DOI: https://doi.org/10.37634/efp.2025.2.24
УДК 342.2.1

Андрій Павлович ***КОЛЕСНІКОВ***
к.е.н., доцент, Західноукраїнський національний університет
ORCID: https://orcid.org/0000-0003-3064-4133
e-mail: kole.ua@gmail.com

Ярослав Русланович ***ЧАПЕЛЬСЬКИЙ***
аспірант, Західноукраїнський національний університет
ORCID: https://orcid.org/0000-0002-3057-8861
e-mail: chapelskyi.slavik@gmail.com

Володимир Ігорович ***БУДНИК***
аспірант, Західноукраїнський національний університет
ORCID: https://orcid.org/0009-0004-7762-5882
e-mail: v.budnyk@wunu.edu.ua

Юрій Володимирович ***КОЖЕНЬОВСЬКИЙ***
аспірант, Західноукраїнський національний університет
ORCID: https://orcid.org/0009-0007-6929-1116
e-mail: Trust7857@gmail.com

ТРАНСФОРМАЦІЯ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ВПЛИВОМ РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

У статті досліджено актуальні проблеми та виклики у сфері захисту персональних даних, що виникають у зв'язку з розвитком технологій штучного інтелекту (ШІ). Проаналізовано ключові аспекти трансформації системи захисту персональних даних, зокрема проблему «чорної скриньки» та етичні аспекти використання великих даних. Розглянуто сучасний стан правового регулювання та технічні засоби захисту персональних даних під час застосування систем ШІ. Запропоновано шляхи вдосконалення механізмів захисту персональних даних завдяки впровадженню комплексного підходу, що включає правові, технічні та організаційні заходи, а також розвиток міжнародного співробітництва у цій сфері.

Ключові слова: *захист персональних даних, штучний інтелект, правове регулювання, безпека даних, «чорна скринька», приватність, обробка даних, GDPR*

ВСТУП

Стрімкий розвиток технологій штучного інтелекту (ШІ) створює принципово нові виклики у сфері захисту персональних даних. Масштабне його застосування в різних сферах суспільного життя призводить до безпрецедентного збільшення обсягів збору та оброблення персональних даних, що суттєво підвищує ризики порушення приватності особи. За даними дослідження компанії IBM «Cost of a Data Breach Report 2023» середня вартість витоку даних у 2023 році досягла 4,45 млн дол. США, причому інциденти, пов'язані із застосуванням ШІ, призводять до збільшення цієї суми в середньому на 37% [1].

Особливістю сучасного етапу розвитку технологій є те, що алгоритми машинного навчання здатні виявляти приховані взаємозв'язки між даними та створювати детальні профілі особистості навіть з обмеженого набору інформації. Традиційні механізми захисту персональних даних, розроблені для роботи з конвенційними інформаційними системами, виявляються недостатньо ефективними в умовах використання технологій ШІ через технічні особливості їх функціонування та складність забезпечення прозорості оброблення даних.

Проблема захисту персональних даних особливо загострюється в період значного зростання кількості кіберзагроз з боку росії. За даними Всесвітнього економічного форуму, у 2023 р. кібератаки із застосуванням технологій ШІ увійшли до топ-5 глобальних ризиків [2]. Подвійна природа технологій ШІ, які може бути застосовано як для захисту персональних даних, так і для здійснення атак на системи захисту, створює необхідність трансформації наявних підходів до забезпечення інформаційної безпеки та приватності.

Дослідження питань захисту персональних даних в умовах розвитку ШІ набуває все більшої актуальності серед науковців. Зокрема, фундаментальні аспекти регулювання оброблення персональних даних системами ШІ розглядали О. Пунда та Д. Арзянцева [3]. Проблематику захисту приватності у застосуванні технологій ШІ досліджували К. Резворович, М. Береда [4] та В. Базалицький [5]. Питанням викликів та загроз захисту персональних даних у роботі із ШІ присвячено працю М. Бєлової та Д. Бєлова [6].

В контексті міжнародно-правового регулювання захисту персональних даних у застосуванні ШІ важливими є дослідження M. Veale та F. Zuiderveen Borgesius [7], які проаналізували положення GDPR стосовно автоматизованого прийняття рішень. Питання демістифікації «чорної скриньки» ШІ та забезпечення прозорості обробки персональних даних розглядали R. Guidotti та його колеги [8]. Значний внесок у розуміння викликів приватності в епоху ШІ зробили B. Mittelstadt та L. Floridi [9], які дослідили етичні аспекти алгоритмічного оброблення даних.

