УДК 342.7:004.8

https://doi.org/10.52058/3041-1254-2026-1(23)-855-865

Криштанович Світлана Володимирівна доктор педагогічних наук, професор, професор кафедри педагогіки та психології, Львівський державний університет фізичної культури імені Івана Боберського, Львів, https://orcid.org/0000-0002-2147-9028

Криштанович Мирослав Франкович доктор наук з державного управління, професор, завідувач кафедри загальновійськової підготовки, Національний університет «Львівська політехніка», Львів, https://orcid.org/0000-0003-1750-6385

ПРАВА І СВОБОДИ ЛЮДЕЙ В ЕПОХУ МАСОВОГО ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ: СУЧАСНИЙ ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ СТАБІЛІЗАЦІЇ ТА ЗАХИСТУ

Анотація. Мета дослідження полягає у визначенні та теоретичному обґрунтуванні сучасного організаційного і правового механізму стабілізації та захисту прав і свобод людей в умовах масового впровадження технологій на базі штучного інтелекту. Об’єктом дослідження є суспільні відносини, що виникають у процесі розроблення, впровадження та використання технологій на базі штучного інтелекту і впливають на реалізацію та захист прав і свобод людей. Визначено ключові суспільні та правові виклики, що виникають у період масового впровадження технологій на базі штучного інтелекту, коли автоматизовані моделі дедалі частіше застосовуються для ухвалення рішень у сфері публічних послуг і комерційних сервісів. Охарактеризовано вплив алгоритмічних рекомендацій і профілювання на реалізацію права на приватність і захист персональних даних, права на рівність і недискримінацію, свободи вираження поглядів, а також права людини на справедливу процедуру і ефективний засіб правового захисту. Встановлено, що непрозорість моделі, дефіцит пояснюваності та складність простеження відповідальності між розробником, постачальником і користувачем створюють бар’єри для оскарження рішень, а масштабованість алгоритмічних помилок перетворює локальні збої на системні наслідки. Доведено, що поширення генеративних інструментів посилює ризики маніпуляцій інформацією та підробок зображення і голосу, що впливає на репутацію, автономію особи та довіру до доказів у публічній комунікації. Обґрунтовано необхідність комплексної нормативної відповіді, яка поєднує ризик орієнтоване регулювання, правила прозорості та вимоги до людського контролю, а також взаємодію із режимами

захисту персональних даних і цифрового середовища. Доведено, що стабілізація і захист досягаються лише за умови організаційних процедур, які працюють на всіх стадіях, починаючи з керування даними та оцінювання впливу на права і свободи, продовжуючи вимогами документування, повідомлення людини про використання автоматизованих рішень, забезпеченням можливості пояснення результату, і завершуючи аудитом, моніторингом інцидентів, відповідальністю постачальників і користувачів, а також доступними каналами скарг і відшкодування.

Ключові слова: права людини, парадигма свободи, організаційний і правовий механізм, штучний інтелект.

Kryshtanovych Svitlana Volodymyrivna Doctor of Pedagogical Sciences, Professor, Professor of the Department of Pedagogy and Psychology, Ivan Bobersky Lviv State University of Physical Culture Lviv, https://orcid.org/0000-0002-2147-9028

Kryshtanovych Myroslav Frankovych Doctor of Science in Public Administration, Professor, Head of the Department of Military Training, Lviv Polytechnic National University, Lviv, https://orcid.org/0000- 0003-1750-6385

HUMAN RIGHTS AND FREEDOMS IN THE ERA OF MASS IMPLEMENTATION OF TECHNOLOGIES BASED ON ARTIFICIAL INTELLIGENCE: A MODERN ORGANIZATIONAL AND LEGAL MECHANISM OF STABILIZATION AND PROTECTION

Abstract. The purpose of the study is to identify and theoretically substantiate a modern organizational and legal mechanism for stabilizing and protecting human rights and freedoms in the context of the mass introduction of technologies based on artificial intelligence. The object of the study is social relations that arise in the process of developing, implementing and using technologies based on artificial intelligence and affect the implementation and protection of human rights and freedoms. The key social and legal challenges that arise during the period of mass introduction of technologies based on artificial intelligence, when automated models are increasingly used for decision-making in the field of public services and commercial services, are identified. The impact of algorithmic recommendations and profiling on the realization of the right to privacy and protection of personal data, the right to equality and non-discrimination, freedom of expression, as well as the human right to a fair procedure and an effective remedy is characterized. It is established that the opacity of the model, the lack of explainability and the complexity of tracing responsibility between the developer, provider and user create barriers to challenging decisions, and the scalability of algorithmic errors turns local failures into systemic consequences. It is proven that the

