УДК: 004.9:351.74

https://doi.org/10.52058/3041-1254-2025-2(12)-122-137

Моргунова Тетяна Іванівна кандидат технічних наук, доцент, доцент кафедри кримінального аналізу та інформаційних технологій, Одеський державний університет внутрішніх справ, м. Одеса, https://orcid.org/0000-0002-3512-2425

ЕТИЧНІ ВИКЛИКИ ТА ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Анотація. У статті досліджено етичні виклики та правові аспекти використання інформаційних технологій у правоохоронній діяльності. Розглянуто сучасні тенденції цифрової трансформації правоохоронних органів, зокрема застосування штучного інтелекту, аналітичних систем великих даних, систем відеоспостереження та біометричної ідентифікації. Висвітлено переваги цих технологій у контексті підвищення ефективності оперативно-розшукових заходів, покращення аналітики злочинності та оптимізації процесу ухвалення рішень.

Окрему увагу приділено аналізу етичних ризиків, що виникають у процесі цифровізації правоохоронної сфери. Зокрема, розглянуто питання масового стеження за громадянами, втручання у приватне життя, дискримінаційного характеру алгоритмічних рішень та проблеми відповідальності за дії штучного інтелекту. Досліджено баланс між потребами забезпечення громадської безпеки та дотриманням прав людини, що є ключовою проблемою впровадження цифрових технологій у правозастосувальній діяльності.

Представлено огляд міжнародних та національних нормативно-правових актів, що регулюють використання інформаційних технологій у сфері безпеки. Проведено порівняльний аналіз регуляторних підходів Європейського Союзу, США та України щодо правового статусу алгоритмічного правосуддя, захисту персональних даних і запровадження механізмів громадського контролю за цифровими технологіями.

Акцентовано увагу на необхідності вдосконалення чинного законодавства з метою підвищення прозорості алгоритмічних рішень, усунення ризиків упередженості та гарантування захисту персональних даних громадян. Запропоновано напрями реформування нормативної бази, які включають розробку правових стандартів щодо відповідальності за рішення, ухвалені штучним інтелектом, створення незалежних регуляторних органів для моніторингу цифрових систем у правоохоронній діяльності та розширення міжнародної співпраці у сфері цифрової безпеки.

Зазначено, що впровадження інноваційних технологій у правоохоронну діяльність має супроводжуватися не лише технічними змінами, але й етичними та юридичними реформами, що забезпечать дотримання демократичних цінностей і прав людини в умовах цифрової епохи.

Ключові слова: інформаційні технології, штучний інтелект, етичні виклики, правове регулювання, цифровізація правоохоронної діяльності, кібербезпека, алгоритмічне правосуддя, персональні дані.

Morhunova Tetiana Ivanivna Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Criminal Analysis and Information Technologies, Odesa State University of Internal Affairs, Odesa, https://orcid.org/0000-0002-3512-2425

ETHICAL CHALLENGES AND LEGAL REGULATION OF THE USE OF INFORMATION TECHNOLOGIES IN LAW ENFORCEMENT ACTIVITIES

Abstract. This article examines the ethical challenges and legal aspects of utilizing information technologies in law enforcement. It explores contemporary trends in the digital transformation of law enforcement agencies, particularly the application of artificial intelligence, big data analytics, surveillance systems, and biometric identification technologies. The study highlights the advantages of these technologies in enhancing the efficiency of investigative operations, improving crime analytics, and optimizing decision-making processes.

Special attention is given to analyzing ethical risks arising from the digitalization of the law enforcement sector. Specifically, the article addresses issues related to mass surveillance of citizens, intrusion into private life, the discriminatory nature of algorithmic decision-making, and accountability concerns regarding artificial intelligence actions. The research examines the balance between ensuring public security and upholding human rights, which remains a key challenge in implementing digital technologies in law enforcement activities.

The study provides an overview of international and national regulatory frameworks governing the use of information technologies in the security sector. A comparative analysis of regulatory approaches in the European Union, the United States, and Ukraine is conducted, focusing on the legal status of algorithmic justice, personal data protection, and the introduction of mechanisms for public oversight of digital technologies.

The article emphasizes the need to improve existing legislation to enhance the transparency of algorithmic decision-making, mitigate bias risks, and ensure the protection of citizens' personal data. Proposed directions for regulatory reform include the development of legal standards for AI decision-making accountability,

the establishment of independent regulatory bodies to monitor digital systems in law enforcement, and the expansion of international cooperation in digital security.

The article concludes that the implementation of innovative technologies in law enforcement should be accompanied not only by technical advancements but also by ethical and legal reforms to ensure compliance with democratic values and human rights in the digital era.

Keywords: information technologies, artificial intelligence, ethical challenges, legal regulation, digitalization of law enforcement, cybersecurity, algorithmic justice, personal data.

Постановка проблеми. Сучасна правоохоронна діяльність все більше спирається на використання інформаційних технологій, які кардинально змінюють методи роботи органів правопорядку. Впровадження цифрових рішень, таких як штучний інтелект, біометрична ідентифікація, системи відеоспостереження та аналізу великих даних, сприяє підвищенню ефективності правоохоронних органів, швидкості розслідувань та точності ухвалення рішень. Проте разом із цими перевагами виникають і нові проблеми, пов'язані з правовими та етичними аспектами використання цифрових технологій у правозастосувальній сфері.