Окремі аспекти захисту персональних даних в умовах розвитку ШІ розглянуто раніше [10]. Це дослідження є продовженням наших наукових розвідок.

МАТЕРІАЛИ ТА МЕТОДИ

Методологічну основу дослідження складає комплекс загальнонаукових та спеціальних методів наукового пізнання. Для дослідження теоретичних положень

із захисту персональних даних в умовах розвитку ШІ застосовано діалектичний метод, що дав змогу розглянути досліджувані явища в їх розвитку та взаємозв'язку.

Формально-юридичний метод застосовано в аналізі нормативно-правових актів, що регулюють питання захисту персональних даних та використання технологій ШІ.

Системно-структурний метод дав змогу визначити місце захисту персональних даних в загальній системі правового регулювання застосування ШІ. Методи аналізу та синтезу застосовано для виявлення основних викликів та загроз у сфері захисту персональних даних, пов'язаних із впровадженням технологій ШІ.

ПОСТАНОВКА ЗАВДАННЯ: дослідження актуальних проблем та викликів у сфері захисту персональних даних, що виникають у зв'язку з розвитком та впровадженням технологій ШІ.

РЕЗУЛЬТАТИ

Інтенсивне впровадження технологій ШІ створює нові виклики у сфері захисту персональних даних. Однією з ключових проблем є т.зв. ефект «чорної скриньки», зміст якої полягає у непрозорості і складності для розуміння алгоритмів прийняття рішень системами ШІ. Як зазначають R. Guidotti та його колеги, це створює серйозні виклики для забезпечення підзвітності та контролю за обробкою персональних даних [8].

Особливу увагу привертають етичні аспекти застосування великих даних системами ШІ. B. Mittelstadt та L. Floridi підкреслюють, що оброблення персональних даних у великих масштабах може призводити до порушення приватності та дискримінації [9]. Ця проблема стає особливо гострою в контексті можливого автоматизованого прийняття рішень, що потенційно буде впливати на права та інтереси суб'єктів персональних даних.

М. Бєлова та Д. Бєлов акцентують на тому, що подвійна природа технологій ШІ, що може бути застосовано як для захисту персональних даних, так і для здійснення атак на їх системи, визначає необхідність трансформації наявних підходів до забезпечення інформаційної безпеки [6].

Ще однією обставиною, яку варто враховувати є необхідність забезпечення балансу між інноваційним розвитком технологій ШІ та захистом фундаментальних прав людини. О. Пунда та Д. Арзянцева наголошують на необхідності формування механізмів захисту персональних даних, які б враховували як потреби розвитку технологій, так і вимоги до забезпечення приватності [3].

Європейські інструменти правового застосування ШІ в роботі з персональними даними відображено в положенні GDPR та Акті ЄС про ШІ (EU AI Act), який встановлює чіткі вимоги до прозорості та підзвітності систем ШІ, особливо у разі, коли їх застосовую для оброблення персональних даних.

В. Базалицький, аналізуючи положення GDPR, підкреслює, що цей документ встановлює важливі принципи оброблення персональних даних, такі як законність, справедливість, прозорість, цільове обмеження, мінімізація даних та забезпечення їх безпеки. Водночас особливу увагу приділено правам суб'єктів даних, включаючи право на доступ до інформації про алгоритми оброблення та право не підлягати повністю автоматизованому прийняттю рішень [5].

К. Резворович та М. Береда звертають увагу на необхідність адаптації національного законодавства до нових викликів цифрової епохи. Вони наголошують на важливості розроблення спеціальних правових механізмів, які б враховували особливості застосування ШІ в обробленні персональних даних [4].

Важливим аспектом правового регулювання є встановлення відповідальності за порушення вимог захисту персональних даних. Згідно з даними Global Cybersecurity Outlook 2023, посилення правової відповідальності за порушення у сфері захисту даних є одним з ключових трендів розвитку законодавства [2]. Водночас особливу увагу приділено встановленню відповідальності не лише за сам факт витоку даних, але й за недотримання вимог до забезпечення їх належного захисту.

Слід зазначити, що ефективне правове регулювання вимагає балансу між забезпеченням інновацій та захистом прав суб'єктів персональних даних. Це передбачає розроблення гнучких правових механізмів, які б давали змогу адаптуватися до швидкого розвитку технологій, зберігаючи водночас високий рівень захисту персональних даних.

