МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНИХ КОНФЕРЕНЦІЙ ЧОРНОМОРСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ПЕТРА МОГИЛИ
MATERIALS OF THE SCIENTIFIC AND PRACTICAL CONFERENCE OF PETRO MOGYLA BLACK
Серія «Публічне управління та адміністрування»

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 2(1) 2025
Series «Public management and administration»

DOI 10.34132/mspc2025.02.13.35

Оксана Малікіна
Тетяна Медведенко

РИЗИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ УПРАВЛІННІ

Матеріали представляють аналіз ризиків, що виникають у процесі впровадження та використання технологій штучного інтелекту (ШІ) у системі публічного управління. З'ясовано, що ШІ як комплекс інформаційних технологій генерує соціально-економічні, технологічні та інституційні ризики, які впливають на ефективність функціонування державних інститутів та дотримання прав громадян. Окреслено основні загрози, зокрема упередженість алгоритмів, непрозорість процесів прийняття рішень, порушення конфіденційності персональних даних, мілітаризацію ШІ, ризики втрати контролю над алгоритмами та соціально-економічні наслідки автоматизації. Визначено, що динамічність цих ризиків потребує системного підходу до їх моніторингу, удосконалення нормативно-правового регулювання та підвищення рівня відповідальності органів публічної влади у сфері застосування ШІ.

Ключові слова: *штучний інтелект, публічне управління, ризики, прозорість, упередженість алгоритмів, захист персональних даних, кібербезпека, соціально-економічні наслідки.*

Враховуючи, що штучний інтелект (ШІ) є комплексом інформаційних технологій, ризики його застосування можна умовно поділити на соціально-економічні - пов'язані з впливом на суспільство, людські колективи та добробут населення, і технологічні - зумовлені використанням інформаційно-комп'ютерних систем, алгоритмів і програмного забезпечення.

Для сфери публічного управління особливого значення набувають інституційні ризики, під якими розуміють імовірність зниження результативності, ефективності, узгодженості та збалансованості функціонування управлінських інститутів. Такі ризики безпосередньо впливають на стабільність соціально-економічного розвитку держави, галузі управління чи територіальної громади. Їхнє виникнення значною мірою зумовлене неефективністю чинної системи публічного адміністрування, суперечливістю управлінських процесів, а також незавершеністю реформ у цій сфері.

Технологічні ризики, що можуть виникнути внаслідок застосування штучного інтелекту (ШІ) і здатні підірвати засади діяльності публічного сектору та права громадян, не можна ігнорувати. У цьому контексті головною загрозою є потенційні помилки або збої, пов'язані з проблемами у проєктуванні алгоритмів чи у використаних даних, що можуть призвести до хибних управлінських рішень або дій, упереджених чи дискримінаційних за своєю суттю.

Важливим ризиком є саме ці упередження та дискримінації, що виникають, коли результати, отримані за допомогою алгоритмів, не відображають реальну різноманітність людей чи об'єктів, які підлягають аналізу. Як застерігає Кеті О'Ніл, алгоритми можуть посилювати нерівність і становити загрозу для демократії. Упередження можуть бути свідомо або несвідомо закладені розробниками алгоритмів, а також виникати через використані дані. Щоб уникнути або мінімізувати цей ризик, необхідно забезпечити якість даних, ретельно перевіряти проєктування алгоритмів перед їх впровадженням, а також проводити аудит алгоритмів – як їхньої структури та функціонування, так і результатів, які вони генерують [1].

Ще один технологічний ризик пов'язаний із браком прозорості, тобто складністю або неможливістю зрозуміти, як саме алгоритм було створено, як він працює або яким чином відбувається автоматизована обробка даних, що приводить до певного результату. Непрозорість алгоритмів може мати різні причини:

– технічні – складність і динамічність структури алгоритмів або величезний обсяг даних, що використовуються;

– правові – пов'язані із захистом інших прав чи інтересів (наприклад, громадської безпеки, інтелектуальної власності, конфіденційності, процесу ухвалення рішень чи захисту персональних даних);

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 2(1) 2025
Series «Public management and administration»

– організаційні – коли державний орган не формалізував рішення про використання алгоритму або не має повної інформації про нього.