Однією з ключових проблем є необхідність забезпечення балансу між ефективністю роботи правоохоронних органів та дотриманням основоположних прав і свобод громадян. Виникає питання, наскільки правомірним є застосування масового стеження та наскільки такі технології можуть порушувати право на приватність. Також актуальними залишаються питання кібербезпеки, прозорості ухвалення рішень алгоритмічними системами та ризиків дискримінації через можливі упередження в алгоритмах штучного інтелекту.

Не менш важливим викликом є правове забезпечення цифрових процесів у правоохоронній сфері. Досі не розроблено єдиних міжнародних стандартів щодо відповідальності за рішення, ухвалені на основі штучного інтелекту, а законодавчі норми окремих країн значно відрізняються. Таким чином, виникає потреба у розробці комплексного підходу до регулювання цифрових технологій у сфері правопорядку, що дозволить узгодити ефективне використання новітніх рішень із дотриманням етичних і правових норм.

Аналіз останніх досліджень і публікацій. Проблеми теорії та практики у сфері етичних викликів та правового регулювання використання інформаційних технологій у правоохоронній діяльності розглянуто в багатьох виданнях [1…12]. Загалом проблематика цифровізації правоохоронних органів активно обговорюється у наукових колах, оскільки ця тема має важливе значення для ефективності роботи державних інституцій та захисту прав громадян. У науковій літературі значна увага приділяється питанням

впровадження штучного інтелекту у кримінальні розслідування, використанню аналітичних систем для виявлення злочинних схем та застосуванню цифрових доказів у судових процесах.

Зокрема, багато дослідників розглядають переваги впровадження технологій великих даних (Big Data) у правоохоронній діяльності, що дозволяє аналізувати величезні масиви інформації та знаходити закономірності, які можуть бути недоступними для традиційних методів розслідування. Водночас дослідники наголошують на ризиках використання штучного інтелекту, таких як можливість хибної ідентифікації осіб, дискримінація за расовими або соціальними ознаками, а також недостатня відповідальність за рішення, ухвалені автоматизованими системами.

Крім того, питання захисту персональних даних громадян є одним із ключових аспектів сучасних досліджень у сфері цифрової трансформації правоохоронних органів. Науковці аналізують міжнародні підходи до регулювання цієї проблеми, зокрема Загальний регламент захисту даних (GDPR) Європейського Союзу, та порівнюють їх із національним законодавством різних країн.

Попри значну кількість наукових публікацій, все ще бракує комплексних досліджень, що поєднують технічний, правовий та етичний аспекти цифровізації правоохоронної діяльності. Тому важливим є подальший розвиток цієї тематики, особливо у напрямку визначення чітких стандартів правового регулювання та запобігання зловживанням у сфері застосування цифрових технологій у правозастосуванні.

Метою статті є аналіз етичних викликів та правового регулювання інформаційних технологій у правоохоронній діяльності, оцінка основних загроз, пов’язаних із цифровізацією правоохоронної сфери, а також надання рекомендацій щодо вдосконалення правового регулювання та забезпечення захисту прав людини у контексті цифрової трансформації.

Виклад основного матеріалу. Інформаційні технології відіграють дедалі важливішу роль у правоохоронній діяльності, змінюючи традиційні підходи до розслідування злочинів, підтримки правопорядку та забезпечення громадської безпеки. Використання цифрових рішень дозволяє правоохоронним органам більш ефективно виконувати свої функції, знижувати рівень злочинності та оптимізувати роботу силових структур. Завдяки впровадженню аналітики великих даних, штучного інтелекту та автоматизованих систем, правоохоронні органи отримують можливість оперативніше реагувати на загрози, точніше прогнозувати злочини та підвищувати загальний рівень безпеки в суспільстві.

Проте, крім очевидних переваг, цифровізація правоохоронної сфери породжує низку викликів, серед яких головними є загрози кібербезпеці, етичні дилеми щодо використання технологій стеження, а також можливі

дискримінаційні аспекти у функціонуванні алгоритмів штучного інтелекту. Тому важливо не тільки аналізувати сучасний стан розвитку інформаційних технологій у правоохоронній діяльності, а й оцінювати їхні потенційні ризики та визначати перспективи подальшого вдосконалення з урахуванням принципів законності, етичності та прав людини.

Інформаційні технології, які застосовуються у правоохоронній сфері, охоплюють широкий спектр рішень, що забезпечують ефективну боротьбу зі злочинністю, моніторинг громадського порядку та швидке реагування на правопорушення.

До найважливіших технологій, що використовуються в діяльності правоохоронних органів, належать:

– системи відеоспостереження та розпізнавання облич. Камери спостереження з інтелектуальними алгоритмами аналізу відеопотоку стають невід'ємним елементом сучасних систем громадської безпеки. Вони дозволяють не лише фіксувати події у режимі реального часу, але й автоматично визначати осіб, розпізнавати їхні емоції та ідентифікувати потенційні загрози. Такі технології допомагають правоохоронним органам не лише розслідувати злочини, але й запобігати їм, прогнозуючи ризики у певних місцях на основі історичних даних;

– біометричні технології та бази даних. Використання біометричних даних значно спрощує процес ідентифікації осіб у правоохоронній практиці. Відбитки пальців, сітківка ока, голосові характеристики, а також інші біометричні параметри дедалі частіше використовуються для швидкої ідентифікації підозрюваних та забезпечення точності при перевірці документів. Поєднання біометричних систем із централізованими базами даних дозволяє оперативно відстежувати переміщення осіб, що перебувають у розшуку;

