УДК 34:004.8
DOI 10.31732/2708-339X-2024-11-A11

ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ПРИВАТНОСТІ В УМОВАХ РОЗШИРЕНОГО ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Бакуменко А.В.,
аспірант юридичного факультету
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: bakumenko.andrii@meta.ua
ORCID: https://orcid.org/0009-0005-1859-0859

Загребельна Н.А.,
кандидат юридичних наук
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail:NataliaZa@krok.edu.ua
ORCID: https://orcid.org/0000-0002-3390-7149

PROTECTION OF CONFIDENTIALITY AND PRIVACY IN THE CONTEXT OF WIDESPREADING USE OF ARTIFICIAL INTELLIGENCE

Bakumenko A.V.,
PhD student, «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: bakumenko.andrii@meta.ua
ORCID: https://orcid.org/0009-0005-1859-0859

Zahrebelna N.A.,
Ph.D. in Law, «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail:NataliaZa@krok.edu.ua
ORCID: https://orcid.org/0000-0002-3390-7149

***Анотація**. У статті проаналізовано сучасні проблеми захисту режиму приватності людського життя в умовах застосування технологій штучного інтелекту. Дослідження дозволяє провести комплексний аналіз щодо ступеня впливу штучного інтелекту на захист персональних даних. Розширення меж використання таких технологій у повсякденному житті людинини та в сфері державного регулювання водночас оголило деякі проблемні моменти й потенційні загрози щодо процедури обробки і збору конфіденційної інформації.*

Зростання потоків даних та інформації свідчить про сьогоднішній інформаційний вибух. Інформація стає все більш доступною і різноманітною, тому постійно виникають питання щодо захисту приватності стейкхолдерів цієї інформації. А наявність та динамічний розвиток штучного інтелекту прискорює ці тенденції. Процеси сучасного аналізу даних на 100% залежать від машинних алгоритмів і технологій, особливо стосовно алгоритмів пошуку рекомендацій. Використання інтелекту порушує відповідні конфіденційні інтереси власників за рахунок швидкості збору й детального аналізу персональної інформації.

У статті визначено, що інформаційна безпека – це захищений інформаційний простір, здатний забезпечити реалізацію державних інтересів та збереження стійкості держави до внутрішніх і зовнішніх чинників, які становлять загрозу та пов'язані з активним розвитком діджиталізації. Доведено, що використання технології штучного інтелекту дозволяє приймати рішення швидше та з більшою ефективністю. А це, в свою чергу, дозволяє ідентифікувати оптимальні варіанти реагування на потенційні безпекові інциденти. Також доведено, що більшість інтелектуальних систем не мають у своїх алгоритмах «людського чинника» і практично цілком виключають людину з процесу прийняття рішення із забезпечення захисту інфобезпеки.

Розвиток та використання штучного інтелекту зміцнюють усі стратегічні рішення, однак необхідно з

обережністю ставитися до безапеляційного його використання для задоволення потреб й інтересів усіх стейкхолдерів у питанні інформаційної безпеки. Прийняття рішень за допомогою технологій штучного інтелекту допомагає знаходити загрози, попереджувати ризики та виконувати відповідні дії. Більш того, методи штучного інтелекту і машинного навчання відіграють вирішальну роль у покращенні протоколів інформаційної безпеки.

Ключові слова: *штучний інтелект, конфіденційність, приватність, персональні дані, інформаційна безпека, права і свободи людини і громадянина.*