spread of generative tools increases the risks of information manipulation and image and voice forgery, which affects reputation, personal autonomy and trust in evidence in public communication. The need for a comprehensive regulatory response that combines risk-based regulation, transparency rules and human control requirements, as well as interaction with personal data protection regimes and the digital environment, is justified. It is proven that stabilization and protection are achieved only under the condition of organizational procedures that work at all stages, starting with data management and assessment of the impact on rights and freedoms, continuing with documentation requirements, notification of a person about the use of automated solutions, ensuring the possibility of explaining the result, and ending with auditing, incident monitoring, liability of providers and users, as well as accessible channels of complaints and redress.

Keywords: human rights, freedom paradigm, organizational and legal mechanism, artificial intelligence.

Постановка проблеми. Сучасні генеративні інструменти здатні швидко створювати переконливі підробки зображення та голосу, і на практиці це вже провокує нові форми втручання у приватне життя та зловживань без згоди людини, що фіксують і національні регулятори, і публічні попередження про ризики дипфейків у Європі. Одночасно формується багаторівнева нормативна відповідь, зокрема Регламент (Європейський Союз) 2024/1689 про правила для систем на базі штучного інтелекту, який набрав чинності 1 серпня 2024 року та закладає підхід, орієнтований на ризики, із заборонами окремих практик і посиленими вимогами до високоризикових застосувань. Паралельно Рада Європи відкрила для підписання Рамкову конвенцію про технології на базі штучного інтелекту, права людини, демократію та верховенство права, і це важливо, бо створює міжнародний орієнтир для узгоджених гарантій поза межами одного ринку, а Європейський Союз уже оформив рішення щодо підписання цього документа. Проте сам факт появи нових норм не усуває ключової організаційної проблеми, адже права людини порушуються не лише через відсутність правил, а й через слабке впровадження, дефіцит інституційної спроможності, нестачу незалежного нагляду, фрагментацію відповідальності між розробником, постачальником і користувачем системи, а також через складність доказування шкоди, коли рішення є результатом статистичного моделювання. Саме тому сучасний організаційний та правовий механізм стабілізації і захисту має бути не декларативним, а процедурним, він має поєднувати превентивні інструменти, такі як оцінювання впливу на права і свободи та керування ризиками, із вимогами прозорості, простежуваності та людського контролю, а також із дієвими каналами скарг і відшкодування, що узгоджується з позиціями Європейської ради із захисту даних щодо обробки персональних даних у контексті моделей на базі штучного інтелекту.

Аналіз останніх досліджень і публікацій. В науковій дискусії щодо прав і свобод людей в умовах масового впровадження технологій на базі штучного інтелекту домінує підхід, за якого технологічний прогрес розглядається як чинник одночасного підвищення ефективності управління та зростання правових ризиків, що потребують чітких організаційних і правових запобіжників. Наприклад, Ю.В. Камардіна, С.О. Поляруш-Сафроненко, Ю.В. Вишневська [1] у контексті сучасних викликів наголошують на необхідності переосмислення традиційних гарантій прав людини, оскільки алгоритмічні рішення впливають на реальну можливість реалізації приватності, рівності та доступу до правосуддя. А.Є. Шевченко, С.В. Кудін, О.І. Косілова [2] аналізують вплив технологій на базі штучного інтелекту на реалізацію прав і свобод людини і громадянина, акцентуючи на тому, що найбільші ризики виникають у сферах, де рішення ухвалюються швидко, масово і на основі великих даних, а людина стикається з труднощами отримання пояснень і оскарження. С. Кравчук [3] розвиває цю лінію аргументації через фокус на сталому втіленні технологій, доводячи, що без загальних рекомендацій і процедур керування ризиками технологічні інновації можуть поглиблювати нерівність, створювати нові форми дискримінації та підривати довіру до інституцій, які мають гарантувати права і свободи. Є.З. Остіян [4] аналізує взаємозв'язок технологій на базі штучного інтелекту та персональних даних, підкреслюючи, що захист приватності у цифровому середовищі вимагає не лише формальних правових норм, а й організаційних рішень щодо мінімізації даних, прозорості інформаційних процесів, обмеження доступу та належної безпеки. Ю.М. Жорнокуй [5] розглядає захист прав людини у ширшій рамці, де важливе місце посідають етичні стандарти, і показує, що етика у цьому контексті не замінює право, але підсилює його через вимоги до доброчесного проєктування, відповідального впровадження і контролю за наслідками використання технологій на базі штучного інтелекту. А. Штангрет, О. Силкін [8] аналізують безпекові аспекти управління персоналом у гіпердинамічному зовнішньому середовищі, що дозволяє пов'язати правову проблематику з реальними організаційними умовами, де людський фактор, інциденти, дефіцит компетенцій і тиск швидких змін можуть знижувати ефективність запобіжників.