– аналітичні інструменти великих даних (Big Data) у кримінальних розслідуваннях. Сучасні правоохоронні органи щодня працюють з величезними масивами інформації, включаючи записи телефонних дзвінків, відеоспостереження, банківські транзакції, соціальні мережі та багато інших джерел. Використання технологій Big Data дозволяє не лише структурувати ці дані, але й знаходити закономірності, які можуть допомогти в розслідуванні злочинів, оцінці потенційних загроз і виявленні аномальної поведінки;

– використання штучного інтелекту (AI) для прогнозування злочинності. Алгоритми машинного навчання та штучного інтелекту все частіше застосовуються для аналізу кримінальних даних та прогнозування ймовірності вчинення злочинів у певних районах. Наприклад, AI-системи можуть аналізувати попередні випадки злочинності, демографічні дані, економічну ситуацію та інші фактори, щоб прогнозувати місця з підвищеним рівнем ризику та пропонувати відповідні заходи безпеки.

Застосування цифрових рішень у правоохоронній сфері надає значні переваги, які стосуються як підвищення ефективності слідчих дій, так і оптимізації ресурсів. Серед основних позитивних аспектів варто відзначити:

– підвищення ефективності розслідувань. Використання цифрових технологій дозволяє правоохоронцям швидше отримувати, обробляти та аналізувати докази. Наприклад, алгоритми розпізнавання облич можуть за лічені секунди порівняти фото з відеоархівів з базами даних, що значно прискорює процес розкриття злочинів;

– автоматизація процесів та оперативне ухвалення рішень. Сучасні інформаційні системи дозволяють мінімізувати вплив людського фактору на прийняття рішень. Наприклад, автоматизовані системи можуть аналізувати фінансові транзакції на предмет підозрілої діяльності та оперативно передавати відповідну інформацію слідчим;

– посилення контролю за громадською безпекою. Завдяки розширенню мережі відеоспостереження та використанню сенсорних пристроїв правоохоронні органи можуть значно покращити моніторинг міських територій, транспортних вузлів, адміністративних будівель та інших потенційно уразливих об'єктів.

Попри численні переваги, цифровізація правоохоронної діяльності супроводжується низкою серйозних викликів та ризиків, які вимагають ретельного аналізу та ефективних механізмів управління. Серед основних загроз можна виділити такі:

– загрози кібербезпеці. Використання цифрових технологій робить правоохоронні органи вразливими до хакерських атак, спроб злому баз даних та витоку конфіденційної інформації. Наприклад, злочинці можуть маніпулювати даними у базах поліції, що може призвести до викривлення правосуддя;

– використання технологій для незаконного стеження. Незважаючи на позитивні аспекти розпізнавання облич і відеоспостереження, ці технології можуть бути використані без належного правового регулювання, що створює загрозу для прав людини. У деяких країнах вже виникають побоювання щодо масового стеження за громадянами без їхньої згоди;

– помилки алгоритмів та дискримінаційні аспекти. Якщо штучний інтелект навчений на історичних даних, що містять дискримінаційні патерни, це може призвести до упередженого профайлінгу громадян. Наприклад, автоматизовані системи можуть частіше спрямовувати правоохоронців до районів, де проживають менш захищені соціальні групи, що спричиняє несправедливе ставлення до певних категорій населення.

Зважаючи на сучасні виклики, цифровізація правоохоронної діяльності потребує комплексного та зваженого підходу, який враховує не лише підвищення ефективності технологічних рішень, але й дотримання прав людини, відповідність чинному законодавству та етичним принципам.

У сучасних умовах впровадження інформаційних технологій у діяльність правоохоронних органів значно покращує якість роботи у сфері боротьби зі злочинністю, підвищує оперативність розслідувань і забезпечує ефективніше надання правоохоронних послуг. Водночас такі технологічні зміни супроводжуються суттєвими етичними та правовими викликами, які потребують ретельного аналізу та розроблення механізмів належного регулювання й контролю. Зокрема, одним із ключових питань є збереження конфіденційності персональних даних, запобігання дискримінації внаслідок алгоритмічної упередженості, визначення меж відповідальності за рішення, ухвалені системами штучного інтелекту, а також забезпечення ефективного громадського контролю за процесом цифрової трансформації у сфері правопорядку.

Цифрові технології безпосередньо впливають на реалізацію фундаментальних прав і свобод людини [13], тому актуальним завданням є пошук оптимального співвідношення між забезпеченням громадської безпеки та недопущенням надмірного державного контролю за діяльністю громадян. Автоматизовані алгоритми, які використовуються у сфері кримінального правосуддя, потенційно можуть сприяти швидкому виявленню та запобіганню правопорушенням. Однак їх непрозоре застосування створює ризики необ'єктивних висновків, обмеження прав людини та поширення механізмів тотального контролю. У зв'язку з цим важливим аспектом залишається всебічний аналіз етичних дилем, що виникають у процесі цифровізації правоохоронної діяльності.

