



УДК: 004:34

[https://doi.org/10.52058/2786-6300-2025-3\(33\)-613-628](https://doi.org/10.52058/2786-6300-2025-3(33)-613-628)

**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>

## ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У ПРАВОЗАСТОСУВАННІ: СУЧАСНІ ВИКЛИКИ ТА ПЕРСПЕКТИВИ

**Анотація.** В статті показується, що розвиток інформаційно-комунікаційних технологій (ІКТ) суттєво змінює підходи до правозастосування та забезпечення безпеки. Використання цифрових інструментів у правоохоронній діяльності дозволяє автоматизувати ключові процеси, підвищити ефективність оперативно-розшукової роботи, покращити аналітику злочинності та оптимізувати прийняття рішень. Досліджено основні напрями цифрової трансформації правоохоронної сфери, зокрема впровадження штучного інтелекту, систем аналізу великих даних, відеоспостереження та біометричної ідентифікації.

Окрему увагу приділено розгляду етичних викликів, які виникають у процесі цифровізації. Досліджено проблеми втручання у приватне життя, можливі прояви дискримінації в алгоритмічних рішеннях та ризики порушення прав людини через масове використання технологій стеження. Висвітлено питання відповідальності за рішення, ухвалені автоматизованими системами, що набуває особливого значення в умовах зростаючої залежності правоохоронних органів від технологічних рішень.

Стаття також містить аналіз міжнародного досвіду правового регулювання ІКТ у правозастосуванні. Проведено порівняльний аналіз підходів Європейського Союзу, США та України щодо використання цифрових технологій у боротьбі зі злочинністю. Позначено основні положення щодо захисту персональних даних, правового статусу алгоритмічного правосуддя та механізмів громадського контролю за впровадженням ІКТ у сфері безпеки.

Акцентовано увагу на необхідності вдосконалення законодавства, спрямованого на запобігання упередженості в алгоритмічних рішеннях, забезпечення прозорості цифрових технологій та гарантування дотримання прав громадян. Запропоновано шляхи реформування правового регулювання, включаючи розробку стандартів відповідальності за роботу штучного інтелекту, створення незалежних наглядових органів для контролю цифрових систем у правоохоронній діяльності та посилення міжнародної співпраці у сфері цифрової безпеки.



Зазначено, що успішна інтеграція ІКТ у правозастосування можлива лише за умови гармонійного поєднання технологічного прогресу, правових реформ та етичних стандартів, що дозволить забезпечити баланс між громадською безпекою та захистом прав людини у цифрову епоху.

**Ключові слова:** інформаційні технології, цифрове правосуддя, правозастосування, штучний інтелект, алгоритмічні рішення, персональні дані, правове регулювання, етичні виклики, кібербезпека, міжнародний досвід.

**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>

## **INFORMATION AND COMMUNICATION TECHNOLOGIES IN LAW ENFORCEMENT: CURRENT CHALLENGES AND PROSPECTS**

**Abstract.** The article shows that the development of information and communication technologies (ICT) is significantly changing approaches to law enforcement and security. The use of digital tools in law enforcement allows you to automate key processes, increase the efficiency of operational and investigative work, improve crime analytics and optimize decision-making. The main directions of digital transformation of the law enforcement sphere are studied, in particular, the introduction of artificial intelligence, big data analysis systems, video surveillance and biometric identification.

Particular attention is paid to the consideration of ethical challenges that arise in the process of digitalization. The problems of interference in private life, possible manifestations of discrimination in algorithmic decisions and the risks of human rights violations due to the mass use of surveillance technologies are studied. The issues of responsibility for decisions made by automated systems are highlighted, which is of particular importance in the context of the growing dependence of law enforcement agencies on technological solutions.

The article also contains an analysis of international experience in the legal regulation of ICT in law enforcement. A comparative analysis of the approaches of the European Union, the USA and Ukraine to the use of digital technologies in the fight against crime is carried out. The main provisions on the protection of personal data, the legal status of algorithmic justice and mechanisms of public control over the implementation of ICT in the security sector are indicated.

