3. Iurydychna entsyklopediia (1999) [Legal encyclopedia]: v 6 t. K : Ukr. Entsykl.– T. 2.(in Ukrainian).
4. Mishyna, N. V., & Mikhalov, V. O. (2014) Konstytutsiine pravo zarubizhnykh krain [Constitutional law of foreign countries]. Dnipropetrovsk: Seredniak T. K. (in Ukrainian).
5. Riiaka, V. O. (2006) Konstytutsiine pravo zarubizhnykh krain [Constitutional law of foreign countries]. K: Iurinkom Inter. (in Ukrainian).
6. Entin, L. M. (2005) Evropeiskoe pravo. Pravo Evropeiskoho Soiuza y pravovoe obespechenye zashchytы prav cheloveka [ European law. European Union law and legal protection of human rights]. Moskva: Norma (in Russian).
7. Pro vikonannya rishen ta zastosuvannya praktiki Evropeyskogo sudu z prav lyudini, Zakon Ukrai'ny [On the implementation of decisions and application of the case law of the European Court of Human Rights, Law of Ukraine] № 3477-IV-VR (2006) Vidomosti Verhovnoi Rady Ukrai'ny [Information of the Verkhovna Rada of Ukraine], (30), 260 (in Ukrainian).
8. Orliuk, O. P. (2010) Finansove pravo [Finance law]. K: Yurinkom Inter (in Ukrainian).
9. Fedorenko, V. L. (2016) Konstytutsiine pravo Ukrainy [Constitutional law of Ukraine]. K: Lira (in Ukrainian).

**Received: 07/08/2021**
**1st Revision: 29/08/2021**
**Accepted: 18/09/2021**

**N. Mialovytska, Dr. Sc. (Law), Prof.**
**Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,**
**N. Zlatina, PhD (Law), Associate Prof.**
**Kyiv National Linguistic University, Kyiv, Ukraine**

## THE ROLE AND SIGNIFICANCE OF JUDICIAL PRECEDENT IN THE SYSTEM OF SOURCES OF LAW

***The article explores the concepts of sources of law and their main types. The source of law means the way of external influence of legal norms, which certifies their binding nature. The concepts and place of judicial precedent in the system of sources of law are defined. It is noted that judicial precedent should be understood as a court decision rendered in a particular case and entered into force, and which is the basis for resolving similar cases by other bodies. As part of the integration process in Europe, two important judicial bodies have been formed – the European Court of Human Rights (hereinafter – the ECtHR) and the Court of Justice. Each of these courts plays an important role in the rule-making process within its competence. The ECtHR's function is not limited to dealing with specific complaints. Its decisions also provide a comprehensive interpretation of the main provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms. As a result, they acquire a special significance that is precedent-setting. Therefore, the application of the case law of the ECtHR is considered as a source of law. It is also noted that EU courts play a role in the development of the rule-making process within the EU. They interpret the main provisions of the founding treaties and other regulations and formulate autonomous concepts and concepts that complement and clarify the provisions of regulations and implement new fundamentally important for the development of integration law provisions. Recognition of judicial precedent as a source of law means that judicial bodies perform not only a jurisdictional function (resolving conflicts on the basis of law), but also law-making. This function increases the role and importance of the judiciary in the mechanism of checks and balances of abuse of state power.***

***Keywords: source of law, judicial precedent, constitution, convention, European Union.***

**Bulletin of Taras Shevchenko National University of Kyiv.**
**Legal Studies, 2021; 4 (119): 53-59**
**УДК 342.7**
**DOI: https:doi.org/10.17721/1728-2195/2021/4.119-10**

ISSN 1728-2195
© Taras Shevchenko National University of Kyiv,
Publishing center "Kyiv University", 2021

**В. Р. Некрутенко, асп.**
**ORCID ID: 0000-0002-1333-5032**
**Київський національний університет імені Тараса Шевченка, Київ, Україна**

# ДО ПИТАННЯ СИСТЕМАТИЗАЦІЇ РИЗИКІВ, СПРИЧИНЕНИХ ОБРОБЛЕННЯМ ПЕРСОНАЛЬНИХ ДАНИХ ІЗ ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

***Метою дослідження є систематизація ризиків, які можуть бути викликані обробленням персональних даних із використанням технологій штучного інтелекту, за критерієм стадій оброблення персональних даних і норм законодавства, які можуть бути порушені внаслідок настання ризику.***

***На основі систематизації ризиків за мету було також поставлено проаналізувати засоби запобігання та мінімізації ризиків, викликаних використанням технологій штучного інтелекту.***

***Для досягнення мети цієї роботи використано загальнонаукові структурно-функціональний, системний, порівняльно-правовий методи, а також метод аналізу.***

***Серед спеціальнонаукових методів можна виокремити методи системного та динамічного тлумачення норм законодавства у сфері захисту персональних даних.***

***У ході дослідження отримано такі результати:***

- ***надано, проаналізовано за нормами законодавства України та систематизовано правові ризики, викликані обробленням персональних даних із використанням технологій штучного інтелекту;***
- ***установлено фактори й інтереси, з якими необхідно балансувати мінімізацію правових ризиків;***
- ***запропоновано складові комплексної регуляторної системи, спрямованої на мінімізацію ризиків і забезпечення балансу між інтересами фізичних осіб та організаціями, які здійснюють збір та оброблення персональних даних.***

***Отримані результати дозволили дійти таких висновків:***

***1. Використання алгоритмів штучного інтелекту у разі взаємодії з людиною дає беззаперечні переваги та соціальну вигоду.***

***2. Нерегульоване використання технології спричиняє значні ризики порушення права людини на повагу до приватного життя та право на захист персональних даних. Основними аспектами таких ризиків є незаконне використання зібраних персональних даних для машинного навчання, непрозорість і втрата контролю над логікою прийняття рішень і використанням алгоритмів, а також ризики порушення безпеки персональних даних.***

***3. Для мінімізації ризиків і забезпечення балансу між приватним і публічним інтересом необхідно знайти комплексний підхід, який передбачає залучення всіх зацікавлених сторін. Наявність комплексного підходу передбачає використання обов'язкових правил поведінки та норм так званого м'якого права.***

***Ключові слова: захист персональних даних; персональні дані; штучний інтелект; інноваційні технології; приватність; машинне навчання; дискримінація.***

## ВСТУП

За даними дослідницького центру "Gartner" [1], станом на 2019 р. приблизно 37 % організацій по всьому світу використовують технологію штучного інтелекту для виконання певних завдань, що є втричі більшим показником порівняно з 2015 р. Технології машинного навчання та штучного інтелекту починають застосовувати у практично будь-якій сфері життя: починаючи від

**© Некрутенко В. Р., 2021**

автоматичної генерації та редагування текстів до допомоги суддям у винесенні рішень і до вирішення питань щодо схвалення або відмови у розгляді кредитних заявок у фінансових установах.