У контексті застосування систем ШІ технічні та організаційні заходи захисту персональних даних абувають особливого значення. До ключових технічних заходів належать:

– шифрування даних під час їхнього зберігання та передачі;

– застосування методів анонімізації та псевдонімізації;

– впровадження систем контролю доступу та антентифікації;

– застосування технологій виявлення та запобігання витокам даних.

Організаційні заходи включають:

– розроблення політик та процедур захисту персональних даних;

– проведення регулярних аудитів безпеки;

– навчання персоналу безпечному обробленню персональних даних;

– впровадження процедур реагування на інциденти безпеки.

Особливу увагу слід приділити процесу оцінювання впливу на захист персональних даних (DPIA) у впровадженні систем ШІ. Цей процес дає змогу виявити потенційні ризики та розробити відповідні заходи їх мінімізації ще на етапі проєктування системи.

Важливим елементом є також забезпечення прозорості оброблення даних, що передбачає документування всіх процесів оброблення та надання суб'єктам даних інформації про те, як їхні дані обробляються системами ШІ.

Подальший розвиток системи захисту персональних даних в умовах застосування ШІ потребує комплексного підходу, що включає правові та технологічні аспекти. Ключовим напрямом вдосконалення є розроблення адаптивних механізмів регулювання, які зможуть оперативно реагувати на появу нових технологічних рішень та пов'язаних з ними ризиків.

Важливим аспектом є розвиток культури захисту персональних даних серед розробників систем ШІ. Це передбачає впровадження принципу «приватність за дизайном», коли захист персональних даних враховується вже на етапі проєктування системи. Такий підхід дає змогу забезпечити більш ефективний захист прав

суб'єктів персональних даних.

Особливу увагу слід приділити розвитку механізмів міжнародного співробітництва у сфері захисту персональних даних. Глобальний характер технологій ШІ вимагає узгоджених підходів до регулювання та спільних стандартів захисту даних. Це особливо важливо в контексті транскордонної передачі даних в умовах розвитку ШІ.

Перспективним напрямом є також розвиток спеціалізованих інститутів та механізмів контролю за дотриманням вимог до захисту персональних даних, які можуть включати створення спеціалізованих наглядових органів, розвиток систем сертифікації та аудиту, а також впровадження механізмів громадського контролю.

В майбутньому важливо забезпечити баланс між інноваційним розвитком технологій ШІ та захистом фундаментальних прав людини. Це вимагає постійного діалогу між розробниками технологій, регуляторами та громадянським суспільством для вироблення оптимальних рішень щодо захисту персональних даних.

ВИСНОВКИ

Проведене дослідження демонструє, що розвиток технологій штучного інтелекту створює нові виклики у сфері захисту персональних даних, зокрема проблему «чорної скриньки» та етичні аспекти застосування великих даних. Вирішення цих проблем вимагає комплексного підходу, що включає вдосконалення правового регулювання, впровадження технічних та організаційних заходів захисту, а також розвиток міжнародного співробітництва. Особливу увагу слід приділити забезпеченню балансу між інноваційним розвитком технологій та захистом фундаментальних прав людини. Це передбачає впровадження принципу «приватність за дизайном» та розвиток механізмів контролю за дотриманням вимог до захисту персональних даних.

Список використаних джерел

1. IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. URL: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

2. Global Cybersecurity Outlook 2023. URL: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

3. Пунда О.О., Арзянцева Д.А. Забезпечення захисту персональних даних фізичних осіб в умовах розвитку штучного інтелекту. *Наука і техніка сьогодні*. 2024. №2 (30). С. 132-141.

4. Резворович К.Р., Береда М.В. Вплив штучного інтелекту на правову систему та захист персональних даних у цифрову епоху. *Успіхи і досягнення у науці*. 2024. №4 (4). С. 241-248.

5. Базалицький В.І. Врегулювання питання обробки персональних даних штучним інтелектом у загальному регламенті із захисту персональних даних (GDPR). *Актуальні питання у сучасній науці. Серія Право*. 2024. № 6(24). С. 406-419.

6. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 79(2). С. 17-22.

7. Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*. 2021. Vol. 22(4). pp. 97-112.

8. Guidotti R., Monreale A., Ruggieri S., Turini F., Giannotti F., Pedreschi D. A Survey of Methods for Explaining Black Box Models. *ACM Computing Surveys*. 2019. Vol. 51(5).