Одним із ключових викликів цифровізації правоохоронної діяльності є необхідність пошуку оптимального співвідношення між забезпеченням громадської безпеки та захистом персональних даних громадян. У сучасних умовах правоохоронні органи дедалі частіше застосовують технології аналізу великих даних, розпізнавання облич, геолокаційного моніторингу та цифрового профайлінгу. Ці інструменти сприяють оперативному виявленню злочинних намірів, прогнозуванню потенційних загроз та ефективнішій координації дій у кризових ситуаціях. Водночас масове впровадження подібних технологій може призвести до ризиків надмірного державного контролю над приватним життям громадян.

Доступ правоохоронних структур до персональних даних часто аргументується необхідністю запобігання та розслідування злочинів, проте в багатьох юрисдикціях бракує чітких правових норм, які б регламентували порядок збору, зберігання та використання цієї інформації. Відсутність належного регулювання може призвести до зловживань, необґрунтованого стеження та обмеження громадянських свобод. Наприклад, у низці країн зафіксовані випадки використання технологій розпізнавання облич для ідентифікації учасників протестів, журналістів або громадських активістів, що

викликало суспільний резонанс і гостру критику з боку правозахисних організацій.

Крім того, розширення систем відеоспостереження здатне сформувати так званий «ефект суспільства спостереження», коли громадяни усвідомлюють, що перебувають під постійним контролем, і змушені змінювати свою поведінку, навіть якщо не вчиняють правопорушень. Подібна ситуація може мати негативні наслідки для демократичних процесів, сприяючи обмеженню громадянських прав і свобод. Тому важливим завданням залишається розробка механізмів, які забезпечуватимуть ефективне використання технологій у сфері громадської безпеки без порушення фундаментальних прав людини, зокрема права на приватність.

Окремим викликом у застосуванні цифрових технологій у правоохоронній діяльності є проблема алгоритмічної упередженості. Багато сучасних систем безпеки функціонують на основі машинного навчання, аналізуючи великі обсяги даних для оцінки ризиків і ухвалення управлінських рішень. Проте алгоритми, що використовуються в таких системах, можуть мати вроджені похибки через специфіку вихідних даних, на яких вони були навчені.

Зокрема, проблема цифрового профайлінгу (digital profiling) полягає в тому, що автоматизовані системи класифікують осіб за демографічними ознаками, місцем проживання чи соціально-економічним статусом. Це створює ризик дискримінації окремих етнічних чи соціальних груп, які алгоритми можуть помилково ідентифікувати як «потенційно небезпечні» без реальних підстав. Подібні виклики потребують ретельного аналізу та розроблення запобіжних механізмів, які унеможливлять використання алгоритмів для неправомірного обмеження прав окремих груп населення.

Приклади подібних проблем вже були зафіксовані у країнах, що активно застосовують алгоритмічні системи у поліцейській діяльності. Так, у США деякі програми прогнозування злочинності частіше ідентифікували представників расових меншин як потенційних правопорушників, що спричинило серйозні дискусії щодо етичності таких технологій. Для запобігання подібним ситуаціям необхідно запроваджувати регулярний аудит алгоритмів та створювати механізми їхнього незалежного тестування.

З огляду на зростаючу залежність правоохоронних органів від рішень, ухвалених штучним інтелектом, особливої актуальності набуває питання відповідальності за можливі помилки алгоритмічних систем. У традиційній системі правосуддя рішення ухвалюються конкретними посадовими особами, що дає змогу чітко встановити відповідальність у разі зловживань або судових помилок. Водночас у випадку автоматизованих технологій залишається невизначеним, хто має нести відповідальність за їхні дії — розробники програмного забезпечення, правоохоронні органи чи самі алгоритмічні системи.

Якщо алгоритм помилково ідентифікує невинну особу як підозрюваного, наслідки можуть бути серйозними: незаконний арешт, обмеження прав людини або навіть судове переслідування. У таких ситуаціях необхідно мати чітко визначені правові механізми, що дозволяють оскаржувати подібні рішення, а також гарантують захист від несправедливих висновків автоматизованих систем.

Запобігання можливим зловживанням цифрових технологій у правоохоронній діяльності неможливе без ефективного громадського контролю. Важливу роль у цьому процесі відіграють громадські організації, які можуть здійснювати незалежну оцінку ефективності алгоритмічних систем, аналізувати їхній вплив на дотримання прав людини та пропонувати заходи для підвищення прозорості їхнього застосування.

Одним із можливих шляхів розв'язання цієї проблеми є запровадження механізмів незалежного аудиту алгоритмів, що використовуються в правоохоронних органах. Це сприятиме запобіганню ситуаціям, коли державні структури мають виключний контроль над такими технологіями, що може призвести до надмірного втручання в приватне життя громадян.

Залучення громадськості до процесу розроблення політик у сфері цифрової безпеки сприятиме створенню балансу між технологічним прогресом і захистом громадянських прав. Правоохоронні органи повинні бути відкритими до діалогу із суспільством, щоб гарантувати справедливе та прозоре впровадження новітніх технологій.

Швидкий розвиток інформаційних технологій відкриває нові можливості для підвищення ефективності розслідувань, аналізу кримінальних даних та боротьби з правопорушеннями. Проте одночасно з цими можливостями зростають і правові ризики, пов'язані із забезпеченням захисту персональних даних, дотриманням прав людини та правовою визначеністю застосування штучного інтелекту в правоохоронній сфері.