Штучний інтелект допомагає автоматизувати й оптимізувати процеси, мінімізуючи людський фактор і надаючи вигоду його користувачам. У той же час, зі збільшенням ролі алгоритмів у прийнятті рішень, які раніше покладалися на людину, зокрема і рішень, які мають юридичні наслідки, ціна помилки та міра відповідальності за надійну та правомірну роботу алгоритмів стає все вищою.

Ця стаття дає огляд викликів і ризиків, пов'язаних з обробленням персональних даних із використанням технологій штучного інтелекту.

**Об'єктом дослідження** є суспільні відносини, що виникають у зв'язку з використанням технологій штучного інтелекту для оброблення персональних даних. **Предметом дослідження** є правове регулювання захисту персональних даних в умовах використання технологій штучного інтелекту.

**Мета статті** – актуалізувати проблемні питання використання штучного інтелекту для оброблення персональних даних і надати огляд шляхів їхнього можливого вирішення.

Теоретичною основою цієї статті є роботи таких науковців, як О. А. Заярний, Сандра Вахтер, Брент Міттельштадт, Майкл Вель, Мішель Фінк та ін. Окрім цього, вплив технологій штучного інтелекту проаналізовано у розрізі законодавства України та міжнародних стандартів із захисту персональних даних, стратегії Європейського Союзу щодо штучного інтелекту, а також роз'яснень європейських наглядових органів із захисту персональних даних.

## ОСНОВНІ РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

**І. Ризики використання технологій штучного інтелекту.** Оскільки важливою складовою цього дослідження є технологія штучного інтелекту, варто розпочати з визначення цій технології. Для цілей статті термін "штучний інтелект" застосовується у найбільш широкому значенні. А саме, для визначення штучного інтелекту взято визначення, надане в Енциклопедії Британіка [2]: здатність цифрового комп'ютера або керованого комп'ютером робота виконувати завдання, які зазвичай виконуються розумними істотами.

Особливий інтерес для вказаного дослідження складають алгоритми штучного інтелекту на основі машинного навчання, що означає створення алгоритмів шляхом пошуку закономірностей серед широкого обсягу даних на певну тему. Такі алгоритми, зазвичай, успадковують логіку поведінки та прийняття рішень людей, які є суб'єктами прийняття рішень у наборах тренувальних даних для машинного навчання.

Актуальність використання технологій штучного інтелекту для оброблення персональних даних спостерігається у приватному і публічному секторах. Унікальність цього явища полягає у тому, що штучний інтелект, за умови наявності необхідних технічних можливостей, може у перспективі застосовуватися у будь-якій сфері діяльності людини. Такі технології, як машинне навчання, дають можливість адаптувати логіку прийняття рішень алгоритму на основі попередніх рішень, виконаних людиною у тій чи іншій площині. Більше того, використання алгоритмів дозволяє мінімізувати вірогідність помилки, яка є високою у разі залучення у процес людини.

Для приватного сектора головним інтересом у використанні штучного інтелекту є збільшення економічної вигоди шляхом створення та подальшого використання наборів великих даних, що дозволять робити точніші й ефективніші економічні прогнози. Це, як приклад, дозволяє надавати більш якісні послуги, рекламувати та продавати товари або послуги ефективніше.

Використання технологій штучного інтелекту в публічному секторі допомагає забезпечити публічний порядок і підвищити якість публічних послуг. Окрім цього, це дозволяє мінімізувати людський фактор, який може призвести до дискримінації людини або корупційних правопорушень.

Ефективна робота алгоритмів, особливо тих, створення яких засновується на технологіях машинного навчання, передбачає постійне збільшення об'єму інформації про людину. Неконтрольоване прагнення збільшити обсяг даних, що збирають, спокушає до практик, за яких за життям людини встановлюється постійне спостереження.

Сучасна система взаємодії людини з мережею інтернет дозволяє збирати дані відвідувань вебсайтів користувачем, а технології так званого інтернету речей (IoT) дають можливість аналізувати інформацію про людину у місцях, які раніше залишалася поза зоною доступу до мережі інтернет. Наприклад, дані користування побутовими пристроями, як дані користування холодильником, кавовою машиною, або навіть дзеркалом.

Подібну практику можна спостерігати і в публічному секторі. Системи, які сьогодні забезпечують порядок і запобігають вчиненню правопорушень у публічних місцях, передбачають розміщення великої кількості засобів спостереження, зокрема і через камери відеоспостереження або відслідковування місцеперебування особи.

Усе більшої популярності набувають технології автоматизованого передбачення вчинення правопорушень людиною та розпізнавання через камеру відеоспостереження обличчя підозрюваного, який перебуває у публічному місці.

Збирання й оброблення персональних даних для створення, роботи або оптимізації алгоритмів штучного інтелекту, з одного боку, та подальше використання таких алгоритмів для прийняття рішення щодо людини, з іншого боку, спричиняє ризики. Відсутність контролю за алгоритмами може призвести до порушення прав, свобод та інтересів людини і, як наслідок, вимог відповідного законодавства України.

Для цілей цієї статті, під терміном "ризик" розуміють гіпотетичний сценарій настання події, що призведе до порушення права людини на приватність та/або на захист персональних даних. Ризики, у свою чергу, спричиняються певними внутрішніми або зовнішніми факторами (загрозами), які дозволять небажаній події статися.