Мета дослідження полягає у визначенні та теоретичному обгрунтуванні сучасного організаційного і правового механізму стабілізації та захисту прав і свобод людей в умовах масового впровадження технологій на базі штучного інтелекту. Об'єктом дослідження є суспільні відносини, що виникають у процесі розроблення, впровадження та використання технологій на базі штучного інтелекту і впливають на реалізацію та захист прав і свобод людей.

Виклад основного матеріалу. Масове впровадження технологій на базі штучного інтелекту змінює спосіб, у який суспільство організовує доступ до послуг, розподіляє ресурси та ухвалює рішення, і саме тому права і свободи

людей переходять із суто декларативної площини у площину повсякденних практик, де ризики виникають не епізодично, а системно. Коли рішення про кредит, працевлаштування, страхування, медичний маршрут, доступ до освіти, соціальної допомоги або модерацію контенту ухвалюються з опорою на автоматизовані моделі та профілювання, зростає небезпека помилок, непрозорості та нерівності, оскільки один і той самий дефект даних або логіки може відтворюватися у великих масштабах. Додатково посилюється дисбаланс між людиною і організацією, адже технології на базі штучного інтелекту здатні збирати, поєднувати і аналізувати персональні дані у темпі, який людина не може контролювати індивідуально, тому правова гарантія приватності, автономії та людської гідності потребує не лише заборон, а й організаційних запобіжників, які працюють до настання шкоди (табл.1).

Таблиця 1.

Ключові ризики для прав і свобод людей та інструменти стабілізації і захисту в умовах масового впровадження технологій на базі штучного інтелекту

Загрози для прав і свобод людей	Організаційно-правові інструменти стабілізації та захисту
Порушення приватності та неконтрольована обробка персональних даних, коли дані збираються ширше, ніж потрібно для мети, поєднуються з різних джерел і використовуються для профілювання без зрозумілої для людини логіки	Впровадження політик мінімізації даних, обмеження доступів і чіткої мети обробки, оцінювання впливу на права і свободи до запуску, ведення реєстрів обробки і наборів даних, регулярні внутрішні перевірки відповідності, процедури реагування на інциденти, повідомлення про порушення, а також зрозумілі повідомлення для людей про те, які дані використано і для чого
Дискримінація та нерівність, коли модель відтворює історичні упередження, використовує непрямі ознаки, що корелюють із чутливими характеристиками, і призводить до різної якості рішень для різних груп	Вимоги до якості даних і представництва груп, тестування на упередженість до впровадження і після змін у моделі, заборона використання неприйнятних критеріїв, формалізація відповідальності власника процесу, незалежний аудит і протоколи виправлення, а також обов'язок фіксувати причини відхилень і робити коригувальні дії, якщо виявлено системну нерівність
Порушення права на справедливу процедуру та ефективний засіб правового захисту, коли людина не розуміє, чому отримала відмову, хто ухвалив рішення і як його оскаржити, а організація не може пояснити логіку через складність моделі	Процедури пояснення результату у зрозумілій формі, визначення відповідальної посадової особи за автоматизовані рішення, правила людського перегляду у значущих ситуаціях, стандарти документування моделей і змін, канали подання скарг і строки розгляду, фіксація підстав рішення і доказів, а також механізми відшкодування шкоди та відновлення порушених прав