Використання автоматизованих систем, алгоритмічного аналізу та великих баз даних у правоохоронній діяльності потребує ретельного нормативного регулювання, що дозволить забезпечити баланс між громадською безпекою та правами громадян. Однією з ключових проблем є те, що чинне законодавство багатьох країн не встигає адаптуватися до швидких технологічних змін. Це створює правові прогалини, які можуть сприяти як зловживанням з боку державних інституцій, так і правовим маніпуляціям з боку злочинців, що використовують недоліки регуляторної бази у своїх інтересах.

Тому надзвичайно важливим є не лише розробка нових законодавчих норм, а й уніфікація правових підходів до використання інформаційних технологій у правоохоронній сфері. Розгляд міжнародних стандартів, оцінка національного законодавства, його відповідність європейським та світовим

нормам, а також необхідність модернізації правової системи для ефективного управління цифровими загрозами – усе це є ключовими питаннями цього розділу.

Глобальний розвиток цифрових технологій змусив міжнародну спільноту розробити єдині підходи до їх правового регулювання у правоохоронній діяльності. Серед основних документів, що встановлюють правові рамки застосування інформаційних технологій у правоохоронній сфері, можна виділити Генеральний регламент із захисту даних Європейського Союзу (GDPR), Конвенцію Ради Європи 108+ та інші міжнародні акти, що регламентують обробку та збереження персональних даних.

Регламент GDPR, ухвалений у 2018 році, передбачає жорсткі вимоги до збору, зберігання та обробки персональної інформації, а також встановлює механізми контролю за використанням цифрових технологій у державному секторі. В контексті правоохоронної діяльності це означає, що органи безпеки повинні мати правові підстави для збору персональних даних та використовувати їх виключно для чітко визначених цілей. Крім того, регламент забороняє використання алгоритмічного аналізу для дискримінаційного профілювання осіб.

Конвенція 108+ Ради Європи є доповненою версією першої міжнародної угоди щодо захисту персональних даних. Вона закріплює вимоги до правового регулювання використання технологій спостереження та збору інформації. Зокрема, в документі наголошується на необхідності незалежного нагляду за використанням цифрових технологій у правоохоронній діяльності та встановлення чітких меж для застосування автоматизованих систем ухвалення рішень.

Крім цих документів, ООН та ЮНЕСКО розробили рекомендації щодо етичного використання цифрових технологій у правоохоронній сфері. Вони передбачають принципи справедливості, прозорості, людського контролю над системами штучного інтелекту та запобігання упередженому ухваленню рішень алгоритмами. У світі також розглядаються ініціативи щодо створення єдиного міжнародного підходу до регулювання Predictive Policing (прогнозного поліцейського управління) та алгоритмічного правосуддя.

Однак, попри наявність міжнародних стандартів, їх імплементація у національне законодавство різних країн відбувається нерівномірно. Це створює ситуацію, коли одні держави мають суворе регулювання та високий рівень захисту даних, а інші лише починають адаптацію своїх правових норм до цифрової ери.

В Україні законодавство щодо використання інформаційних технологій у правоохоронній діяльності перебуває на стадії розвитку. Основні законодавчі акти, які регламентують обіг цифрових даних, включають Закон України «Про захист персональних даних», Кримінальний процесуальний кодекс та нормативні акти щодо цифрової безпеки.

Закон «Про захист персональних даних» визначає правила збору та обробки інформації, однак його положення не повною мірою відповідають вимогам GDPR. Зокрема, у законі немає чітко визначених санкцій за неправомірний збір даних, а механізми контролю за їх використанням недостатньо ефективні.

Крім того, у сфері кримінального правосуддя в Україні поки що відсутні законодавчі норми щодо застосування штучного інтелекту у слідчих діях. Це створює ризики зловживань та невизначеність щодо відповідальності за автоматизовані рішення.

Для порівняння, у США діють закони про алгоритмічну справедливість, які зобов'язують правоохоронні органи враховувати ризик дискримінації при використанні технологій аналізу великих даних. В ЄС, окрім GDPR, застосовуються додаткові директиви, що встановлюють контроль за використанням систем автоматизованого ухвалення рішень у судочинстві.

Таким чином, аналіз національного законодавства вказує на необхідність його вдосконалення та приведення у відповідність до міжнародних стандартів.

Розвиток технологій штучного інтелекту, біометричних систем та прогнозного аналізу злочинності вимагає нових підходів до їхнього правового регулювання. Одним із ключових питань є визначення правового статусу штучного інтелекту у правоохоронній діяльності. На сьогодні в Україні немає чітких норм, які б визначали межі відповідальності за помилки алгоритмів та автоматизованих систем.

Крім того, необхідно розширити механізми громадського контролю за використанням інформаційних технологій у сфері безпеки. Це може включати незалежні аудити алгоритмів, перегляд нормативних вимог щодо прозорості цифрових рішень та створення механізмів захисту прав громадян від неправомірного використання їхніх персональних даних.

Пропоновані зміни до законодавства повинні включати:

– впровадження обов'язкових незалежних перевірок алгоритмів ШІ, що використовуються у кримінальних розслідуваннях;

– розробку чітких норм щодо застосування технологій розпізнавання облич;

– запровадження додаткових гарантій конфіденційності даних для громадян.