Формул*: 0, рис.: 0, табл.: 0, бібл.: 11.*

Abstract*. The article analyzes the current problems of protecting the privacy of human life in the context of artificial intelligence technologies. The research allows for a comprehensive analysis of the degree of AI's impact on personal data protection. The expansion of the use of such technologies in everyday human life and in the sphere of government regulation has exposed certain problematic issues and potential threats to the process of processing and collecting confidential information. The increase in data and information flows indicates today's information explosion. Information is becoming increasingly accessible and diverse, which raises constant questions about the privacy protection of stakeholders of this information. And the presence and dynamic development of artificial intelligence accelerate these trends. Modern data analysis processes are 100% dependent on machine algorithms and technologies, especially regarding recommendation algorithms. The use of AI disrupts the corresponding confidential interests of owners through the speed of data collection and detailed analysis of personal information. The article defines information security as a protected information space capable of ensuring the realization of state interests and the preservation of the state's resilience to internal and external factors that pose a threat and are related to active digitalization. It has been proven that the use of artificial intelligence technology allows for faster and more efficient decision-making, which, in turn, enables the identification of optimal responses to potential security incidents. It has also been demonstrated that most intelligent systems do not have a «human factor» in their algorithms and practically exclude humans from the process of decision-making in ensuring information security. The development and use of artificial intelligence strengthen all strategic decisions, but caution must be exercised in its unconditional use to satisfy the needs and interests of all stakeholders regarding information security. Decision-making using AI technologies helps identify threats, prevent risks, and take appropriate actions. Furthermore, artificial intelligence and machine learning methods play a crucial role in improving information security protocols.*

Keywords*: artificial intelligence, confidentiality, privacy, personal data, information security, human rights and freedoms.*

Formulas*: 0, fig.: 0, tabl.: 0, bibl.: 11.*

Постановка проблеми. Наразі важко собі уявити сьогодення без технологій штучного інтелекту. Вони з кожним днем захоплюють усе більше аспектів повсякденного життя, а також професійну сферу. Такі технології використовують у медицині, промисловості, господарстві, не кажучи вже про освіту та оборонний сектор. За допомогою алгоритмів штучного інтелекту в новітніх смартфонах влаштовано технологію розпізнавання обличчя, в автомобілях частіше з'являються (як базові) функції «Автопілот» і бортовий комп'ютер, є безліч роботів та віртуальних помічників. Саме процес швидкого поширення відповідної технології вимагає отримання детальних знань і навичок, що допоможуть розібратися з процесом та можливими наслідками використання.

Застосовуючи штучний інтелект, можна не тільки збільшити швидкість обробки великих масивів даних, а й одночасно проаналізувати та в подальшому використати отримані результати в навчанні чи для розробки адаптивних моделей і проведення аналітичних заходів. Також слід зазначити, що, застосовуючи технології, можна зіткнутися з певними закритими та відкритими ризиками. Насамперед важливо приділити увагу тим ризикам, які пов'язані з отриманням недостовірної чи неправильної інформації й, відповідно, отримання негативного результату аналізу. А також ризикам, пов'язаним з розкриттям приватності та конфіденційності для всіх стейкхолдерів цієї інформації. Непередбачуваність наслідків використання нейронних мереж здатна створити проблеми на приватному рівні, а також на рівні держави через загрозу дискримінації даних чи «грою» з конфіденційністю.

Аналіз останніх досліджень та публікацій. Цими питаннями опікувалися багато теоретиків і практиків від науки. Окремої уваги слід приділяти роботам М. Бурової, О. Баранова, О. Глазова, А. Гончарової, О. Адамчука, Є. Харитонова, О. Кармази, Д. Проць, Л. Вікторової, Л. Живцової та інших.

Не вирішені раніше частини загальної проблеми. Серед представників

різних кіл і статусів побутує думка, що найбільш перспективною технологією сьогоднішнього дня є саме штучний інтелект, який усе більше впливає на всі аспекти життя, а також на прийняття рішень у цих аспектах. Особливого значення та актуальності в спектрі суспільних відносин набуває його використання в системі забезпечення інформаційної безпеки, оцінки та аналізу інформаційних загроз у контексті інформаційного опору з метою захисту територіальної цілісності України і суверенітету, що належить до концептуальних основ діяльності суспільства. Також необхідно зауважити, що не повністю розкритим і дослідженим є питання щодо правового регулювання та забезпечення штучного інтелекту. Наприклад, його співвідношення з основоположними правами людини й громадянина, а також з правом інтелектуальної власності. Зараз точиться багато теоретичних дискусій щодо цього питання, але, на жаль, без однозначних відповідей.

Формулювання цілей статті. Метою статті є повноцінне обґрунтування використання штучного інтелекту в інформаційній безпеці в умовах зовнішніх та внутрішніх загроз.