Джерело: сформовано авторами

Ключові загрози для прав і свобод проявляються у кількох взаємопов'язаних блоках, які підсилюють один одного. Відтак, це приватність і захист персональних даних, оскільки моделі можуть навчатися на великих масивах інформації з різним походженням, а також можуть відтворювати фрагменти даних, що ускладнює виконання принципів законності, мінімізації та прозорості обробки, і саме тому органи з захисту даних у Європейському Союзі окремо роз'яснюють, за яких умов моделі можуть вважатися анонімними, як обґрунтовувати законний інтерес і які наслідки має незаконна обробка на етапі розробки для подальшого використання моделі. Так, це рівність і недискримінація, адже автоматизовані рішення можуть закріплювати історичні упередження, непомітно вводити непрямі критерії, що корелюють із вразливими ознаками, і створювати різну якість послуг для різних груп. Також, це право на справедливу процедуру і ефективний засіб правового захисту, оскільки людині часто складно зрозуміти, чому система на базі штучного інтелекту видала саме такий результат, хто відповідальний за помилку і як отримати пояснення та виправлення. Так, це свобода вираження поглядів та інформаційна безпека, бо генеративні технології здатні масштабувати маніпуляції, створювати правдоподібні підробки зображення та голосу, прискорювати поширення дезінформації і підривати довіру до доказів, а у відповідь держави починають запроваджувати вимоги маркування контенту, створеного або зміненого за допомогою технологій на базі штучного інтелекту, з істотними санкціями за порушення (табл.2).

Таблиця 2

Життєвий цикл систем на базі штучного інтелекту та контрольні точки захисту прав і свобод людей

Етап життєвого циклу	Типові дії організації
Проєктування і постановка мети	Визначення задачі, вибір сфери застосування, опис того, на кого впливатиме рішення, визначення ролей розробника, постачальника і користувача, попередня оцінка ризиків для приватності, рівності та доступу до оскарження
Розроблення, навчання і тестування	Підбір і очищення даних, налаштування моделі, тестування точності та стійкості, перевірка на упередженість, оцінювання кібербезпеки, підготовка інструкцій для користувачів і персоналу, планування моніторингу після запуску
Впровадження і використання у процесах	Інтеграція в робочі системи, налаштування доступів, визначення сценаріїв, де рішення має підтверджувати людина, запуск комунікацій для користувачів, створення каналів звернень і процедур розгляду скарг

Джерело: сформовано авторами

Сучасна відповідь у Європейському Союзі та ширшому європейському правовому просторі вибудовується як поєднання правил, інституцій і процедур, які мають стабілізувати розвиток і водночас запобігати системній шкоді. Центральним елементом стала рамка Регламенту Європейського Союзу 2024/1689 про правила для систем на базі штучного інтелекту, яка запроваджує ризик-орієнтовану логіку, де частина практик забороняється, а для високо-ризикових застосувань встановлюються жорсткі вимоги щодо якості даних, технічної документації, людського контролю, простежуваності, кібербезпеки та нагляду після виведення на ринок, при цьому сам регламент уже має поетапне застосування, зокрема заборонені практики і вимоги грамотності у сфері технологій на базі штучного інтелекту почали застосовуватися з 2 лютого 2025 року, правила управління і зобов'язання для моделей загального призначення почали застосовуватися з 2 серпня 2025 року, а повна застосовність передбачена з 2 серпня 2026 року з довшими перехідними строками для частини регульованих продуктів. Паралельно діють і взаємодіють інші режими, передусім Загальний регламент про захист даних Європейського Союзу, а також правила цифрового середовища, які стосуються прозорості платформ і відповідальності за контент, що є важливим для протидії маніпуляціям і підробкам. Додатковий рівень задає Рамкова конвенція Ради Європи про технології на базі штучного інтелекту, права людини, демократію та верховенство права, яка відкрита для підписання 5 вересня 2024 року як міжнародний юридично зобов'язальний інструмент, і Європейський Союз ухвалив рішення щодо підписання цієї конвенції від імені Європейського Союзу. Водночас дискусії про спрощення регулювання і можливі відтермінування окремих вимог показують, що механізм захисту залежить не лише від текстів норм, а й від політичної волі, інституційної спроможності та балансу між конкурентоспроможністю і фундаментальними гарантіями (рис.1).