Особливо ризиковим для людини вбачається використання автоматизованого прийняття рішень, яке має юридичні або подібні наслідки для людини. Як зазначено у керівних принципах Європейського наглядового органу WP29 відносно профілювання від 2017 р., до цієї сфери належать як юридично значимі рішення – винесення судового рішення, передбачення вірогідності вчинення людиною проступку тощо – так і рішення, які мають значний соціальний або економічний ефект [3, с. 21].

Прикладами останнього можуть слугувати автоматизоване прийняття рішень щодо працевлаштування кандидата на посаду, видачі кредиту або навіть персоналізована реклама товарів і послуг, яка впливає на визначення ціни запропонованих товарів або послуг.

За характером операцій з оброблення персональних даних можна виокремити два види ризиків:

1. *Ризики, пов'язані з використанням персональних даних для розроблення (тренування) алгоритмів штучного інтелекту.* Цей вид ризиків найчастіше характеризується вторинним характером оброблення персональних даних. Організація спочатку зібрала персональні дані для задоволення таких цілей, як надання

послуг або проведення аналізу поведінки певної групи людей, після чого використовує зібрану інформацію для процесу генерування комп'ютерних алгоритмів через пошук закономірностей і спільних ознак у наборі даних (технологія так званого машинного навчання). Для цього етапу характерні такі ризики:

- **непоінформованість людини** про намір використання її персональних даних для машинного навчання. Позбавлення людини інформації про використання її даних призводить до неможливості здійснювати контроль над обробленням;
- **позбавлення вибору (згоди)** людини щодо того, чи можна використовувати її персональні дані для машинного навчання. Як наслідок, людина втрачає можливість вибору та контролю над власними персональними даними;
- **ризик порушення захисту даних** та їхнього подальшого витоку у зв'язку з незабезпеченням безпеки процесу машинного навчання [4, с. 5]. У цьому розрізі на особливу увагу заслуговує невжиття додаткових організаційно-технічних заходів, як попереднє знеособлення даних, що може призвести до порушення конфіденційності та викриття особистості людини;
- **упереджені (biased), статистично неправильні та помилкові висновки алгоритмів**. Остання проблематика є особливо актуальною, оскільки відомості, на основі яких тренується алгоритм штучного інтелекту (наприклад, судові рішення), можуть носити дискримінаційний або нерепрезентативний характер. Як наслідок порушення методології проведення машинного навчання, штучний інтелект сприймає такі відомості за модель правильної поведінки, що призводить до ризику автоматизації порушення прав, свобод та інтересів людини.

2. *Ризики, пов'язані з використанням алгоритмів штучного інтелекту для генерування певних висновків або прийняття рішення щодо конкретної людини.* На цьому етапі організація аналізує "ввідні" персональні дані про людину (input data) за допомогою вже натренованої моделі штучного інтелекту для того, щоб отримати певні висновки або прогнози поведінки такої людини та, у певних випадках, прийняти рішення щодо неї (output data). Як приклад, сьогодні на основі ввідних даних про перегляди вебсторінок та інші дії людини в мережі інтернет алгоритм оцінює, яку саме рекламу показати та яку ціну сформувати під конкретного глядача такої реклами. Для другого виду характерні такі ризики:

- нездатність пояснити, чому саме було прийнято рішення щодо людини, що не дає можливості зробити висновки про законність рішення. Це може призвести до зміни поведінки людини у разі взаємодії зі штучним інтелектом, зниження довіри до алгоритмів, а також підвищення ризику зловживань зі сторони володільця персональних даних;
- порушення прав або економічних інтересів людини внаслідок помилкового рішення та нездатність отримати перегляд такого рішення.

У розрізі захисту права людини на повагу до приватного життя та права на захист персональних даних ключовий набір правил для оброблення встановлюється Законом України "Про захист персональних даних" [5] (далі – ЗУ).

Розглянемо детальніше, до порушення яких вимог законодавства України може призвести оброблення персональних даних із використанням технологій штучного інтелекту:

1. Неправомірне вторинне використання персональних даних без відома та згоди людини для машинного навчання порушує вимоги щодо чітко встановленої мети оброблення персональних даних (ч. 1 ст. 6 ЗУ), а також наявності необхідних правових підстав для цього (ст. 11 ЗУ).

Вказана проблема, зокрема, була актуалізована раніше вченим С. М. Брайчевським в огляді оброблення персональних даних із використанням технологій штучного інтелекту та інтернету речей. Як зазначає дослідник, для створення детального профілю людини можуть застосовуватися вже існуючі набори персональних даних, про використання яких людина може не мати уявлення. Такі дані можуть бути пізніше використані у неправомірних цілях володільцем персональних даних або третіми особами [25].

2. Нездатність пояснити логіку роботи алгоритмів призводить до порушення принципу прозорості оброблення персональних даних (ч. 1 ст. 6 ЗУ), а також принципу точності та достовірності персональних даних, отриманих унаслідок такого оброблення (ч. 2 ст. 6 ЗУ). Одним із найбільших ризиків аналізу великих даних та автоматизованого прийняття рішень є втрата контролю над сприйняттям алгоритмами людей і передбачуваність чи інтуїтивний зв'язок між діями та сприйняттям інших [6, с. 97]. Ця проблема проявляється у кількох аспектах:

- неточність ввідних даних людини або побудованого алгоритму може призвести до помилкових висновків і негативних наслідків для людини. Як приклад, у кінці 2020 р. людина у Сполучених Штатах Америки помилково отримала 10 діб ув'язнення внаслідок, як зазначає її адвокат, використання технології для автоматизованого пошуку та розпізнавання правопорушників через камери відеоспостереження [7];
- відсутність належного контролю процесу машинного навчання може також призвести до того, що алгоритм перейняв упередженість людини, на рішеннях якої здійснювалось машинне навчання (algorithmic bias / discrimination);
- у випадку, коли людина не розуміє логіки прийняття рішень/висновків, це може призвести до зміни поведінки людини та стримування у прийнятті рішень. Унаслідок некоректно обраного методу натреновані нейронні мережі можуть мати проблему 'black box', яка означає, що організація-оператор мережі нездатна пояснити, яким чином алгоритм приймає рішення.