Удосконалення правових механізмів регулювання цифрових технологій у правоохоронній діяльності не лише забезпечить відповідність українського законодавства міжнародним стандартам, а й сприятиме створенню прозорої системи застосування інформаційних технологій у сфері правопорядку. Це, своєю чергою, гарантуватиме захист прав громадян та зміцнення державної безпеки.

Сучасні інформаційні технології істотно змінюють підходи до роботи державних інституцій [13], зокрема правоохоронних органів, удосконалюючи методи розслідувань, підвищуючи рівень громадської безпеки та сприяючи ефективнішому забезпеченню правопорядку. Водночас поряд із розвитком цифрових рішень зростає й кількість викликів, пов'язаних із правовими аспектами їхнього застосування. Використання штучного інтелекту, технології блокчейну, інтернету речей та алгоритмів прогнозування злочинності відкриває нові можливості для правоохоронних структур, однак одночасно створює ризики потенційного порушення фундаментальних прав і свобод людини.

З огляду на те, що цифрові технології активно застосовуються для обробки персональних даних, контролю за громадянами та аналізу поведінкових моделей, постає нагальна потреба у формуванні ефективних правових механізмів їхнього регулювання. Світова практика демонструє різноманітні підходи до правового забезпечення використання новітніх технологій у правоохоронній сфері, проте наявні механізми ще не досягли належного рівня уніфікації. Це ускладнює міжнародну взаємодію в боротьбі з кіберзлочинністю та запобіганням неправомірному застосуванню цифрових систем.

У зв'язку з цим одним із ключових напрямів розвитку правового регулювання є встановлення чітких стандартів, які б визначали допустимі межі застосування інформаційних технологій у правоохоронній діяльності. Основне завдання полягає у пошуку балансу між підвищенням ефективності цифрових рішень та гарантуванням дотримання прав людини. Крім того, важливою є адаптація національних законодавств до міжнародних норм, що сприятиме гармонізації підходів до використання цифрових технологій у правоохоронній сфері та посиленню міжнародної співпраці у протидії злочинності.

Динамічний розвиток цифрових технологій не лише розширює можливості їхнього використання в правоохоронній сфері, але й зумовлює появу нових викликів, які потребують належного правового врегулювання. Одним із перспективних напрямів є застосування блокчейну для захисту баз даних, що дозволяє підвищити прозорість і безпеку інформації. Завдяки своїй децентралізованій структурі ця технологія мінімізує ризики несанкціонованого доступу до даних та їхньої фальсифікації, що робить її ефективним інструментом для ведення реєстрів доказової бази, забезпечення прозорості кримінальних проваджень і контролю за діяльністю правоохоронних органів.

Ще одним перспективним напрямом є вдосконалення алгоритмів автоматизованого виявлення підозрілої поведінки. Використання штучного інтелекту у системах відеоспостереження та аналізу великих масивів даних сприяє ідентифікації потенційних загроз і прогнозуванню ймовірності

вчинення злочинів. Такі алгоритми здатні аналізувати переміщення громадян, їхню поведінку у громадських місцях, виявляти нетипові дії та автоматично передавати відповідні сповіщення правоохоронним органам. Однак подібні системи не позбавлені недоліків, зокрема ймовірності хибних спрацьовувань, що може призводити до необґрунтованих підозр та порушення прав громадян.

Таким чином, ефективне використання цифрових технологій у правоохоронній діяльності потребує комплексного правового регулювання, яке забезпечить їхню безпеку, прозорість і відповідність стандартам захисту прав людини. Формування збалансованої нормативно-правової бази сприятиме не лише вдосконаленню механізмів забезпечення громадської безпеки, а й запобіганню ризикам надмірного державного контролю над суспільством.

Не менш важливим є інтеграція інтернету речей (IoT) у правоохоронну діяльність, що дозволяє створювати інтелектуальні системи безпеки. Сенсори, камери відеоспостереження, датчики руху та інші пристрої, що працюють у єдиній мережі, можуть оперативно передавати інформацію про потенційні загрози, підвищуючи швидкість реагування на інциденти. Водночас необхідно враховувати ризики, пов’язані з можливими кібератаками на такі системи, що може створити загрозу для критичної інфраструктури.

Щоб ефективно використовувати цифрові технології у правоохоронній діяльності, необхідно розробити відповідну нормативно-правову базу, яка б регулювала їхнє застосування. Один із ключових напрямів – вдосконалення законодавства про штучний інтелект у сфері безпеки. Важливим питанням є визначення правової відповідальності за рішення, ухвалені алгоритмами ШІ, зокрема у сфері кримінальних розслідувань. Крім того, слід встановити стандарти прозорості алгоритмів та механізми їхнього незалежного аудиту, що допоможе запобігти дискримінації та упередженості у правоохоронній практиці.

Ще одним важливим аспектом є співпраця міжнародних організацій у розробці цифрових стандартів. Глобальні ініціативи щодо регулювання використання інформаційних технологій мають стати основою для створення єдиних підходів до їхнього застосування у правоохоронній діяльності. Міжнародні організації, такі як ООН, Європейський Союз та Інтерпол, вже розробляють стандарти щодо збереження та обробки даних, які можуть бути використані для розробки національного законодавства.

Окремо слід розглядати захист персональних даних у правоохоронних системах, оскільки масове впровадження цифрових технологій створює загрози для конфіденційності громадян. Необхідно забезпечити жорсткий контроль над обробкою та зберіганням даних, а також запровадити механізми відповідальності за їхнє неправомірне використання.