The emphasis is on the need to improve legislation aimed at preventing bias in algorithmic decisions, ensuring the transparency of digital technologies and guaranteeing compliance with citizens' rights. Ways of reforming legal regulation are



proposed, including the development of standards of responsibility for the work of artificial intelligence, the creation of independent supervisory bodies to control digital systems in law enforcement activities and strengthening international cooperation in the field of digital security.

It is noted that the successful integration of ICT in law enforcement is possible only under the condition of a harmonious combination of technological progress, legal reforms and ethical standards, which will ensure a balance between public safety and the protection of human rights in the digital age.

**Keywords:** information technology, digital justice, law enforcement, artificial intelligence, algorithmic solutions, personal data, legal regulation, ethical challenges, cybersecurity, international experience.

**Постановка проблеми.** Сучасна правоохоронна діяльність усе більше залежить від цифрових технологій, які суттєво змінюють методи збору, аналізу та використання інформації у сфері безпеки. Впровадження штучного інтелекту, автоматизованих систем розпізнавання облич, біометричних баз даних і аналітики великих даних дозволяє правоохоронним органам працювати швидше та ефективніше. Проте поряд із цими перевагами з'являється низка викликів, зокрема ризики порушення прав людини, питання захисту персональних даних та необхідність нормативно-правового врегулювання нових технологій.

Одним із головних питань є баланс між безпекою суспільства та правами громадян. Використання технологій масового стеження, аналітики поведінки та алгоритмічного прогнозування злочинності викликає дискусії щодо їхньої відповідності принципам верховенства права та прав людини. Окремі дослідження доводять, що алгоритмічні системи ухвалення рішень можуть мати вбудовані упередження, що призводить до дискримінації окремих груп населення.

Ще однією важливою проблемою є кібербезпека правоохоронної діяльності. Використання цифрових реєстрів, баз даних та автоматизованих систем створює потенційні загрози кібератак, підробки цифрових доказів та витоку конфіденційної інформації. Це вимагає розробки комплексних механізмів захисту даних та посилення нормативно-правового контролю за кіберзагрозами.

Зважаючи на швидкий розвиток цифрових технологій, актуальним завданням залишається формування ефективної правової бази, яка регулюватиме використання інформаційно-комунікаційних технологій (ІКТ) у правоохоронній діяльності. Важливо розробити стандарти відповідальності за рішення, ухвалені штучним інтелектом, та створити прозорі механізми громадського контролю за цифровими системами безпеки.

**Аналіз останніх досліджень і публікацій.** Проблеми теорії та практики впровадження і використання інформаційно-комунікаційних технологій, зокрема, у правозастосуванні висвітлено в багатьох виданнях [1...10].



Дослідження цифровізації правозастосування активно ведуться у світовій науковій спільноті. Значна увага приділяється використанню штучного інтелекту у правоохоронній діяльності, зокрема Predictive Analytics та алгоритмічному прогнозуванню злочинності. У США широко застосовуються автоматизовані системи аналізу злочинних патернів, що дозволяє правоохоронцям розподіляти ресурси ефективніше.

У Європейському Союзі дослідники акцентують увагу на проблемах захисту персональних даних та запобіганні алгоритмічній дискримінації. Загальний регламент захисту даних (GDPR) містить суворі вимоги щодо використання цифрових технологій у сфері правопорядку. Водночас ведеться активна дискусія щодо необхідності створення правових стандартів для регулювання штучного інтелекту у правозастосуванні.

В Україні процес цифровізації правоохоронної діяльності лише набирає обертів. Основними напрямками є впровадження ЄСІТС, розвиток електронного судочинства та інтеграція міжнародних стандартів у сферу безпеки. Однак проблеми нормативно-правового регулювання та кіберзахисту залишаються актуальними.

**Метою статті** є аналіз викликів та перспектив використання інформаційно-комунікаційних технологій у правозастосуванні, оцінка ризиків цифровізації у сфері права та позначення рекомендацій щодо вдосконалення нормативно-правового регулювання інформаційно-комунікаційних технологій.