Для зменшення цього ризику деякі уряди вже публікують на своїх порталах відкритих даних інформацію про використані алгоритми, їхню структуру та принципи роботи. Інші, як-от Міська рада Барселони та Уряд (Женералітат) Каталонії, створюють реєстри алгоритмів.

Також деякі установи зобов'язані надавати громадянам інформацію про використані алгоритми на їхній запит відповідно до законодавчо гарантованого права на доступ до публічної інформації. Наприклад, про це заявляли такі органи, як Французька комісія з доступу до адміністративних документів (CADA) (рішення №20144578 від 8 січня 2015 року), Регіональний адміністративний суд Лаціо (Італія) (рішення від 14 лютого 2017 року) та Каталонський комітет із гарантування права доступу до публічної інформації (Іспанія) (рішення від 21 вересня 2016 року та 21 червня 2017 року). Втім, саме право на доступ до інформації не завжди є достатнім механізмом для забезпечення прозорості використання алгоритмів [2].

Ще один технологічний ризик стосується захисту персональних даних та приватності осіб. Як зазначає Рада Європи у Декларації про маніпулятивні можливості алгоритмічних процесів (ухваленій 13 лютого 2019 року), «обчислювальні засоби дають змогу робити висновки про найінтимнішу та найдетальнішу інформацію про людину на основі відкритих даних. Це сприяє поділу людей на категорії, посилюючи соціальну, культурну, релігійну, правову та економічну сегрегацію й дискримінацію» [3].

Паралельно з цим, активний розвиток і поширення технологій штучного інтелекту та робототехніки формує новий спектр додаткових соціально-економічних ризиків, які посилюють наявні інституційні та технологічні загрози:

– Заміщення людської праці як у низькокваліфікованих, так і в інтелектуальних секторах («сині» та «білі комірці»), що може спричинити зростання безробіття, соціальну напругу та нові виклики для системи соціального захисту.

– Самонавчання та адаптивність ШІ, які створюють ризик часткової або повної втрати контролю з боку людини над процесами прийняття рішень.

– Невизначеність у сфері відповідальності за наслідки управлінських рішень, ухвалених із використанням ШІ, зокрема питання соціальної чи юридичної відповідальності алгоритмів.

– Мілітаризація штучного інтелекту та обмежені можливості міжнародного й національного регулювання цього процесу, що створює загрози безпеці.

– Дискримінаційні ефекти, пов'язані з використанням неповних, неточних або упереджених даних, що можуть призводити до несправедливих управлінських рішень.

– Порушення конфіденційності персональних даних і, як наслідок, зниження довіри громадян до органів публічної влади.

– Порушення етичних та правових норм під час розроблення й впровадження систем штучного інтелекту.

– Проблеми кібербезпеки, що полягають у необхідності забезпечення стійкості ШІ до кібератак, спрямованих на незаконне втручання, знищення чи викрадення баз даних, персональної інформації або блокування публічних ресурсів і мереж [4].

Водночас варто підкреслити, що ризики, пов'язані із застосуванням штучного інтелекту в системі публічного управління, не є сталими. Вони змінюються під впливом геополітичних обставин, соціально-економічної ситуації, політичного клімату та поточних суспільно-політичних процесів, що зумовлює потребу у постійному моніторингу, адаптації нормативно-правових підходів і розвитку механізмів управління цими ризиками.