Нерозуміння механізму та наслідків взаємодії з алгоритмами може призводити до зміни лінії поведінки людини та самоцензури. [8, с. 14] Особливо актуальною проблема непрозорості алгоритмів є для сфер із підвищеним публічним інтересом – наприклад, судова система, де обґрунтування рішення має бути прозорим і відповідати високим стандартам.

3. Неправомірне використання систем штучного інтелекту порушує вимоги щодо наявності законної підстави для оброблення персональних даних (ст. 7, 8 та 11 ЗУ). До цієї групи ризиків належать:

- неправомірне отримання та розголошення даних, оброблення яких становить особливий ризик для прав, свобод та інтересів людини (ст. 8). Наприклад, визначення стану здоров'я людини через запис її голосу побутовим IoT-приладом голосової допомоги [9];
- таргетована цензура інформації, що отримує людина в медіа, та створення ефекту інформаційної бульбашки. Такі алгоритмічні обмеження здійснюються часто без відома та згоди людини, що порушує не тільки право на захист персональних даних (ст. 11 ЗУ), але і право на доступ до інформації людини, призводить до дискримінації у доступі до товарів і послуг [10, с. 6] тощо.

4. Недостатній рівень інформаційної безпеки систем із використанням технологій штучного інтелекту порушує вимоги щодо забезпечення захисту персональних даних (ст. 24 ЗУ). Дослідження безпеки алгоритмів ма-

шинного навчання показують, що використання такої технології несе як загальні безпекові ризики, характерні для всіх інформаційних систем, так і створює нові. Зокрема, певні види атак (Membership inference, Model inversion attack [4, с. 8]) дозволяють отримати доступ до персональних даних, які використовувалися для машинного навчання, маючи попередньо доступ до певного обсягу інформації про людину.

Варто згадати, що питанню дотримання вимог законодавства із захисту персональних даних було приділено увагу на рівні української правової доктрини. Зокрема, канд. юрид. наук. Т. Г. Каткова у статті "Штучний інтелект в Україні: правові аспекти" наголошує на дотриманні таких аспектів захисту персональних даних, як забезпечення конфіденційності даних, отримання згоди від людини, а також безпека персональних даних [26].

Утім, авторкою не було чітко розмежовано, про що саме йдеться у понятті конфіденційність даних. Це поняття пізніше за текстом ототожнюється із "забезпеченням захисту персональних даних". Із цього приводу доцільно зазначити, що конфіденційність і захист персональних даних або приватності не тотожні між собою: конфіденційність є лише одним з аспектів забезпечення приватності та полягає у нерозголошенні персональних даних у такий спосіб, який не був дозволений людиною або порушує вимогу законодавства.

Неприпустимою також вбачається пропозиція вченої щодо регуляторного вибору між "інформованою" та "диференційованою" згодою на оброблення персональних даних при написанні стратегії регулювання підстав для оброблення персональних даних за допомогою технологій штучного інтелекту [26]. На нашу думку, згода на оброблення персональних даних може бути законною лише у тому випадку, якщо вона відповідає обом стандартам, а також є вільно наданою та недвозначною. Підтримку подібної позиції можна віднайти в законодавстві із захисту персональних даних Європейського Союзу, яке встановлює вимоги до згоди як підстави для оброблення персональних даних (ст. 7 Регламенту 2016/680) [13].

## II. Необхідність забезпечення балансу інтересів

Як підсумок описаної вище проблематики, подальше розроблення та імплементація технологій штучного інтелекту для оброблення персональних даних надає і безспірні переваги, і спричиняє виникнення значних ризиків для прав, свобод та інтересів людини.

У подібних ситуаціях розвиток сфери має супроводжуватися дотриманням балансу інтересів та послідовним управлінням ризиками. Як приклад, Європейська комісія у стратегії щодо штучного інтелекту [11, с. 1] визначає дві ключові цілі Союзу:

**1. Підтримка та подальше заохочення розробок і розвитку технології штучного інтелекту.** Сфера розробки технологій штучного інтелекту є висококонкурентною – одними з найсильніших гравців у цій сфері є Сполучені Штати Америки та Китайська народна республіка. Європейський Союз ставить за ціль мати змогу конкурувати з лідерами у сфері розробки штучного інтелекту;

**2. Дотримання основоположних прав людини та цінностей Європейського Союзу.** Для розуміння того, про які саме цінності йдеться варто звернутися до Хартії ЄС про основоположні права (ст. 7 та 8) [12] та пов'язані з нею інші акти ЄС – наприклад, Загальний регламент про захист даних ЄС 2016/680 [13]. У першу чергу, мова йде про недискримінацію людини, повагу до права на приватність, захист персональних даних, гідність тощо.

## III. Складові комплексної регуляторної системи

З огляду на складність систем із використанням штучного інтелекту та наявність великої кількості ролей, задіяних у їхньому функціонуванні, адресувати всі названі ризики лише одним інструментом не вбачається можливим.

О. А. Заярний пропонує таку класифікацію напрямів удосконалення способів захисту інформаційних прав: юридичний напрям та етичний (морально-психологічний) напрям [14, с. 96]. Учений зазначає, що кожен із напрямів має проявлятися як у нормативному і правозастосовному розширенні існуючої в нормах законодавства України системи способів захисту, так і в закріпленні нових способів впливу на порушників, безпосередньо пов'язаних зі сферою застосування технологій штучного інтелекту. У розрізі теми цієї статті цікавими, у першу чергу, є правові й етичні стандарти захисту права на повагу до приватного життя та права на захист персональних даних.

Дійсно, мінімізація ризиків, викликаних використанням штучного інтелекту, можлива лише за умови системного підходу до проблематики. Як приклад, наглядовий орган із захисту інформації Великої Британії вважає, що крім вимог і керівних принципів, яким має відповідати штучний інтелект, доцільно розробляти комплексні регуляторні системи (frameworks) з аудиту систем зі штучним інтелектом, які допоможуть знайти та забезпечити необхідний баланс між інтересами сторін відносин [15].

Розглянемо деякі з прикладів складових регуляторної системи, які покликані допомогти знайти необхідний баланс між економічної вигодою та захистом права на повагу до приватного життя у процесі обробляння персональних даних із використанням штучного інтелекту.