**Виклад основного матеріалу.** Цифрові технології дедалі більше змінюють правову систему, перетворюючи класичні підходи до правосуддя та правоохоронної діяльності. Раніше правозастосування вимагало паперових документів та особистої присутності учасників. Сьогодні цифрові технології роблять правосуддя швидшим, прозорішим і доступнішим.

До ІКТ у сфері права належать електронне судочинство, цифрові юридичні сервіси, штучний інтелект, блокчейн для цифрових доказів та автоматизовані системи в правоохоронних органах. Таке різноманіття технологій не лише полегшує доступ до правосуддя, а й змінює саму суть правової взаємодії, роблячи її швидшою та ефективнішою.

Одним із ключових наслідків цифровізації є підвищення ефективності правових процесів. Електронний документообіг прискорює розгляд справ, знижує ризик втрати документів та зменшує вплив людського фактора. Цифрові платформи роблять правосуддя доступнішим: громадяни можуть подавати документи, стежити за справами та брати участь у засіданнях онлайн.

Автоматизація юридичних послуг та електронне урядування також відіграють значну роль у розвитку правозастосування. Державні цифрові платформи для реєстрації договорів, подання позовів та юридичних консультацій скорочують бюрократію та підвищують ефективність правової системи. Це не



лише полегшує життя громадян, а й сприяє зменшенню корупційних ризиків у сфері адміністративних і судових процедур.

ІКТ стали ключовою частиною правової системи, змінюючи підхід до правосуддя та роблячи юридичні послуги доступнішими.

Однією з найважливіших складових цифровізації правозастосування є впровадження електронного судочинства. У багатьох країнах, зокрема в Україні, активно розвиваються спеціалізовані платформи, які дозволяють автоматизувати роботу судів. Наприклад, Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) передбачає цифрове адміністрування судових процесів, ведення електронних реєстрів, обмін документами між учасниками судових процесів та можливість дистанційних засідань. Це значно скорочує витрати часу і ресурсів, роблячи судочинство більш доступним та прозорим.

Ще одним важливим напрямом є застосування штучного інтелекту (AI) у правовому аналізі. У деяких країнах алгоритми штучного інтелекту вже використовуються для аналізу судових рішень, прогнозування результатів розгляду справ та підготовки проєктів судових рішень. Такі технології не тільки підвищують точність юридичного аналізу, а й дозволяють мінімізувати ризик судових помилок, які можуть бути наслідком людського фактора. Однак застосування AI у правовій сфері породжує етичні питання щодо його об'єктивності та можливих упереджень у прогнозах рішень.

Блокчейн-технології також знаходять своє застосування у правозастосуванні, особливо в аспекті забезпечення достовірності цифрових доказів. Використання децентралізованих реєстрів унеможливорює підробку документів, що може бути критично важливим для судових розглядів. Крім того, смарт-контракти, що базуються на блокчейні, дають змогу автоматизувати юридично значущі дії, наприклад, виконання договорів без необхідності людського втручання.

Важливу роль у боротьбі зі злочинністю та профілактиці правопорушень відіграють Big Data та Predictive Analytics. Аналіз великих масивів даних дозволяє правоохоронним органам ідентифікувати закономірності у злочинній діяльності, прогнозувати потенційні загрози та оптимізувати стратегії протидії злочинності. Вже сьогодні в деяких містах світу поліція використовує алгоритми прогнозування злочинів, що допомагає ефективніше розподіляти ресурси та знижувати рівень злочинності.

Не менш значущими є хмарні технології у правовій сфері, які сприяють зберіганню та обміну юридичними документами в безпечному цифровому середовищі. Хмарні платформи дозволяють забезпечити доступ до справ у будь-який час, що особливо актуально в умовах пандемії, коли дистанційна робота стала нормою для багатьох юридичних установ.

Отже, застосування ключових інформаційних технологій у правозастосуванні забезпечує ефективність, безпеку та доступність правових процесів, що є критично важливим для розвитку правової держави.