Використовуючи ШІ, органи публічної влади мають діяти в повній відповідності до норм законодавства про захист персональних даних. Для цього необхідно оцінювати вплив будь-яких рішень або дій, заснованих на ШІ, на захист персональних даних; дотримуватися таких принципів, як законність, справедливість і прозорість; обмеження мети; мінімізація даних; точність; обмеження строків зберігання; цілісність і конфіденційність; підзвітність; гарантувати реалізацію прав громадян, передбачених законодавством, зокрема права на інформування, доступ, виправлення, видалення та обмеження обробки даних.

Отже, використання штучного інтелекту у публічному управлінні відкриває значні можливості для підвищення ефективності державного управління, проте супроводжується низкою ризиків, що потребують усвідомленого та системного врегулювання. Основними з них є інституційні, технологічні та соціально-економічні ризики, серед яких особливу небезпеку становлять упередженість алгоритмів, непрозорість прийняття рішень, порушення етичних і правових норм, а також загрози приватності громадян. Для їх мінімізації необхідно забезпечити якість даних, аудит алгоритмів, відкритість інформації про їхнє застосування, дотримання принципів законності та підзвітності, а також формування ефективної системи моніторингу впливу ШІ на суспільство.

ISSN 3083-6417 (online)
ISSN 3083-6409 (print)
№ 2(1) 2025

References

1. O'Neil, C. (2018). Armas de destrucción matemática. *capitanswing.com.* Retrieved from: https://capitanswing.com/libros/armas-de-destruccion-matematica/ [in Spanish].
2. Brauneis, R. & Goodman, E.P. (2017). Algorithmic transparency for the smart city. *Yale Journal of Law & Technology*, 20, (pp. 104-176) [in English].
3. Cerrillo Martínez, A. (2024). The use of artificial intelligence in public administration. *Review of International and European Economic Law*, 3(5). Retrieved from https://rieel.com/index.php/rieel/article/view/91 [in English].
4. Obolenskyi, O.Iu., Kosytska, V., & Rvach, A. (2023). Shtuchnyi intelekt u publichnomu upravlinni: vymohy, problemy ta ryzyky [Artificial intelligence in public administration: requirements, problems and risks]. *Vcheni zapysky: zb. nauk. pr. - Scientific notes: collection of scientific papers*, 33, (pp. 121-137) [in Ukrainian].

DOI 10.34132/mspc2025.02.13.35

Oksana Malikina
Tetiana Medvedenko

RISKS OF USING ARTIFICIAL INTELLIGENCE IN PUBLIC ADMINISTRATION

The materials present an analysis of the risks that arise in the process of implementing and using artificial intelligence (AI) technologies in the public administration system. It is found that AI as a complex of information technologies generates socio-economic, technological and institutional risks that affect the effectiveness of the functioning of state institutions and the observance of citizens' rights. The main threats are outlined, in particular, the bias of algorithms, the opacity of decision-making processes, violation of the confidentiality of personal data, the militarization of AI, the risks of losing control over algorithms and the socio-economic consequences of automation. It is determined that the dynamism of these risks requires a systematic approach to their monitoring, improvement of regulatory and legal regulation and an increase in the level of responsibility of public authorities in the field of AI application.

Keywords: *artificial intelligence, public administration, risks, transparency, algorithmic bias, personal data protection, cybersecurity, socio-economic consequences.*

Відомості про авторів / Information about the authors

Оксана Малікіна, старший викладач кафедри публічного управління та адміністрування, Юридичного факультету, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: oksi_mal@ukr.net, https://orcid.org/0000-0002-3377-3443.

Oksana Malikina, Senior Lecturer, Department of Public Management and Administration, Faculty of Law, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: oksi_mal@ukr.net, https://orcid.org/0000-0002-3377-3443.

Тетяна Медведенко, магістр кафедри публічного управління та адміністрування, Юридичного факультету, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: redmired1980@gmail.com.

Tetiana Medvedenko, Master's student of the Department of Public Management and Administration, Faculty of Law, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: redmired1980@gmail.com.

 Стаття отримана редакцією 03.10.2025.