**Міжнародні правові й етичні принципи та стандарти,** яким має відповідати оброблення персональних даних із використанням штучного інтелекту. Цінність цього інструменту полягає в першу чергу, у можливості створити між країнами спільний підхід до регулювання, який позитивно сприятиме інтеграційним процесам і глобалізації економіки. Як приклади можна навести Азіломарські принципи штучного інтелекту [16], які визначають керівні засади та цілі, у яких мають проводитися подальші дослідження у сфері штучного інтелекту. Серед основних таких принципів закріплені повага до приватного життя, захист персональних даних і забезпечення контролю людини за рішеннями штучного інтелекту.

**Закріплення захисту персональних даних і захисту права на приватність як складової політики держави у сфері штучного інтелекту**. Подібні заходи дозволяють ієрархічно зробити акцент на захисті персональних даних, що пізніше відобразиться у кроках, спрямованих на реалізацію політики. У цьому розрізі варто звернути увагу на Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р "Про схвалення Концепції розвитку штучного інтелекту в Україні". Недостатній рівень захисту персональних даних визнається в постанові як одна з першочергових проблем, а тому належний захист персональних даних закріплюється одним із принципів розвитку та використання технологій штучного інтелекту [17].

**Спеціальні законодавчі норми**. З огляду на високий рівень ризиковості використання штучного інтелекту у випадку взаємодії з людиною, доцільним вбачається закріплення спеціальних правил, що заповнюють прогалини в законодавстві із захисту персональних даних. Такими спеціальними правилами можуть бути:

1) норми, що стосуються певного сектора оброблення персональних даних (наприклад, правоохоронна діяльність [18]);

2) норми, що деталізують існуючі права та свободи людини. Зокрема, вбачається необхідність у доповненні права людини бути поінформованою щодо того, яким чином приймає рішення система з використанням штучного інтелекту [13, ст. 13]. Деякі з країн, зокрема Словенія, деталізує також і підхід до оцінювання ризиків у разі використання штучного інтелекту, вимагаючи додаткового проведення "оцінки впливу алгоритмів" (algorithmic impact assessment) на оброблення персональних даних [19, с. 7];

3) норми, що закріплюють специфічні права, пов'язані із застосуванням технології штучного інтелекту. 2016 р. Європейський Союз значно деталізував права людини, пов'язані з автоматизованим прийняттям рішень, що мають юридичні або подібні наслідки. Було закріплено значне обмеження сфер застосування таких рішень, а також право на втручання людини у процес прийняття рішення й оспорювати рішення, прийняте повністю автоматизовано [12, ст. 22]. У той же час, як зазначає український вчений І. М. Городиський, Європейський Парламент наполягає на необхідності додаткового врегулювання окремих аспектів захисту персональних даних у цій сфері [27]. Як приклад, наводиться питання використання камер і сенсорів у робототехніці. На сьогодні в Європі також триває наукова дискусія щодо закріплення нового права людини на обґрунтовані висновки, зроблені штучним інтелектом [6, с. 81].

Варто зазначити, що ЗУ "Про захист персональних даних" (п. 13 ч. 2 ст. 8) також закріплює право людини "на захист від автоматизованого рішення, яке має для неї правові наслідки". Об'єктом регулювання цієї статті є, у тому числі, прийняття автоматизованих рішень за допомогою алгоритмів штучного інтелекту. У той же час, ця норма потребує деталізації у таких аспектах: чи відноситься це право лише до повністю автоматизованих рішень, чи також таких, що приймаються із залученням людського фактора; а також, що розуміти під "правом на захист" та яким чином його можна реалізувати.

**Роз'яснення, керівні принципи та публічні консультації наглядових органів**. Більшість норм із захисту персональних даних розробляються "технологічно-нейтральними", тобто такими, що не мають прив'язки до конкретної технології та застосовуються до широкого кола суспільних відносин. Це, у свою чергу, обумовлює високий ступінь абстрактності та загальності правил, що викликає необхідність у подальшому тлумаченні норм. Допомогти у цьому можуть роз'яснення компетентних органів (норми так званого м'якого права), спрямовані на деталізацію правил поведінки у конкретних сценаріях з оброблення. За приклад можна поставити роз'яснення щодо захисту персональних даних у штучному інтелекті одразу двох країн: США [20] і Великої Британії [21].

**Розроблення сертифікацій, кодексів поведінки та стандартизації у сфері штучного інтелекту**. Розроблення стандартів і найкращих практик дозволяє, з одного боку, виробити уніфіковану модель поведінки, якої можуть дотримуватися учасники ринку для правомірного використання технології. З іншого боку, прийнявши зобов'язання дотримуватися певного стандарту, організація може тим самим продемонструвати відповідність вимогам і належний рівень захисту персональних даних перед іншими сторонами. Як приклад стандартизації у публічній площині можна навести кодекс належної поведінки Національної системи охорони здоров'я, який застосовується до використання штучного інтелекту у процесі взаємодії з пацієнтами [22]. Іншим прикладом можуть послугувати такі ініціативи представників індустрії, як "Open Ethics", ціллю яких є стандартизація форми надання повідомлення про оброблення персональних даних із використанням технологій штучного інтелекту [23].

**Створення регуляторних "пісочниць" (sandboxes).** У межах цієї ініціативи компетентний регуляторний орган запрошує до співпраці проєкти з використанням штучного інтелекту, які отримують фінансову, правову й організаційну допомогу від експертів і наглядових органів у сфері захисту персональних даних. На окрему увагу у цьому розрізі заслуговують ініціативи Норвезького наглядового органу із захисту персональних даних, який створив спеціальну "пісочницю" під проєкти, які розробляють технології штучного інтелекту. Метою цієї ініціативи є сприяння розробленню інноваційних рішень зі штучного інтелекту, які з погляду захисту даних є етичними та відповідальними [24].

## ВИСНОВКИ

Аналіз поточної ситуації з використання технологій штучного інтелекту для оброблення персональних даних дозволяє дійти кількох висновків.