Розвиток цифрових технологій у правозастосуванні відбувається нерівномірно в різних країнах, але загальна тенденція свідчить про поступове впровадження електронного правосуддя та автоматизації правоохоронної діяльності. США, ЄС та Китай є лідерами у застосуванні інноваційних рішень у цій сфері.

У США активно використовуються системи AI для аналізу кримінальних справ та управління судовими процесами. Також існують масштабні бази даних судових рішень, що дозволяють швидко знаходити прецеденти для прийняття рішень у нових справах.

Європейський Союз активно розвиває концепцію цифрового правосуддя. Наприклад, у Естонії вже функціонує система онлайн-судочинства, де справи малозначного характеру можуть розглядатися без фізичної присутності учасників.

Китай пішов ще далі, створивши повністю цифрові «Інтернет-суди», де судові засідання проходять у віртуальному середовищі, а AI допомагає у розгляді типових справ.

Україна має реальні можливості адаптувати міжнародний досвід. Запуск ЄСІТС та розвиток «Дії» сприяють цифровізації правозастосування. Важливо також створити правову базу, що враховує етичні та безпекові аспекти технологій.

Таким чином, міжнародний досвід свідчить, що майбутнє правозастосування нерозривно пов'язане з цифровими технологіями, і їхнє впровадження є необхідною умовою для розвитку сучасної правової системи.

Цифровізація правозастосування, незважаючи на численні переваги, супроводжується низкою серйозних викликів, які впливають на ефективність, законність та соціальну справедливість юридичних процесів. Щоб цифрові технології ефективно працювали в правозастосуванні, необхідно адаптувати законодавство, усунути етичні суперечності, посилити кібербезпеку та зменшити цифровий розрив. Саме тому критичний аналіз цих проблем є необхідним для подальшого успішного розвитку інформаційно-комунікаційних технологій у правозастосуванні.

Головна проблема цифровізації правозастосування – відсутність чіткого законодавства щодо ІКТ у судочинстві та правоохоронних органах. Законодавство багатьох країн, у тому числі України, не встигає за швидкими темпами розвитку цифрових рішень. У результаті виникають ситуації, коли суди та правоохоронні органи змушені імпровізувати у правовому полі, оскільки не існує чітких механізмів для регулювання, наприклад, електронних доказів або застосування штучного інтелекту для винесення судових рішень.

Не менш серйозною проблемою є колізії між національним та міжнародним законодавством. У різних країнах існують різні підходи до захисту персональних даних, використання технологій розпізнавання облич, цифрового



моніторингу громадян тощо. Наприклад, у країнах Європейського Союзу діє Загальний регламент про захист персональних даних (GDPR), тоді як у США відсутній єдиний загальнонаціональний закон про захист персональних даних. Це створює правові розбіжності, які можуть спричиняти труднощі у співпраці між країнами, особливо в питаннях боротьби з кіберзлочинністю та міжнародного судочинства.

Ще одним викликом є відповідальність за рішення, прийняті автоматизованими системами. Використання штучного інтелекту у правозастосуванні дає змогу оптимізувати процеси, але водночас породжує питання щодо відповідальності у разі судової помилки або дискримінаційного рішення, ухваленого алгоритмом. Якщо система прогнозування злочинів помилиться, хто відповідатиме – розробники чи суддя, який використав її дані? Така правова невизначеність створює ризики для громадян і потребує ретельного регулювання.

Розвиток цифрових технологій у правозастосуванні неминує порушує питання етичної відповідальності. Одним із найбільш дискусійних аспектів є проблема дискримінації алгоритмів. Алгоритми штучного інтелекту, які використовуються в судовій системі та правоохоронних органах, можуть відтворювати упередження, закладені у вихідних даних. Наприклад, у США були випадки, коли система COMPAS, що прогнозує ризики рецидиву злочинців, демонструвала расову упередженість. Такі ситуації свідчать про необхідність ретельного тестування та коригування алгоритмів, щоб уникнути автоматизованої дискримінації.