9. Mittelstadt B.D., Floridi L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics*. 2016. Vol. 22. pp. 303-341.

10. Колесніков А.П., Карапетян О.М. Штучний інтелект: переваги та загрози використання. *Ефективна економіка*. 2023. № 8. URL: https://doi.org/10.32702/2307-2105.2023.8.9

References

1. IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs. URL: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

2. Global Cybersecurity Outlook 2023. URL: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

3. Punda O.O., Arziantseva D.A. Ensuring Protection of Personal Data of Individuals in the Context of Artificial Intelligence Development. *Science and Technology Today*. 2024. No. 2(30). pp. 132-141. (in Ukrainian).

4. Rezvorovych K.R., Bereda M.V. The Impact of Artificial Intelligence on the Legal System and Personal Data Protection in the Digital Age. *Successes and Achievements in Science*. 2024. No. 4(4). pp. 241-248. (in Ukrainian).

5. Bazalytskyi V.I. Regulation of Personal Data Processing by Artificial Intelligence in the General Data Protection Regulation (GDPR). *Current Issues in Modern Science. Law Series*. 2024. No. 6(24). pp. 406-419. (in Ukrainian).

6. Bielova M.V., Bielov D.M. Challenges and Threats to Personal Data Protection in Working with Artificial Intelligence. *Scientific Bulletin of Uzhhorod National University. Series: Law*. 2023. Issue 79(2). pp. 17-22. (in Ukrainian)

7. Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*. 2021. Vol. 22(4). pp. 97-112.

8. Guidotti R., Monreale A., Ruggieri S., Turini F., Giannotti F., Pedreschi D. A Survey of Methods for Explaining Black Box Models. *ACM Computing Surveys*. 2019. Vol. 51(5).

9. Mittelstadt B.D., Floridi L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics*. 2016. Vol. 22. pp. 303-341.

10. Kolesnikov A.P., Karapetian O.M. Artificial Intelligence: Benefits and Threats of Use. *Efficient Economy*. 2023. No. 8. URL: https://doi.org/10.32702/2307-2105.2023.8.9 (in Ukrainian).

Andrii KOLESNIKOV
PhD in Economics, Associate Professor, West Ukrainian National University
ORCID: https://orcid.org/0000-0003-3064-4133
e-mail: kole.ua@gmail.com

Yaroslav CHAPELSKYI
postgraduate student, West Ukrainian National University
ORCID: https://orcid.org/0000-0002-3057-8861
e-mail: chapelskyi.slavik@gmail.com

Volodymyr BUDNYK
postgraduate student, West Ukrainian National University
ORCID: https://orcid.org/0009-0004-7762-5882
e-mail: v.budnyk@wunu.edu.ua

Yurii KOZHENOVSKYI
postgraduate student, West Ukrainian National University
ORCID: https://orcid.org/0009-0007-6929-1116
e-mail: Trust7857@gmail.com

TRANSFORMATION OF THE PERSONAL DATA PROTECTION SYSTEM UNDER THE INFLUENCE OF ARTIFICIAL INTELLIGENCE TECHNOLOGY DEVELOPMENT

Introduction. *The rapid development of artificial intelligence technologies creates new challenges in personal data protection. With the widespread implementation of AI systems across various sectors of society, there is an unprecedented increase in the collection and processing of personal data, significantly elevating privacy risks. According to IBM's Cost of a Data Breach Report 2023, AI-related incidents lead to a 37% increase in average breach costs, highlighting the growing significance of this issue.*

The purpose of the paper *is to investigate current challenges and issues in personal data protection arising from the development and implementation of artificial intelligence technologies, with particular focus on the transformation of existing protection mechanisms and regulatory frameworks.*

Results. *The research identifies several key challenges in personal data protection related to AI systems, particularly the "black box" problem where AI decision-making processes become opaque and difficult to understand. The study highlights ethical concerns regarding large-scale data processing by AI systems, which can lead to privacy violations and discrimination. Analysis of current legal frameworks, including GDPR and the EU AI Act, reveals the importance of comprehensive regulation at both international and national levels. The research emphasizes the need for technical and organizational measures, including data encryption, anonymization techniques, and access control systems. The study also identifies the crucial role of international cooperation in developing unified standards for personal data protection in AI systems.*

Conclusion. *The effective protection of personal data in the age of artificial intelligence requires a comprehensive approach combining legal regulation, technical measures, and international cooperation. The implementation of the «privacy by design» principle and the development of control mechanisms for compliance with data protection requirements are essential. The study emphasizes the importance of maintaining a balance between innovative technological development and the protection of fundamental human rights in data privacy.*

Keywords: *personal data protection, artificial intelligence, legal regulation, data security, black box, privacy, data processing, GDPR*