Виклад основного матеріалу дослідження. Сучасний динамічний розвиток нашого суспільства та технологій потребує більш уважного й ретельного ставлення до такого його аспекту знань, як інформація. Саме остання стає тим стратегічним ресурсом, що систематично накладає свій відбиток як на процес становлення сучасного демократичного суспільства, так і на безпеку країни загалом. Основною складовою будь-якої системи державної безпеки є її інформаційна безпека. Це поняття є якісним мірилом розвитку: державного, економічного, соціального, інформаційного. Водночас воно залежить від впливу чинників усередині країни та тих, які знаходяться за її межами. Гарантом забезпечення безпеки і стримування політичної ситуації у країні має бути саме держава [4, с. 17].

Важливого значення в сучасних умовах регулювання інформаційної безпеки набуває технологія штучного інтелекту. Він представляє собою результат людської діяльності, здатний до логічного мислення, управління своїми діями, обґрунтовування своїх рішень, які не може коригувати в разі зміни умов. Технології сьогодення реалізуються за такими напрямами: розпізнавання та синтез мови; інтелектуальні системи підтримки прийняття рішень та інші [5].

Для регулювання всіх внутрішніх процесів використання штучного інтелекту розпорядженням Кабінету Міністрів України №1556-р схвалено Концепцію його розвитку в Україні, яка передбачає визначення основних напрямів і пріоритетних завдань розвитку технології штучного інтелекту з метою забезпечення конкурентоспроможності національної економіки та захисту технологічних інформаційно-комунікаційних систем. При чому забезпечення інформаційної безпеки визначено як її основний напрямок [6].

З плином часу й удосконаленням життя штучний інтелект уже став не лише чимось сюрреалістичним чи просто теоретичним надбанням творів наукової фантастики. Він тепер розглядається вже в реальній площині та потужно вливається в усі сфери нашого життя. Нові можливості машинного аналізу даних і прийняття рішень перетворили вчорашнє неможливе в розряд повсякденності, водночас автоматично ставить перед суспільством нові питання щодо юридичного статусу цієї технології та наслідків від її діяльності.

Варто зазначити, що використання інтелекту в роботі й повсякденному житті дозволяє отримати безліч переваг у швидкості обробки інформації та в оптимізації процесів. Так, наприклад, він допомагає у процесі написання електронних листів, повідомлень або презентацій. Зараз кожен з нас, використовуючи відомий ChatGPT, має можливість швидко знайти інформацію і підготувати доповідь. Алгоритми машинного інтелекту згладжують людські недоліки, відсутність знань та навичок для того, щоб перетворити окремі розрізнені думки на сформульоване й змістовне повідомлення чи висновок.

Проте не слід забувати про те, що, ви-

користовуючи будь-яке джерело інформації, слід раціонально та з обережністю ставитися до цієї інформації. Це також стосується рішень, які були запропоновані алгоритмами ChatGPT.

Завдяки зворотній реакції користувачів на використання штучного інтелекту ми отримуємо вигоду як для себе, так і для самої технології. З одного боку, отримуємо те рішення чи аналіз, що нам потрібен, з іншого – покращуємо діючі текстові й голосові алгоритми, а також з'являться нові. Не варто бездумно та необережно ставитися до надання повного й відкритого доступу штучному інтелекту як до персональної, так і до корпоративної інформації. Наразі немає повної гарантії відсутності зловживання нею зі сторони власників відповідних алгоритмів. Саме це питання щодо захисту інформації, а також її збереження та недоторканність стали ключовими аспектами подальшого динамічного розвитку технології без завдання шкоди його користувачам.