Ще однією гострою етичною проблемою є захист приватності та право на забуття. У цифрову епоху всі дії користувачів залишають цифровий слід, що може бути використано як доказ у суді або для профілактики злочинів. Однак право людини на приватність та видалення даних, закріплене у європейському законодавстві (GDPR), часто вступає в конфлікт із необхідністю державних органів мати доступ до інформації для забезпечення правопорядку.

Не менш важливим є питання втручання держави в особисте життя громадян через цифровий контроль. Технології розпізнавання обличчя і цифровий моніторинг допомагають боротися зі злочинністю, але можуть призвести до надмірного державного контролю. У Китаї, наприклад, подібні технології використовуються для соціального рейтингу громадян, що викликає серйозні дискусії щодо прав людини.

Окремий виклик становить забезпечення кібербезпеки у правовій сфері. Використання цифрових реєстрів, електронних доказів та віддалених судових процесів робить правозастосування більш вразливим до злому державних баз даних та маніпуляцій цифровими доказами. Наприклад, у випадку атаки на судові інформаційні системи або витоку даних із правоохоронних органів існує ризик компрометації ключових юридичних процесів.



Одним із головних завдань є захист електронних правових документів. Враховуючи, що все більше судових рішень та юридичних документів зберігаються в цифровому форматі, необхідно забезпечити їхню достовірність, незмінність і доступність. Технології блокчейн можуть частково розв'язати цю проблему, оскільки вони гарантують неможливість несанкціонованої зміни записів у реєстрах.

Крім того, важливим напрямом розвитку є використання технологій для протидії кіберзлочинності. Аналітичні системи, що базуються на великих даних, можуть допомогти у прогнозуванні та запобіганні кіберзлочинам, але вони також вимагають високого рівня захисту від стороннього втручання.

Цифровізація правозастосування також породжує соціальні виклики, пов'язані з доступністю нових технологій для різних груп населення. Однією з головних проблем є цифровий розрив між різними соціальними верствами. У той час як великі міста мають доступ до сучасних правових технологій, у віддалених регіонах відсутність інтернет-з'єднання, цифрової інфраструктури та низький рівень цифрової грамотності можуть призвести до фактичної недоступності правосуддя для значної частини громадян.

Ще однією важливою проблемою є низький рівень цифрової грамотності, який ускладнює використання новітніх юридичних платформ. Багато громадян, особливо літні люди, не можуть самостійно користуватися електронними сервісами для подання позовів, отримання юридичних консультацій чи участі в судових засіданнях.

Окрім того, варто звернути увагу на виклики автоматизації робочих місць у правозастосуванні. Впровадження алгоритмів та цифрових платформ поступово зменшує потребу у традиційних посадах, таких як судові секретарі або аналітики. Це може призвести до скорочення робочих місць та необхідності перекваліфікації працівників.

Таким чином, цифровізація правозастосування супроводжується низкою юридичних, етичних, кібербезпекових та соціальних викликів, які потребують ретельного аналізу та правового регулювання. Збалансований підхід до впровадження ІКТ у правовій сфері дозволить мінімізувати ризики та забезпечити ефективне використання технологій в інтересах суспільства.

Інформаційно-комунікаційні технології (ІКТ) стали невід'ємною частиною сучасного правозастосування, істотно змінюючи підходи до здійснення правосуддя, правоохоронної діяльності та надання юридичних послуг. Якщо раніше правова сфера значною мірою спиралася на паперову документацію та безпосередню фізичну взаємодію між учасниками процесів, то сьогодні цифрові рішення забезпечують швидкість, ефективність і прозорість роботи судів, правоохоронних органів та юридичних фірм. Практичне впровадження ІКТ у правозастосуванні відбувається у трьох основних



напрямах: розвиток електронного судочинства, використання цифрових технологій у правоохоронній діяльності та автоматизація юридичних послуг через LegalTech-сервіси.