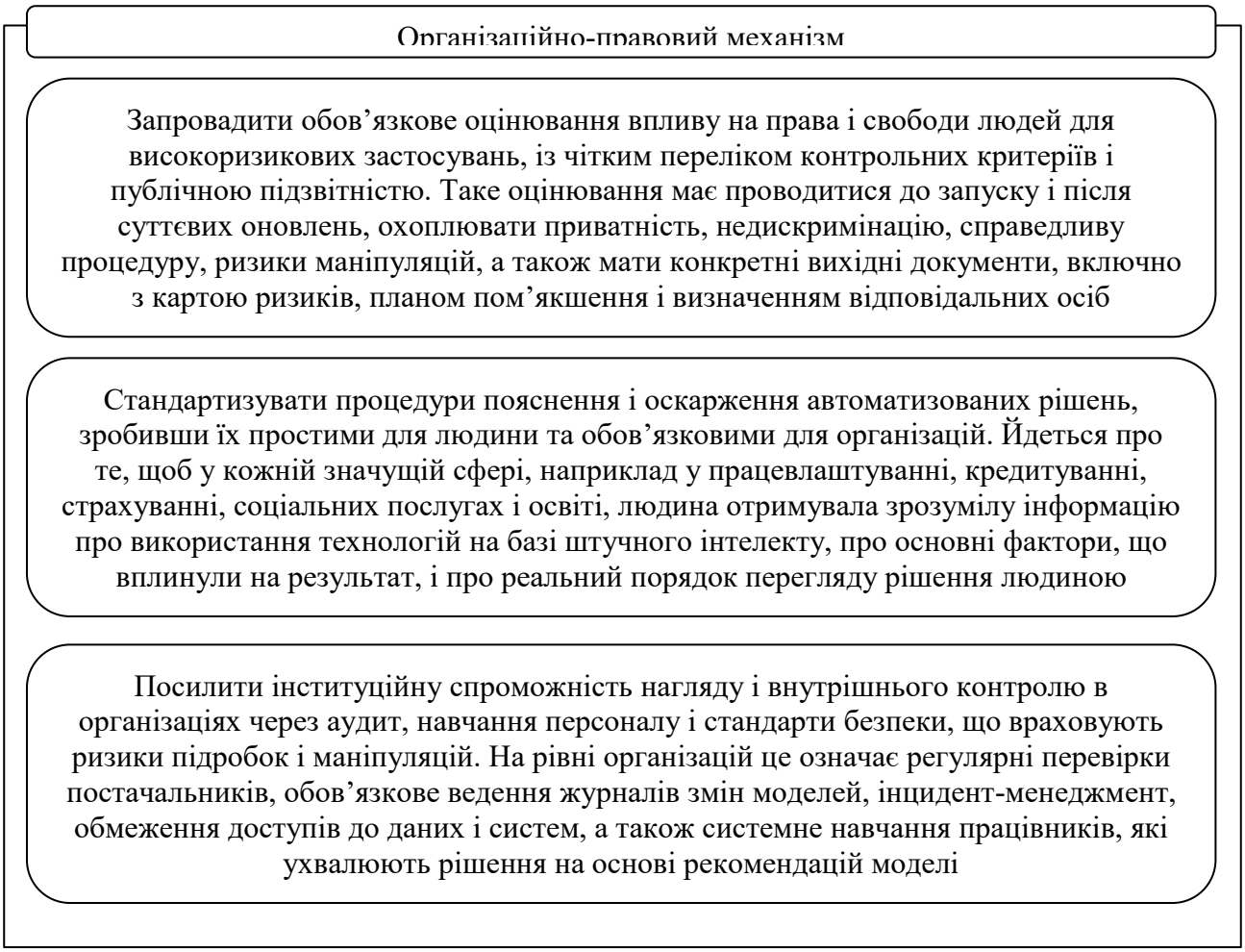

Рис.1. Організаційно-правовий механізм стабілізації та захисту права і свободи людей в епоху масового впровадження технологій на базі штучного інтелекту

Джерело: сформовано авторами

Якщо розкривати сучасний організаційно-правовий механізм стабілізації та захисту по суті, то він має працювати як ланцюг взаємопов'язаних запобіжників на всьому життєвому циклі систем на базі штучного інтелекту, від задуму і підбору даних до експлуатації та виведення з використання. На етапі розробки ключовими стають політики якості даних і недискримінації, оцінка впливу на права і свободи, обґрунтування правових підстав для використання персональних даних, а також тестування на безпечність і стійкість до зловживань, що прямо пов'язано з підходами, які окреслює Європейська рада із захисту даних у своїх роз'ясненнях щодо моделей і персональних даних. На етапі впровадження потрібні зрозумілі для людини повідомлення про використання технологій на базі штучного інтелекту, процедури пояснення результату, можливість зверну-

тися до відповідальної особи, а також реальний людський контроль там, де ціна помилки висока, наприклад у працевлаштуванні, кредитуванні, освіті, охороні здоров'я і публічних послугах. На етапі експлуатації важливими стають аудит, моніторинг інцидентів, обов'язок повідомляти про серйозні порушення, контроль постачальників і підрядників, а також правила закупівель у державному секторі, які мають унеможливлювати придбання непрозорих рішень без доказів відповідності.