Використання алгоритмів штучного інтелекту у процесі взаємодії з людиною дає беззаперечні переваги й соціальну вигоду, дозволяючи підвищити ефективність прийняття рішень і знизити ризик помилки з огляду на людський фактор. Переваги використання штучного інтелекту є актуальними як для публічного, так і для приватного сектора з огляду на універсальність алгоритмізації та здатності точного налаштування рішень на основі попередніх даних про логіку прийняття рішень у тому чи іншому секторі.

Водночас нерегульоване використання технології спричиняє значні ризики порушення прав, свобод та інтересів людини, зокрема і право на повагу до приватного життя та право на захист персональних даних. Основними аспектами ризиків є незаконне використання зібраних персональних даних для машинного навчання, непрозорість і втрата контролю над логікою прийняття рішень і використанням алгоритмів, а також ризики порушення безпеки персональних даних.

Для мінімізації ризиків і забезпечення балансу між приватним і публічним інтересами, пов'язаними з використанням технології, необхідно знайти комплексний підхід, який передбачає залучення всіх зацікавлених сторін. Для забезпечення такого балансу необхідно використовувати і загальнообов'язкові правила поведінки, і норми м'якого права, стандартизацію, закріплення принципів, на яких має будуватися штучний інтелект на міжнародному та найвищому національних рівнях, і створення сприятливого регуляторного середовища, як регуляторні "sandboxes".

**Список використаних джерел:**

1. STAMFORD, Conn.: Gartner Survey Shows 37 Percent of Organizations Have Implemented AI in Some Form // Gartner. January 21, 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have (дата звернення: 20.02.2021).

2. Copeland, B.J.. "Artificial intelligence". *Encyclopedia Britannica*, URL: https://www.britannica.com/technology/artificial-intelligence. Accessed 29 March 2021.

3. Working Party 29: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). October 3, 2017. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (дата звернення: 01.03.2021).

4. Veale Michael, Binns Reuben and Edwards Lilian: Algorithms that remember: model inversion attacks and data protection law. 2018. Phil. Trans. R. Soc. A.3762018008320180083. URL: http://doi.org/10.1098/rsta.2018.0083 (дата звернення: 01.03.2021).

5. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/main/2297-17 (дата звернення: 04.03.2021).

6. Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI

(October 5, 2018). Columbia Business Law Review, 2019(2). URL: https://ssrn.com/abstract=3248829 (дата звернення: 04.03.2021).

7. A man spent 10 days in jail based on a facial recognition error: Article // Inputmag. December 29, 2020. URL: https://www.inputmag.com/tech/a-man-spent-10-days-in-jail-based-on-misclassification-by-clearview-ai (дата звернення: 05.03.2021).

8. PENAMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 3–4 (2013); Jonathon W. Penney, Chilling Effects: Online Surveillance and Wikipedia Use (Sept. 8, 2016). URL: https://papers.ssrn.com/abstract=2769645[https://perma.cc/FGW8-WMVP (дата звернення: 05.03.2021).

9. James Cook, Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine, TELEGRAPH (Oct.9, 2018), URL: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/ https://perma.cc/V346-HFWE (дата звернення: 05.03.2021).

10. Finck, Michèle and Biega, Asia, Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems (January 11, 2021). Max Planck Institute for Innovation & Competition Research Paper No. 21-04, URL: https://ssrn.com/abstract=3749078 (дата звернення: 05.03.2021).

11. White Paper 'On artificial intelligence – A European approach to excellence and trust', Brussels, 19.2.2020 COM (2020) 65 final. URL: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (дата звернення: 09.03.2021).

12. Хартія основних прав Європейського Союзу від 7 грудня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/994_524 (дата звернення: 09.03.2021).

13. 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 (дата звернення: 09.03.2021).

14. Заярний О.А. Деякі напрями удосконалення способів захисту інформаційних прав фізичних осіб в умовах застосування технологій штучного інтелекту. Актуальні проблеми захисту інформаційних прав особи в умовах технологічних викликів та цифрової реальності: Збірник матеріалів Міжнародної науково-практичної конференції. Херсон: ВД "Гельветика", 17-18 вересня 2019. С. 94-98.

15. A call for participation: Building the ICO's auditing framework for Artificial Intelligence // Information commissioner's office official website. 18 March 2019. URL: https://ico.org.uk/about-the-ico/news-and-events/ai-blog-a-call-for-participation/ (дата звернення: 07.04.2021).

16. Asilomar AI Principles. January 17, 2017 // Future of life. URL: https://futureoflife.org/ai-principles/ (дата звернення: 10.03.2021).

17. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження 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: 07.04.2021).

18. Artificial Intelligence and law enforcement: challenges and opportunities. December 01, 2020 // Interpol website. URL: https://www.interpol.int/en/News-and-Events/News/2020/Artificial-Intelligence-and-law-enforcement-challenges-and-opportunities (дата звернення: 10.03.2021).

19. Kaminski, Margot E. and Malgieri, Gianclaudio, Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations (September 18, 2019). International Data Privacy Law, 2020, forthcoming., U of Colorado Law Legal Studies Research Paper No. 19-28, URL: https://ssrn.com/abstract=3456224 (дата звернення: 10.03.2021).

20. Guidance on AI and data protection // Information commissioner's office official website. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-artificial-intelligence-and-data-protection/ (дата звернення: 07.04.2021).

21. Using Artificial Intelligence and Algorithms // FTC official website, Apr 8 2020. URL: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms (дата звернення: 07.04.2021).

22. A guide to good practice for digital and data-driven health technologies. Updated 19 January 2021 // UK's Department of Health and Social Care. URL: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (дата звернення: 10.03.2021).

23. Open Ethics Initiative. Ethics as Open Data. URL: https://openethics.ai/ (дата звернення: 10.03.2021).

24. Sandbox for responsible artificial intelligence // Datatilsynet website. URL: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/ (дата звернення: 07.04.2021).

25. Брайчевський С.М. Проблема персональних даних в системах інтернету речей з елементами штучного інтелекту. Інформація і право. No 4(31)/2019. URL: https://ippi.org.ua/sites/default/files/9_13.pdf (дата звернення: 11.05.2021).