Однією з найвагоміших змін у сфері правозастосування є впровадження електронного судочинства, яке дозволяє значно скоротити бюрократичні процедури та зробити судові процеси більш доступними. Важливу роль у цьому процесі відіграють автоматизовані системи судового документообігу, що дають змогу учасникам процесу подавати документи в електронному форматі, відстежувати їхній статус і взаємодіяти із судовими органами дистанційно. Зокрема, в Україні функціонує Єдина судова інформаційно-телекомунікаційна система (ЄСІТС), яка передбачає ведення електронного діловодства, доступ до судових матеріалів онлайн та автоматизований розподіл справ між суддями.

Крім цього, значний прогрес у сфері електронного судочинства пов'язаний із використанням відеоконференцій у судових процесах. Проведення судових засідань у дистанційному режимі стало особливо актуальним у період пандемії COVID-19, коли багато країн були змушені оперативно адаптувати судові процедури до нових реалій. Впровадження відеозв'язку дозволило зменшити витрати на транспортування учасників процесу, підвищити безпеку свідків та спростити участь у судових засіданнях для осіб із фізичними обмеженнями.

Ще одним інноваційним напрямом є практика онлайн-правосуддя, яка передбачає повністю цифровий розгляд справ без необхідності фізичної присутності учасників. У деяких країнах, таких як Естонія та Китай, вже діють суди, де певні категорії справ розглядаються без традиційних засідань. Це особливо ефективно у випадках малозначних правопорушень або цивільних спорів, які можуть бути вирішені на основі поданих документів і алгоритмічного аналізу справи. Такі технології відкривають перспективи для розширення доступу до правосуддя, зменшення навантаження на судову систему та зниження корупційних ризиків.

Розвиток цифрових технологій також суттєво впливає на роботу правоохоронних органів, підвищуючи ефективність боротьби зі злочинністю та покращуючи механізми кримінальних розслідувань. Одним із найперспективніших напрямів є застосування Predictive Analytics (аналітики прогнозування) у кримінальних розслідуваннях. Ця технологія базується на аналізі великих масивів даних (Big Data) для виявлення закономірностей злочинної поведінки та прогнозування потенційних загроз. Наприклад, у США використовуються алгоритми, які на основі історичних даних можуть прогнозувати, у яких районах найімовірніше буде скоєно злочин, що дозволяє правоохоронцям розміщувати патрулі більш ефективно.

Ще одним важливим кроком у цифровізації правоохоронної діяльності є використання дронів, камер спостереження та технологій розпізнавання облич.



Безпілотники активно застосовуються у моніторингу громадського порядку, розшуку зниклих осіб, контролі масових заходів та протидії нелегальній діяльності. Водночас розпізнавання облич дозволяє ідентифікувати злочинців за допомогою відеозаписів із камер спостереження та порівняння отриманих даних із наявними базами. Наприклад, у Великобританії та Китаї такі системи вже допомогли розкрити сотні злочинів та спростити процес ідентифікації підозрюваних.

Однак цифровізація правоохоронної діяльності не обмежується лише збором та аналізом відео- та фотоматеріалів. Автоматизовані системи контролю та цифрові бази даних дозволяють ефективніше зберігати, обробляти та передавати інформацію про правопорушників, розшукуваних осіб та кримінальні справи. Наприклад, в Європі діє Шенгенська інформаційна система (SIS), що об'єднує бази даних поліції, прикордонників та спецслужб країн ЄС, забезпечуючи швидку взаємодію між правоохоронними органами різних держав.

Поряд із цифровізацією судочинства та роботи правоохоронних органів значних змін зазнає й сектор юридичних послуг. LegalTech (юридичні технології) – це напрям, який охоплює використання програмного забезпечення та автоматизованих систем для спрощення та оптимізації юридичних процесів.

Одним із найперспективніших напрямів є використання AI у юридичних консультаціях. Алгоритми штучного інтелекту здатні аналізувати юридичні документи, надавати правові висновки та навіть готувати проекти договорів чи позовних заяв. Наприклад, такі платформи, як ROSS Intelligence або DoNotPay, дозволяють громадянам отримувати автоматизовані консультації без залучення адвокатів, що суттєво знижує витрати на юридичні послуги.