Висновки. Підсумовуючи, зазначимо, що саме права і свободи людей у період масового впровадження технологій на базі штучного інтелекту потребують не лише загальних декларацій, а дієвого організаційно-правового механізму, який одночасно запобігає системній шкоді та забезпечує реальний захист у конкретних ситуаціях, оскільки саме масштабованість алгоритмічних рішень робить помилки, упередження, непрозорість і маніпуляції ризиками суспільного рівня. Ефективна стабілізація досягається тоді, коли правила ризик-орієнтованого регулювання поєднані з якістю даних, прозорістю, простежуваністю, людським контролем, незалежним наглядом і доступними процедурами оскарження та відшкодування, а також із підвищенням грамотності у сфері технологій на базі штучного інтелекту, що зменшує асиметрію між організаціями і громадянами. У такій конструкції технологічний прогрес зберігає суспільну користь, але не підміняє верховенство права, і гарантії приватності, рівності, справедливої процедури та свободи вираження поглядів стають практично здійсненними, а не суто формальними.

Література:

1. Камардіна Ю.В., Поляруш-Сафроненко С.О., Вишневська Ю.В. Права людини в епоху розвитку штучного інтелекту. Вип. 27, 2024. Вісник Маріупольського державного університету. Серія «Право». С. 71–78.

2. Шевченко А.Є., Кудін С.В., Косілова О.І. Вплив штучного інтелекту на реалізацію прав і свобод людини і громадянина в Україні. № 2(8), 2023. Legal Bulletin. С. 65–74.

3. Кравчук С. Вплив штучного інтелекту на права людини та загальні рекомендації для сталого втілення. № 3(43), 2024. Вісник Національного університету «Львівська політехніка». Серія «Юридичні науки». С. 101–109.

4. Остіян Є.З. Штучний інтелект та персональні дані: захист приватності в цифровому середовищі. Випуск 85, частина 3, 2024. Науковий вісник Ужгородського Національного Університету. Серія «Право». С. 47–53.

5. Жорнокуй Ю.М. Штучний інтелект: охорона та захист прав людини та етичні стандарти. № 1(108), 2025, ч. 1. Вісник Харківського національного університету внутрішніх справ. С. 71–83.

6. Берназюк І.М. Штучний інтелект і права людини: виклики для Європейської конвенції з прав людини. Випуск № 03, 2025, частина 1. Аналітично-порівняльне правознавство. С. 89–99.

7. Зибарева О.В., Гольцова І.Л. Ключові аспекти та сучасні тренди розвитку цифрових технологій в діяльності підприємств України. Ефективна економіка. 2020. №12. URL: http://www.economy.nayka.com.ua/?op=1&z=8444

8. Штангрет А., Силкін О. Безпекові аспекти управління персоналом в умовах гіпердинамічного зовнішнього середовища. № 9(37), 2024. Наукові інновації та передові технології. С. 227-237. https://doi.org/10.52058/2786-5274-2024-9(37)-227-237

9. Криштанович, М., & Силкін, О. Оцінювання стратегічних напрямів реалізації державно-приватного партнерства в царині безпекового розвитку агропромислового сектора. Socio-Economic Relations in the Digital Society, 1(55), 2025, 44-55. https://doi.org/10.55643/ser.5.55.2025.587

10. Штангрет А., Силкін О., Шляхетко В. Трудова міграція як зовнішня загроза для кадрової безпеки підприємства. № 10(38), 2024. Наукові інновації та передові технології. С. 190-201. https://doi.org/10.52058/2786-5274-2024-10(38)-190-201

11. Криштанович, М., Богоніс А. Інформаційне забезпечення роботи системи публічного управління. Актуальні питання у сучасній науці, 4(22), 2024, 359-368.

References:

1. Kamardina, Yu. V., Poliarush-Safronenko, S. O., & Vyshnevska, Yu. V. (2024). Prava liudyny v epokhu rozvytku shtuchnoho intelektu [Human rights in the era of artificial intelligence development]. Visnyk Mariupolskoho derzhavnoho universytetu. Seriia “Pravo” – Bulletin of Mariupol State University. Law Series, 27, 71–78. [in Ukrainian].