Яскравим прикладом попереднього твердження є реальний та вже історичний факт. Починаючи з перших тижнів воєнного вторгнення, компанія з розпізнавання облич Clearview AI стала співпрацювати з українським урядом і передала Україні свою технологію. Наразі Мінцифри зазначає, що завдяки Clearview AI вже зібрано понад 30 млрд світлин, які вже повноцінно та з користю застосовуються для допомоги в розкритті військових злочинів рф [8]. З одного боку, це крок, який можна розглядати як позитивний в умовах військової агресії, а з іншого – це стало наріжним каменем для суспільства. Причиною є те, що технологія Clearview AI почала використовуватися не лише для первинної ідентифікації загиблих чи полонених військових з обох сторін, а й для використання проти цивільного населення, особливо для розпізнавання громадян на блокпостах та видачі повісток. Як сама компанія, так і український уряд запевняють про безпечність її використання, адже всі дані зашифровані алгоритмами штучного інтелекту, що унеможливлює отримання до них доступу. Проте варто зазначити, відкритим є факт порушення правового основоположного принципу – права на конфіденційність інформації. Адже така технологія самостійно та автоматично збирає й використовує дані користувачів з відкритих джерел без їх згоди.

На наш погляд, головна цінність від використання технології штучного інтелекту є те, що він враховує навіть ті фактори, які є «закритими» для людини, а також те, що ці дані додаються до загального аналізу й формують нові знання, яких не було раніше. Відбувається розширення набутої бази знань та досвіду. Виходячи з основного чинника розвитку, безпека інформації є важливим фактором національного розвитку і можливості держави відчувати та долати кризу, навіть в умовах воєнної агресії ззовні. Саме реальна й своєчасна реакція з боку держави для забезпечення інформаційної безпеки є гарантом стабільного соціально-економічного та політичного життя країни [3, с. 528].

То що ж слід відносити до конфіденційної інформації й що варто вважати несанкційованим доступом до неї? Без сумніву, це коли персональні дані користувачів застосовуються та поширюються без їх особистої згоди. Виняток становлять лише приписи частини 2 статті 14 Закону України «Про захист персональних даних». За цією нормою, поширення персональних даних без згоди дозволяється у випадках, визначених Законом, і лише (якщо це практично необхідно) в інтересах національної безпеки, економічного добробуту, прав людини. Для прикладу, формуючи запит до певної структури, ми не можемо реально контролювати, як вони використовуються в подальшому [2].

Однозначним та таким, що не потребує додаткових доказів, є факт, що штучний інтелект не повною мірою може забезпечити захист прав людини. Якщо у країнах ЄС подібний механізм є дієвим і формалізованим, то в Україні він зовсім не працює (навіть якщо такий уже повноцінно використовується на практиці). Для прикладу, в Україні в медицині діє інформаційна система Helsi. У ній зібрано персональну інформацію про пацієнтів не лише загальноприйняту, а й конфіденційну медичну. Тому, потрапивши не в ті руки, ця інформація може бути використана проти її стейкхолдерів. Так, за

умови окупації певної частини території медична інформація про воїнів ЗСУ, учасників інших збройних формувань, волонтерів та простих громадян може нести пряму загрозу життю відповідних осіб.

Захист права приватності – досить широке поняття. Воно стосується не тільки захисту персональних даних, а й системи публічного стеження й перегляду кореспонденції. Наразі в умовах гібридної війни важливо, щоб при використанні штучного інтелекту було забезпечено безпеку інформації і не завдано шкоди людині й соціуму [5, с. 20].

Ще одним аспектом права на приватність є забезпечення права на свободу зборів та висловлювань. Штучний інтелект за допомогою власних алгоритмів і фільтрів може обмежувати право на свободу висловлення через блокування акаунтів у соціальних мережах. Причиною таких дій можуть бути: публікація дописів, що несуть небезпеку чи порушують права людей, прояви булінгу, прояви расової або національної дискримінації. З розвитком технологій та в умовах війни значного поширення набувають ботоферми. Це використання фейкових акаунтів і надсилання алгоритмічних текстів чи коментарів, які мають на меті розпалення ворожнечі та поширення дезінформації чи закликів до терористичних дій. Використання фільтрів й алгоритмів допомагає заблокувати акаунти та запобігти розповсюдженню фейкової інформації. Тут є одна важлива ремарка. При використанні передових технологій слід керуватися моральними принципами. Інакше це призведе до поширення неправдивих закликів, дозволить здійснювати маніпулювання мільйонами думок людей [9].