26. Каткова Т. Г. Штучний інтелект в Україні: правові аспекти. Журнал "Право і Суспільство" No6/2020. Харків – 2020. URL: http://pravoisuspilstvo.org.ua/archive/2020/6_2020/10.pdf (дата звернення: 05.11.2021).

27. Городиський І.М. Тенденції розвитку правового регулювання штучного інтелеку в Європейському Союзі. ІТ право: проблеми і перспективи розвитку в Україні (друга міжнародна щорічна конференція). Львів – 2017. URL: http://aphd.ua/publication-388/ (дата звернення: 05.11.2021).

**References:**

1. Stamford, Conn.: Gartner Survey Shows 37 Percent of Organizations Have Implemented AI in Some Form // Gartner. January 21, 2019. URL: https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have (acceed: 20.02.2021).

2. Copeland, B.J.. "Artificial intelligence". *Encyclopedia Britannica*, URL: https://www.britannica.com/technology/artificial-intelligence. Accessed 29 March 2021.

3. Working Party 29: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01). October 3, 2017. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (acceed: 01.03.2021).

4. Veale Michael, Binns Reuben and Edwards Lilian: Algorithms that remember: model inversion attacks and data protection law. 2018. Phil. Trans. R. Soc. A.3762018008320180083. URL: http://doi.org/10.1098/rsta.2018.0083 (acceed: 01.03.2021).

5. Pro zahyst personalnyh danyh, Zakon Ukrain'y [On personal data protection, Law of Ukraine] № 2297-VI (2010). URL: https://zakon.rada.gov.ua/laws/main/2297-17 (acceed: 04.03.2021).

6. Wachter, Sandra and Mittelstadt, Brent, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI (October 5, 2018). Columbia Business Law Review, 2019(2). URL: https://ssrn.com/abstract=3248829 (дата звернення: 04.03.2021).

7. A man spent 10 days in jail based on a facial recognition error: Article // Inputmag. December 29, 2020. URL: https://www.inputmag.com/tech/a-man-spent-10-days-in-jail-based-on-misclassification-by-clearview-ai (acceed: 05.03.2021).

8. PENAMERICA, CHILLING EFFECTS: NSA SURVEILLANCE DRIVES U.S. WRITERS TO SELF-CENSOR 3–4 (2013); Jonathon W. Penney, Chilling Effects: Online Surveillance and Wikipedia Use (Sept. 8, 2016). URL: https://papers.ssrn.com/abstract=2769645[https://perma.cc/FGW8-WMVP (acceed: 05.03.2021).

9. James Cook, Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine, TELEGRAPH (Oct.9, 2018), URL: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/ https://perma.cc/V346-HFWE (дата звернення: 05.03.2021).

10. Finck, Michèle and Biega, Asia, Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems (January 11, 2021). Max Planck Institute for Innovation & Competition Research Paper No. 21-04, URL: https://ssrn.com/abstract=3749078 (acceed: 05.03.2021).

11. White Paper 'On artificial intelligence – A European approach to excellence and trust', Brussels, 19.2.2020 COM (2020) 65 final. URL: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (acceed: 09.03.2021).

12. Khartiya osnovnykh prav Yevropeys'koho Soyuzu [Charter of Fundamental Rights of the European Union] (2000). URL: https://zakon.rada.gov.ua/laws/show/994_524 (acceed: 09.03.2021).

13. 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 (acceed: 09.03.2021).

14. Zayarnyy, O.A. (2019) Deyaki napryamy udoskonalennya sposobiv zahystu informatsiynukh prav fizychnyh osib v umovah zastosyvannya technologiy shtuchnogo intellectu. Aktual'ni problemy zakhystu informatsiynykh prav osoby v umovakh tekhnolohichnykh vyklykiv ta tsyfrovoyi real'nosti [Some directions of improvement of ways of protection of information rights of individuals in the conditions of application of technologies of artificial intelligence. Relevant problems of protection of information rights of the person in the conditions of technological challenges and digital reality]. Zbirnyk materialiv Mizhnarodnoyi naukovo-praktychnoyi konferentsiyi. Kherson: VD "Hel'vetyka" [collection of publications of the International Scientific and Practical Conference. Kherson: Publisher "Helvetica"] (2019). pp. 94-98.

15. A call for participation: Building the ICO's auditing framework for Artificial Intelligence // Information commissioner's office official website. 18 March 2019. URL: https://ico.org.uk/about-the-ico/news-and-events/ai-blog-a-call-for-participation/ (acceed: 07.04.2021).

16. Asilomar AI Principles. January 17, 2017 // Future of life. URL: https://futureoflife.org/ai-principles/ (дата звернення: 10.03.2021).

17. Pro shvalennya Conceptcii rozvytku shtuchnoho intelektu v Ukraini, Rosporyadzhennya Cabinetu Ministriv Ukrain'y [On approving of the Concept of the development of AI in Ukraine, Order of the Cabinet of Ministers of Ukraine] № 1556-p (2020). URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (acceed: 07.04.2021).

18. Artificial Intelligence and law enforcement: challenges and opportunities. December 01, 2020 // Interpol website. URL: https://www.interpol.int/en/News-and-Events/News/2020/Artificial-Intelligence-and-law-enforcement-challenges-and-opportunities (acceed: 10.03.2021).

19. Kaminski, Margot E. and Malgieri, Gianclaudio, Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations (September 18, 2019). International Data Privacy Law, 2020, forthcoming., U of Colorado Law Legal Studies Research Paper No. 19-28, URL: https://ssrn.com/abstract=3456224 (acceed: 10.03.2021).

20. Guidance on AI and data protection // Information commissioner's office official website. URL: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/guidance-on-artificial-intelligence-and-data-protection/ (acceed: 07.04.2021).

21. Using Artificial Intelligence and Algorithms // FTC official website, Apr 8 2020. URL: https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms (acceed: 07.04.2021).

22. A guide to good practice for digital and data-driven health technologies. Updated 19 January 2021 // UK's Department of Health and Social Care. URL: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (acceed: 10.03.2021).

23. Open Ethics Initiative. Ethics as Open Data. URL: https://openethics.ai/ (acceed:10.03.2021).

24. Sandbox for responsible artificial intelligence // Datatilsynet website. URL: https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/ (acceed: 07.04.2021).

