантувати право на «цифрове забуття» шляхом повного видалення із пам'яті програми усієї інформації про її користувача [13, с.165]. Тільки такі чіткі правила зможуть забезпечити право людина на недоторканість особистого життя.

Упровадження прозорих механізмів обробки даних, застосування надійних заходів інформаційної безпеки, а також проведення регулярного аудиту дозволяють істотно знизити ризики витоку персональних даних і сформувати більш безпечне цифрове середовище. Такий підхід створює передумови для підвищення рівня готовності користувачів до надання власних персональних

даних у межах правомірних і чітко визначених цілей. Саме від цих даних в основному й залежать технології ШІ. Їх використовують щоб забезпечити такі процеси як збирання відомостей, машинне навчання тощо. Системи аналізують логічну послідовність дій та приймають рішення, які мають відповідний вплив на все: від особистих рекомендацій до фінансових показників. Така широка сфера при використанні цих даних зумовлює виникнення ряду питань, а саме як ці дані використовуватимуться, хто матиме доступ до них та які наслідки для конфіденційності можуть настати.

Проблеми забезпечення конфіденційності виникають насамперед на етапах збирання та подальшого використання даних без належної згоди суб'єкта персональних даних. У сучасних умовах окремі системи ШІ здійснюють обробку особистої інформації без чітко вираженого волевиявлення особи щодо подальшого використання її даних. Така практика призводить до істотного порушення принципу конфіденційності, оскільки персональні дані обробляються без відома та належного схвалення осіб, яким вони належать. Споживачі часто не поінформовані або не виявляють належної зацікавленості щодо способів збирання та цілей використання їхніх персональних даних, що зумовлено, зокрема, застосуванням непрозорих умов обробки та обміну даними у багатьох цифрових сервісах. Відсутність належної прозорості суттєво підриває рівень довіри між користувачами та надавачами послуг, а також створює загрози для збереження конфіденційності та нерозголошення персональних даних. Унаслідок обробки даних без належної та інформованої згоди суб'єкта особа може зазнавати негативних наслідків, зокрема впливу цільової реклами, отримання небажаної інформації, а також ризику неправомірного використання чи викрадення персональних даних [9].

Законодавство, яке регулює питання конфіденційності даних перебуває на етапі динамічних змін. Правові основи його забезпечення містяться у міжнародно-правових актах. Так, відповідно до ст. 12 Загальної декларації прав людини, ніхто не може зазнавати безпідставного втручання в його особисте та сімейне життя, посягань на недоторканність його житла, таємницю листування

та кореспонденції, а також на його честь і репутацію. Кожна особа має право на захист від такого втручання або посягання відповідно до закону [2].

Також у цьому контексті варто навести статтю 8 Конвенції про захист прав людини і основоположних свобод 1950 року (далі – ЄКПЛ), відповідно до якої: «1. Кожна особа має право на повагу до свого приватного і сімейного життя, житла та кореспонденції. 2. Органи державної влади не можуть втручатись у реалізацію цього права, за винятком випадків, коли втручання є законним і необхідним у демократичному суспільстві для забезпечення національної та громадської безпеки, економічного добробуту, запобігання заворушенням чи злочинам, захисту здоров'я або моралі, а також для захисту прав і свобод інших осіб» [3].

Основоположним інструментом захисту приватності у Європейському Союзі вважається Регламент 2016/679 про захист фізичних осіб стосовно обробки персональних даних та про вільний рух таких даних (General Data Protection Regulation, далі – GDPR). Його принципи «мінімізації даних», «обмеження мети» та «обмеження зберігання» стають основним бар'єром проти безконтрольного використання приватної інформації для навчання систем ШІ. Проблемою постає складність у реалізації права на забуття у ШІ, адже якщо особисті дані вже опинилися у системі, їх практично неможливо вилучити без повного перенавчання системи [9]. Новий Регламент 2023/2854 про гармонізовані правила справедливого доступу до даних та їх використання (далі – DataAct), доповнюючи GDPR, більше фокусується на справедливому доступі до даних та їх використанні. GDPR захищає суб'єкта даних, а положення DataActрегулюють відносини між користувачами та виробниками пристроїв, які генерують дані [8].

На національному рівні питанню забезпечення конфіденційності даних присвячені окремі положення Конституції України, Цивільного кодексу України та Закону України «Про захист персональних даних». Зокрема у ст.31, 32 Конституції України закріплено право кожного на комунікаційну та інформаційну приватність з гарантуванням кожному дотримання таємниці

листування, телефонних розмов, телеграфної та іншої комунікації, а також заборони збору, зберігання, використання та поширення конфіденційної інформації про особу без її згоди [4].