Варто зазначити, що для ефективного використання новітніх технологій і штучного інтелекту для захисту від кіберзагроз та забезпечення прав і приватності користувачів у віртуальному середовищі слід чітко їх закріпити законодавчо. Першим кроком стало підписання та набуття чинності Загального регламенту про захист персональних даних. Цей документ має наразі встановити правила збору, обробки і зберігання персональних даних [10].

Однак слід зазначити, що це стосується тільки країн ЄС та є вже реальні приклади його застосування. Для прикладу, в Італії було обмежено використання ChatGPT. Таке рішення було прийняте з міркувань і занепокоєнь у питанні обробки персональних даних, а саме через неналежне законодавче закріплення цих процесів. Відсутня правова основа щодо масового збору та обробки інформації для подальшого вдосконалення й самонавчання штучних алгоритмів платформ. Українське право в цьому питанні перебуває в зародку. Винятком можна вважати лише новий Закон «Про авторське право та суміжні права». У цьому документі врегульовано питання закріплення авторського права на продукти, створені за допомогою штучного інтелекту [11].

Водночас постає питання належності авторських прав. Кому вони належать? Тому, хто створив алгоритм, чи тому, хто, його використовуючи, сформулював відповідний запит для штучного інтелекту, чи самому штучному інтелекту? Для різних систем права це питання врегульовується по-різному. Англосаксонське право заперечує можливість надання прав інтелектуальної власності будь-яким сутностям, окрім людини. Саме використання штучного інтелекту є не тільки правом, але й обов'язком та відповідальністю особи [10].

Зараз точаться певні дискусії щодо правосуб'єктості питання використання штучного інтелекту. Немає єдиної думки щодо цього питання. Деякі вважають, що вже настав той час та умови, коли машинному інтелекту слід надавати такі ж права, як і фізичним особам. Інші – правам юридичних осіб. Однак наразі немає чіткої юрисдикції для штучного інтелекту як суб'єкта права. Наступним кроком створення правової основи для штучного інтелекту стало прийняття в Європарламенті проєкту Artificial Intelligence Act. Головна задача Акта – захист прав та свобод особи при використанні штучного інтелекту. В ньому прописано основні принципи і правила обробки персональних даних та застосування машинного інтелекту при прийнятті рішень. Цей проєкт повинен стати першим Законом про штучний інтелект. Наша держава також бере

участь у його імплементації та зробила перший крок – запущено платформу sandbox – для розробників цієї технології [1].

Висновки. Отже, у статті розглянуто актуальну та цікаву тему визначення й регулювання питання застосування новітніх технологій штучного інтелекту, а також їх вплив на основи приватного життя та інформаційну безпеку держави. Це питання, крім позитивних моментів, як-то збільшення швидкості обробки інформації й можливості одночасного аналізу та використання, має негативний бік у вигляді проблеми забезпечення приватності отриманої так інформації.

Не розкритим є питання прав власності на «твори» штучного інтелекту, а також чи є вони персоніфікованими. Немає законодавства про захист персональних даних, в якому повноцінно закріплюється це питання. Слід розробити систему управління, яка не суперечить принципам верховенства права. Саме держава повинна виступити рушійною силою та відігравати головну роль у процесі створення дієвого механізму при розробці системи штучного інтелекту. Необхідно розробляти оновлені механізми, втілювати заходи аби покращувати існуючу систему і структуру захисту конфіденційності та інформаційної безпеки держави й соціуму при використанні технологій штучного інтелекту.

Не потрібно боятися використання штучного інтелекту, треба лише правильно його використовувати та покращувати, бо прийняття рішень за його допомогою дає можливість знаходити загрози, попереджувати ризики і виконувати відповідні дії. Дієва стратегія щодо інформаційної безпеки в майбутньому дозволить захистити дані від несанкціонованого доступу та розробки алгоритмів дій держави для їх захисту. Всі ці процеси перебувають зараз на початковому етапі розвитку, тому необхідно всіляко проводити політику заохочення створення нових принципів діяльності й захисту персональної інформації. Враховуючи той факт, що наша держава є кандидатом для вступу в ЄС, у національному законодавстві передбачена процедура гармонізації з законодавством ЄС. Саме ефективність правового регулювання штучного інтелекту в Україні має забезпечити створення збалансованої системи та сприятиме захисту прав громадян і підтримку інноваційного розвитку країни.