25. Braychevs'kyy S.M. Problema personal'nykh danykh v systemakh internetu rechey z elementamy shtuchnoho intelektu. Informatsiya i pravo. [The problem of personal data in the systems of the internet of things with elements of artificial intelligence. Information and law.] No 4(31)/2019. URL: https://ippi.org.ua/sites/default/files/9_13.pdf (acceed: 05.11.2021).

26. Katkova T. H. Shtuchnyy intelekt v ukrayini: pravovi aspekty. Zhurnal "Pravo i Suspil'stvo" [Artificial intelligence in Ukraine: legal aspects. Magazine "Law and Society"] No6/2020. Kharkiv – 2020. URL: http://pravoisuspilstvo.org.ua/archive/2020/6_2020/10.pdf (acceed: 05.11.2021).

27. Horodys'kyy I.M. Tendentsiyi rozvytku pravovoho rehulyuvannya shtuchnoho inteleku v Yevropeys'komu Soyuzi. IT pravo: problemy i perspektyvy rozvytku v Ukrayini (druha mizhnarodna shchorichna konferentsiya) [Trends in the development of legal regulation of artificial intelligence in the European Union. IT law: problems and prospects of development in Ukraine (second international annual conference)]. Lviv – 2017. URL: http://aphd.ua/publication-388/ (acceed: 05.11.2021).

**Received: 05/05/2021**
**1st Revision: 01/07/2021**
**Accepted: 20/09/2021**

**V. Nekrutenko, PhD Student**
**Taras Shevchenko National University of Kyiv, Kyiv, Ukraine**

## ON THE SYSTEMATISATION OF RISKS CAUSED BY THE PROCESSING OF PERSONAL DATA USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES

***The purpose of the study in this article is to systematise the risks that may be caused by the processing of personal data using artificial intelligence technologies, according to the criteria of stages of personal data processing and legislation that may be violated due to those risks. Based on the systematisation of risks, the aim was also to analyse the means of preventing and minimising the risks caused by the use of artificial intelligence technologies.***

***To achieve the purpose of this work, the following methods were used: structural, functional, systemic, comparative, as well as the method of analysis. Among the special scientific methods are methods of systematic and dynamic interpretation of legislation in the field of personal data protection.***

***The study analysed in accordance with the legislation of Ukraine and systematised legal risks caused by the processing of personal data using artificial intelligence technologies; identified factors and interests with which it is necessary to balance the minimisation of legal risks; proposed components of a comprehensive regulatory system aimed at minimising risks and ensuring a balance between the interests of individuals and organisations that collect and process personal data. The obtained results allowed to come to the following conclusions: 1) The use of artificial intelligence algorithms in human interaction gives undeniable advantages and social benefits; 2) Unregulated use of this technology poses significant risks of violation of the human right for respect for private life and the right to protection of personal data. The main aspects of such risks are the illegal use of collected personal data for machine learning, opacity and loss of control over the logic of decision-making, as well as the risks of breach of personal data security; 3) In order to minimise risks and ensure a balance between private and public interest, it is necessary to find a comprehensive approach that involves all stakeholders. An integrated approach involves the application of mandatory rules of conduct and the rules of so-called soft law.***

***Keywords: personal data protection; personal data; Artificial Intelligence; innovative technologies; privacy; machine learning; discrimination.***

**Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies, 2021; 4 (119): 59-63**
**УДК 340.12**
**DOI: https:doi.org/10.17721/1728-2195/2021/4.119-11**

ISSN 1728-2195
© Taras Shevchenko National University of Kyiv, Publishing center "Kyiv University", 2021

**Г. З. Остапенко, канд. юрид. наук, доц.**
**ORCID ID: 0000-0003-0529-2551**
**Київський національний університет імені Тараса Шевченка, Київ, Україна**

# ПРАВОВА ВИЗНАЧЕНІСТЬ У КОНТЕКСТІ РЕФОРМИ МІСЦЕВОГО САМОВРЯДУВАННЯ

***Висвітлено питання дотримання правової визначеності у процесі реалізації повноважень органами місцевого самоврядування, що були значно розширені в ході проведення реформи місцевого самоврядування. Визначено, що у процесі здійснення органами державної влади повноважень, які в ході реформи були передані до органів місцевого самоврядування, важливим був принцип правової визначеності. Цей принцип вимагає чіткості і зрозумілості законодавчих положень, передбачуваності рішень органів влади, обмеження дискреційних повноважень, вимогу до оприлюднення правових актів і доведення їх до відома громадян наперед та інші елементи. Стверджується, що ці ж вимоги, які складають зміст принципу правової визначеності, мають бути застосовані і у процесі реалізації повноважень органами місцевого самоврядування.***

***Одним з аспектів правової визначеності визнається повага до легітимних очікувань громадян, натомість проаналізована судова практика свідчить, що численними є випадки порушення цієї вимоги правової визначеності під час реалізації повноважень органами місцевого самоврядування. Акцентується увага на недопущенні подібної практики та на необхідності дотримання правової визначеності як обов'язкової вимоги верховенства права.***

***Визначено необхідність дотримання вимог правової визначеності під час оприлюднення актів органами місцевого самоврядування і доведення їхнього змісту до відома громадян.***

***Ключові слова: місцеве самоврядування, правова визначеність, легітимні очікування, визначеність законодавства, верховенство права, децентралізація.***

## ВСТУП

Реформа місцевого самоврядування є умовою демократизації, децентралізації та одним із проявів народовладдя, що визнає право вирішувати питання місцевого значення безпосередньо територіальними громадами, прав та інтересів яких такі питання стосуються. Нині реформа місцевого самоврядування пройшла відповідні етапи, адже після формування територіальних громад, проведення місцевих виборів, відбулося формування нових органів, які наділені необхідною компетенцією для вирішення питань місцевого значення. Питання, які раніше належали до сфери відання державних органів, були передані органам місцевого самоврядування, які набули не тільки прав, а й обов'язків перед членами громади за їхнє здійснення. Отже, постає питання належного здійснення таких повноважень. Ви-

© Остапенко Г. З., 2021