У березні 2024 року Європейським парламентом був ухвалений перший нормативний акт на міжнародному рівні про ШІ – Artificial Intelligence Act (далі – AI Act). Метою AI Act стало забезпечення захисту прав осіб на яких має вплив ШІ. Підкреслено важливість захисту приватності та особистих даних, включено заборону на розпізнавання емоцій та загалом систем біометричної категоризації. Даним актом дозволена подача скарг осіб на роботу систем ШІ. Прийняття такого акту здійснить вплив і на регулювання роботи ШІ в нашій країні, адже Україні, як країна-кандидат на вступ до ЄС зобов'язана адаптувати власне законодавство до таких норм. Імплементація AI Act вже розпочата Україною [1, с.179]. Одним з найважливіших етапів в імплементації стала публікація Білої книги, яка пояснює, як Україна планує адаптувати європейські стандарти. Також ключовим інструментом вважається AI Sandbox, завдяки яким розробники можуть тестувати власні продукти на відповідність майбутнім нормам AI Act [5].

Таким чином, потрібно вносити суттєві зміни та вдосконалювати вже існуючу політику конфіденційності, ініціювати створення суворіших правил використання даних та гарантувати інформування споживачів про те, як використовуватиметься їх інформація. Створення таких чітких механізмів для згоди та гарантія про видалення неприйнятних даних надасть особі правомочності на відновлення контролю над особистою інформацією.

ЛІТЕРАТУРА

1. Гудзь Л.В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання. *Науковий вісник Ужгородського Національного Університету.Серія ПРАВО*. 2024. Вип. 86. Ч.1. С. 175-180.
2. Загальна декларація прав людини від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення: 13.12.2025).

3. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 13.12.2025).
4. Конституція України від 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text (дата звернення: 13.12.2025).
5. Прес-офіс Міністерства цифрової трансформації України. Україна приєдналася до Європейської ради зі штучного інтелекту від 31.10.2025. URL:https://thedigital.gov.ua/news/progress/ukrayina-pryyednalasia-do-yevropeyskoyi-rady-zi-shtuchnoho-intelektu (дата звернення: 12.01.2026).
6. Саванець Л.М., Поперечна Г.М. «Торгівля» персональними даними – порушення прав на приватність чи нова конструкція цивільного права. *Сучасні системи зв'язку як напрям міжнародно-правової, зовнішньополітичної, теле-, радіо, мережевої комунікації*: начерк науково-практичної конференції присвячений пам'яті українського зв'язківця Тітко Валентина Михайловича: збірник тез доповідей. Київ: ГО «УКРО», 2023. С.29-31.
7. Hacker P. Manipulation by algorithms. Exploring the triangle of unfair commercial practice, data protection, and privacy law. *European Law Journal*. 2021. № 29 (1-2). PP.142-175.
8. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.URL: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng(дата звернення: 12.01.2026).
9. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).* URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (дата звернення: 12.01.2026).

10. Savanets L., Stakhyra H. Ensuring the security of personal data on the internet: the commercial use of personal data by digital content providers. *Актуальні проблеми правознавства.* 2021. № 3. С.110-116.
11. Savanets L., Stakhyra H. Digital consumer – how to protect one in big data economy. *Актуальні проблеми правознавства.* № 3 (23). 2020. С.153–159.
12. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review.* 2019. № 1. PP.494-620.
13. Zarsky T. Z. Privacy and Manipulation in the Digital Age. *Theoretical Inquiries in Law.* 2019. № 20(1). PP.157-188.

УДК 341.312

Заставна О.П.

к.ю.н., старший викладач кафедри
міжнародного та європейського права
Західноукраїнський національний університет

КІБЕРОПЕРАЦІЇ У СВІТЛІ ПРАВА ДЕРЖАВИ НА САМООБОРОНУ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

У сучасних умовах кібероперації стали одним із ключових елементів гібридної війни та використовуються паралельно з традиційними військовими засобами. Сторони конфлікту систематично здійснюють кібератаки проти державних органів, енергетичної інфраструктури, фінансової системи, телекомунікаційних мереж та військових ресурсів з метою дестабілізації функціонування ворожої держави, порушення систем управління та створення паніки серед населення. Особливістю сучасних кібероперацій є їх поєднання з інформаційно-психологічними кампаніями та кінетичними ударами, що свідчить про трансформацію кіберпростору у повноцінний театр воєнних дій. Практика російсько-української війни демонструє, що кібератаки можуть мати масштабні