Ефективне використання інформаційних технологій у правоохоронній діяльності можливе лише за умови тісного співробітництва між державами.

Один із ключових напрямів – розширення можливостей міжнародного моніторингу злочинності. Використання цифрових платформ для обміну інформацією про підозрюваних, транзакції та злочинні схеми дозволить значно підвищити ефективність боротьби з організованою злочинністю.

Важливим аспектом цифровізації правоохоронної діяльності є її роль у протидії глобальним загрозам, зокрема тероризму, кіберзлочинності та нелегальному обігу зброї. Впровадження міжнародних баз даних, що містять інформацію про злочинні угруповання та їхню діяльність, сприяє підвищенню ефективності правоохоронних органів, забезпечуючи швидкий обмін даними та покращуючи координацію міждержавних заходів у сфері безпеки.

Однак використання цифрових технологій має відбуватися з дотриманням принципу балансу між технологічним прогресом і захистом прав людини. Регулювання цифрових інструментів у правоохоронній сфері повинно не лише посилювати контроль за злочинністю, а й гарантувати громадянам належний рівень захисту від можливого надмірного втручання державних органів у приватне життя.

Майбутній розвиток правового регулювання цифрових технологій у правоохоронній сфері потребує розробки нових стандартів щодо застосування штучного інтелекту, удосконалення механізмів захисту персональних даних і зміцнення міжнародної співпраці у сфері боротьби зі злочинністю. Важливим завданням залишається створення правових механізмів, які забезпечать прозорість та підзвітність правоохоронних органів у процесі використання цифрових технологій, що дозволить мінімізувати ризики зловживань.

Поєднання технологічного розвитку з неухильним дотриманням прав людини має стати основою ефективного правового регулювання, що сприятиме впровадженню інноваційних технологій без загрози для демократичних принципів і громадянських свобод.

Висновки. Цифрові технології стають невід'ємною частиною сучасної правоохоронної діяльності, значно підвищуючи ефективність боротьби зі злочинністю, прискорюючи розслідування та забезпечуючи громадську безпеку. Впровадження штучного інтелекту, аналітики великих даних, біометричних систем та відеоспостереження дозволяє правоохоронним органам швидше аналізувати інформацію, ідентифікувати загрози та оперативно реагувати.

Проте поряд із перевагами цифровізації виникають серйозні виклики. Одним із ключових питань залишається захист персональних даних і права на конфіденційність. Використання технологій спостереження та розпізнавання осіб може порушувати права громадян за відсутності належного регулювання та контролю. Тому важливим завданням є розробка чітких правових норм, що визначатимуть межі застосування цих технологій, а також забезпечення незалежного контролю за їх використанням.

Окрім правових викликів, значну загрозу становлять ризики кібербезпеки. Бази даних правоохоронних органів стають об'єктами хакерських атак, що може призвести до витоків конфіденційної інформації та маніпуляцій кримінальними записами. З метою посилення захисту інформації необхідно розвивати технології децентралізованого зберігання даних, такі як блокчейн, та впроваджувати міжнародні стандарти кіберзахисту.

Міжнародне співробітництво відіграє важливу роль у створенні єдиних стандартів використання цифрових технологій у правоохоронній сфері. Досвід країн ЄС, США, ООН та Інтерполу може сприяти адаптації найкращих практик до національного законодавства. Проте така адаптація повинна враховувати особливості національної правової системи, соціальні потреби та етичні аспекти.

Перспективи розвитку цифровізації у правоохоронній діяльності включають удосконалення нормативно-правових актів щодо використання штучного інтелекту, запровадження механізмів незалежного аудиту та контролю, а також посилення гарантій захисту персональних даних. Крім того, важливим напрямком є інтеграція Інтернету речей (IoT) у правоохоронні процеси з дотриманням вимог безпеки та етичних стандартів.

Загалом, ефективне використання цифрових технологій у правоохоронній сфері можливе лише за умови збалансованого підходу, що поєднує технологічні інновації з правовими механізмами захисту громадянських прав. Подальша цифровізація є неминучою, але її успішність залежатиме від того, наскільки ефективно буде врегульовано питання етики, безпеки та правового контролю в цій сфері.

Література:

1. Базові аспекти цифровізації та їх правове забезпечення: монографія / за ред. К.В. Єфремової. Харків: НДІ ПЗІР, 2021. 180 с.
2. Бойко В.В. Правове регулювання штучного інтелекту: міжнародний досвід. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Т. 35 (74), № 2. С. 23-29.
3. Василевська Т.Е. Етика державних службовців і запобігання конфлікту інтересів. Київ: НАДУ, 2013. 76 с.
4. Гиляка О.С. Новітні технології та права людини: аналіз деяких критичних проблем цифрової ери. *Вісник Національної академії правових наук України*. 2023. Т. 30, № 2. С. 15-30.
5. Петришин О.В., Гиляка О.С. Права людини в цифрову епоху: виклики, загрози та перспективи. *Вісник Національної академії правових наук України*. 2021. Т. 28, № 1. С. 17-35.
6. Попова Н.О. Міжнародно-правове регулювання штучного інтелекту: сучасний стан та перспективи. *Юридичний науковий електронний журнал*. 2024. № 4. С. 443-447.
7. Правове забезпечення віртуалізації інфраструктури національної економіки України: монографія / за ред. С.В. Глібка, А.В. Стріжкової. Харків: НДІ ПЗІР, 2019. 184 с.
8. Рудакевич М.І. Професійна етика державних службовців: теорія і практика формування в умовах демократизації державного управління: монографія. Тернопіль: Астон, 2007. 398 с.
9. Сердюк О. Етика бізнесу та коло її проблем. *Філософська думка*. 2005. № 4. С. 93-102.