2. Shevchenko, A. Ye., Kudin, S. V., & Kosilova, O. I. (2023). Vplyv shtuchnoho intelektu na realizatsiiu prav i svobod liudyny i hromadianyna v Ukraini [Impact of artificial intelligence on the implementation of human and citizen rights and freedoms in Ukraine]. Legal Bulletin, 2(8), 65–74. [in Ukrainian].

3. Kravchuk, S. (2024). Vplyv shtuchnoho intelektu na prava liudyny ta zahalni rekomendatsii dlia staloho vtilennia [Impact of artificial intelligence on human rights and general recommendations for sustainable implementation]. Visnyk Natsionalnoho universytetu “Lvivska politekhnika”. Seriia “Iurydychni nauky” – Bulletin of Lviv Polytechnic National University. Legal Sciences Series, 3(43), 101–109. [in Ukrainian].

4. Ostiian, Ye. Z. (2024). Shtuchnyi intelekt ta personalni dani: zakhyst pryvatnosti v tsyfrovomu seredovyshchi [Artificial intelligence and personal data: privacy protection in the digital environment]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia “Pravo” – Scientific Bulletin of Uzhhorod National University. Law Series, 85(3), 47–53. [in Ukrainian].

5. Zhornokui, Yu. M. (2025). Shtuchnyi intelekt: okhorona ta zakhyst prav liudyny ta etychni standarty [Artificial intelligence: safeguarding and protection of human rights and ethical standards]. Visnyk Kharkivskoho natsionalnoho universytetu vnutrishnikh sprav – Bulletin of Kharkiv National University of Internal Affairs, 1(108), part 1, 71–83. [in Ukrainian].

6. Bernaziuk, I. M. (2025). Shtuchnyi intelekt i prava liudyny: vyklyky dlia Yevropeiskoi konventsii z prav liudyny [Artificial intelligence and human rights: challenges for the European Convention on Human Rights]. Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence, 3, part 1, 89–99. [in Ukrainian].

7. Zybareva, O. V., & Holtsova, I. L. (2020). Kliuchovi aspekty ta suchasni trendy rozvytku tsyfrovykh tekhnolohii v diialnosti pidpryiemstv Ukrainy [Key aspects and current trends in the development of digital technologies in the activities of Ukrainian enterprises]. Efektyvna ekonomika – Efficient Economy, 12. http://www.economy.nayka.com.ua/?op=1&z=8444[in Ukrainian].

8. Shtangret, A., & Sylkin, O. (2024). Bezpekovi aspekty upravlinnia personalom v umovakh hiperdynamichnoho zovnishnoho seredovyshcha [Security aspects of personnel management under hyperdynamic external environment]. Naukovi innovatsii ta peredovi tekhnolohii – Scientific Innovations and Advanced Technologies, 9(37), 227–237. https://doi.org/10.52058/2786-5274-2024-9(37)-227-237 [in Ukrainian].

9. Kryshtanovych, M., & Sylkin, O. (2025). Otsiniuvannia stratehichnykh napriamiv realizatsii derzhavno-pryvatnoho partnerstva v tsaruni bezpekovoho rozvytku ahropromyslovoho sektora [Assessment of strategic directions for implementing public-private partnership in the field of security development of the agro-industrial sector]. Socio-Economic Relations in the Digital Society, 1(55), 44–55. https://doi.org/10.55643/ser.5.55.2025.587 [in Ukrainian].

10. Shtangret, A., Sylkin, O., & Shliakhetko, V. (2024). Trudova mihratsiia yak zovnishnia zahroza dlia kadrovoi bezpeky pidpryiemstva [Labor migration as an external threat to enterprise's personnel security]. Naukovi innovatsii ta peredovi tekhnolohii – Scientific Innovations and Advanced Technologies, 10(38), 190–201. https://doi.org/10.52058/2786-5274-2024-10(38)-190-201 [in Ukrainian].

11. Kryshtanovych, M., & Bohonis, A. (2024). Informatsiine zabezpechennia roboty systemy publichnoho upravlinnia [Information support for the functioning of the public administration system]. Aktualni pytannia u suchasnii nautsi – Current Issues in Modern Science, 4(22), 359–368. [in Ukrainian].