Література:

1. Artificial Intelligence and Privacy – Issues and Challenges. URL: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificialintelligence-and-privacy-issues-and-challenges/#conclusion (дата звернення: 07.02.2024).
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI /ВРУ. URL : https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 07.02.2024).
3. Долян І. В., Тимошенко Є. А. Правове регулювання використання систем штучного інтелекту в смарт сіті. Юридичний науковий електронний журнал. 2021. № 11. С. 525-528.
4. Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина V.S. Штучний інтелект: проблемні аспекти. Інформація і право. 2020. № 4(35). С. 56-66.
5. Гуржій Т. Інформаційне право: виклики гібридної війни. Зовнішня торгівля: економіка, фінанси, право. 2018. № 4. С. 16-26.
6. Концепція розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 07.02.2024).
7. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17-23.
8. Укроборонпром хоче використовувати штучний інтелект в «оборонці». URL: https://www.epravda.com.ua/news/2021/08/26/677230 (дата звернення: 07.02.2024).
9. Буров М. Хто несе відповідальність за помилки штучного інтелекту? URL: http://uz.ligazakon.ua/ua/magazine_article/EA012676 (дата звернення: 07.02.2024).
10. Бисага Ю. М., Бєлов Д. М., Заборовський В. В. Штучний інтелект та авторські і суміжні права. Науковий вісник УжНУ. Серія «Право». Вип. 76(2). Ч.2. 2023. С. 299-304.
11. Бисага Ю. М., Бєлова М. В. Виклики для прав дитини у зв'язку з розвитком штучного інтелекту. Науковий вісник УжНУ. Серія «Право». Вип. 77. Ч. 1. 2023. С. 90.

Referenses:

1. «Artificial Intelligence and Privacy – Issues and Challenges» (2023), available at: https://ovic.vic.gov.au/privacy/resources-for-organisations/artificialintelligence-and-privacy-issues-and-challenges/#conclusion (Accessed 07 February 2024).

2 .«On the protection of personal data: Law of Ukraine dated 01.06.2010 №.2297-VI / VRofUkr (2010) available at: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Accessed 07 February 2024).
3. Dolyan I. V., Tymoshenko Ye. A. (2021), «Legal regulation of the use of artificial intelligence systems in the smart grid», Yurydychnyy naukovyy elektronnyy zhurnal. Vol. 11, pp. 525-528.
4. Kosilova O. I., Solodovnikova Kh. K. (2020), «Rights and freedoms of man and citizen V.S. Artificial intelligence: problematic aspects», Informatsiya i pravo. Vol. 4(35), pp. 56-66.
5. Hurzhiy T. (2018), «Information law: challenges of hybrid warfare», Zovnishnya torhivlya: ekonomika, finansy, pravo. Vol. 4, pp. 16-26.
6. «Concept of the development of artificial intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine № 1556-r dated 02.12.2020» (2020), available at: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (Accessed 07 February 2024).
7. Nishchymenko O. A. (2016), «Information security of Ukraine at the current stage of development of the state and society», Nashe pravo. Vol. 1,pp. 17-23.
8. «Ukroboronprom wants to use artificial intelligence in «defense» (2021), available at: https://www.epravda.com.ua/news/2021/08/26/677230 (Accessed 07 February 2024).
9. Burov M. (2019), «Who is responsible for errors of artificial intelligence?» available at: http://uz.ligazakon.ua/ua/magazine_article/EA012676 (Accessed 07 February 2024).
10. Bysaha Yu. M., Byelov D. M., Zaborovskyy V. V. (2023), «Artificial intelligence and copyright and related rights», Naukovyy visnyk UzhNU. Seriya «Pravo». Vol. 76(2). Part 2, pp. 299-304.
11. Bysaha YU. M., Byelova M. V. (2023), «Challenges for children's rights in connection with the development of artificial intelligence», Naukovyy visnyk UzhNU. Seriya«Pravo». Vol. 77. Part 1, pp. 90.

Стаття надійшла до друку 22.02.2024 року