10. Сова М., Дєніжна С. Міжнародний досвід правового регулювання небезпеки штучного інтелекту в реаліях воєнного часу: етико-філософський аспект. *Філософські та методологічні проблеми права*. 2024. № 1 (27). С. 45-57.
11. Стеца Н. Етичні засади професійної діяльності соціального працівника. *Молодь і ринок*. 2024. № 11 (231). https://doi.org/10.24919/2308-4634.2024.316427.
12. Товмач А.С. Питання етики державних службовців. *Форум права*. 2015. № 2. С. 159-162.
13. Інноваційна економіка: теоретичні та практичні аспекти: монографія / за ред. Д.е.н., доц. Є.І. Масленнікова. Херсон: Грінь Д.С., 2016. 854 с.

***References*:**

1. Yefremova, K.V. (Ed.). (2021). Bazovi aspekty tsyfrovizatsii ta yikh pravove zabezpechennia [Basic aspects of digitalization and their legal support]. Kharkiv: NDI PZIR. [in Ukrainian].
2. Boiko, V.V. (2024). Pravove rehuliuvannia shtuchnoho intelektu: mizhnarodnyi dosvid [Legal regulation of artificial intelligence: international experience]. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia – Scientific Notes of V.I. Vernadsky TNU. Series: Public Administration and Management*, 35(74), 2, 23-29. [in Ukrainian].
3. Vasilevska, T.E. (2013). Etyka derzhavnykh sluzhbovtsiv I zapobiihannia konflikty interesiv [Ethics of civil servants and prevention of conflicts of interest]. Kyiv: NADU. [in Ukrainian].
4. Hilyaka, O.S. (2023). Novitni tekhnolohii ta prava liudyny: analiz deiakykh krytychnykh problem tsyfrovoi ery [Modern technologies and human rights: analysis of some critical problems of the digital era]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy – Bulletin of the National Academy of Legal Sciences of Ukraine*, 30(2), 15-30. [in Ukrainian].
5. Petryshyn, O.V., & Hilyaka, O.S. (2021). Prava liudyny v tsyfrovu epokhu: vyklyky, zahrozy ta perspektyvy [Human rights in the digital age: challenges, threats, and prospects]. *Visnyk Natsionalnoi akademii pravovykh nauk Ukrainy – Bulletin of the National Academy of Legal Sciences of Ukraine*, 28(1), 17-35. [in Ukrainian].
6. Popova, N.O. (2024). Mizhnarodno-pravove rehuliuvannia shtuchnoho intelektu: suchasnyi stan ta perspektyvy [International legal regulation of artificial intelligence: current state and prospects]. *Yurydychnyi naukovyi elektronnyi zhurnal – Legal Scientific Electronic Journal*, 4, 443-447. [in Ukrainian].
7. Hlibko, S.V., & Strizhkova, A.V. (Eds.). (2019). Pravove zabezpechennia virtualizatsii infrastruktury natsionalnoi ekonomiky Ukrainy [Legal support for the virtualization of Ukraine's national economy infrastructure]. Kharkiv: NDI PZIR. [in Ukrainian].
8. Rudakevich M.I. (2007). Profesiina etyka derzhavnykh sluzhbovtsiv: teoriia I praktyka formuvannia v umovakh demokratyzatsii derzhavnoho upravlinnia [Professional ethics of civil servants: theory and practice of formation in the conditions of democratization of public administration]. Ternopil: Aston. [in Ukrainian].
9. Serdiuk, O. (2005). Etyka biznesu ta kolo yii problem [Business ethics and its problems]. *Filosofska dumka – Philosophical Thought*, 4, 93-102. [in Ukrainian].
10. Sova, M., & Denizhna, S. (2024). Mizhnarodnyi dosvid pravovoho rehuliuvannia nebezpeky shtuchnoho intelektu v realiiakh voiennoho chasu: etyko-filosofskyi 137roble [International experience of legal regulation of artificial intelligence risks in wartime realities: ethical and philosophical aspects]. *Filosofski ta metodolohichni 137roblem prava – Philosophical and Methodological Problems of Law*, 1(27), 45-57. [in Ukrainian].
11. Stetsa, N. (2024). Etychni zasady profesiinoi diialnosti sotsialnoho pratsivnyka [Ethical principles of social worker's professional activity]. *Molod I rynok – Youth and Market*, 11(231). https://doi.org/10.24919/2308-4634.2024.316427. [in Ukrainian].
12. Tovmach, A.S. (2015). Pytannia etyky derzhavnykh sluzhbovtsiv [Ethical issues of civil servants]. *Forum prava – Law Forum*, 2, 159-162. [in Ukrainian].
13. Maslennikov, Ye.I. (Ed.). (2016). Innovatsiina ekonomika: teoretychni ta praktychni aspekty: monohrafiia [Innovative economy: theoretical and practical aspects: monograph]. Kherson: Hrin D.S. [in Ukrainian].