Ще одним важливим аспектом LegalTech є автоматизовані сервіси підготовки юридичних документів. Онлайн-платформи, такі як LegalZoom або Сію, допомагають користувачам швидко генерувати юридичні документи, заповнюючи стандартні шаблони на основі введених даних. Це особливо корисно для малого бізнесу та фізичних осіб, яким потрібен доступний і швидкий спосіб оформлення договорів, угод або заяв.

Не менш важливу роль відіграють дистанційні правові послуги та чат-боти, що надають консультації у режимі реального часу. Такі рішення використовуються як у комерційному секторі, так і в державних установах для полегшення доступу громадян до правової допомоги. Наприклад, у деяких країнах запроваджено чат-боти, які допомагають заповнювати податкові декларації, надавати інформацію про трудове законодавство чи оформлювати звернення до суду.

Практичне впровадження ІКТ у правозастосуванні відбувається стрімкими темпами, змінюючи судову систему, правоохоронну діяльність та юридичні послуги. Незважаючи на виклики, які постають перед цифровізацією,



потенційні переваги значно переважають ризики. Подальший розвиток електронного судочинства, розширення можливостей аналітичних систем для правоохоронців та LegalTech-сервісів сприятиме підвищенню ефективності та доступності правосуддя у цифрову епоху.

Інформаційно-комунікаційні технології (ІКТ) у правозастосуванні продовжують розвиватися, адаптуючи юридичну систему до сучасних викликів цифрової епохи. Однак для ефективної інтеграції новітніх технологій необхідно не лише вдосконалювати технічні рішення, а й створювати належну нормативно-правову базу, забезпечувати кібербезпеку, розвивати цифрову грамотність серед правозастосовців та поглиблювати міжнародну співпрацю.

Відзначимо, що під кібербезпекою слід розуміти забезпечення захисту від кіберзагроз і злочинності, зокрема за допомогою шифрування даних та застосування сучасних методів ідентифікації [15].

Синергія цих факторів стане запорукою ефективного правосуддя та правоохоронної діяльності в умовах глобальної цифровізації.

Цифровізація правозастосування вимагає гармонізації законодавства України з міжнародними стандартами, оскільки технології, що використовуються у сфері права, мають транскордонний характер. Зокрема, необхідно узгодити національні норми з Загальним регламентом про захист даних (GDPR) Європейського Союзу, який визначає принципи використання персональних даних, а також зі стандартами кібербезпеки, розробленими такими міжнародними організаціями, як Європол, ООН та Інтерпол. Це дозволить Україні не лише забезпечити захист прав громадян у цифровому середовищі, а й спростити співпрацю з іншими державами у сфері боротьби з кіберзлочинністю.

Окрім загальної адаптації законодавства до міжнародних норм, необхідним є впровадження спеціальних правових норм щодо електронного судочинства та штучного інтелекту. Використання автоматизованих систем у судочинстві має бути чітко регламентоване, зокрема щодо юридичної сили електронних доказів, можливості прийняття рішень алгоритмами та обмежень використання штучного інтелекту при винесенні судових ухвал. Також слід визначити правовий статус цифрових підписів та блокчейн-рішень у правовій системі, що дозволить закріпити їхню законність та придатність для судового використання.

Ще одним важливим аспектом є вдосконалення законодавства про кібербезпеку. У світі щороку зростає кількість кібератак на державні установи, зокрема й на судові системи та правоохоронні органи. Актуальним завданням є розробка ефективних механізмів захисту правових даних від маніпуляцій та несанкціонованого доступу, що включає використання шифрування, багаторівневого захисту доступу та моніторингу потенційних загроз у режимі реального часу.



Поряд із вдосконаленням нормативного регулювання перспективним напрямом є впровадження інноваційних технологій, що можуть змінити підходи до правозастосування в майбутньому. Однією з таких технологій є квантові системи шифрування, що забезпечують абсолютний захист правових даних від несанкціонованого доступу. Завдяки унікальним властивостям квантової криптографії навіть найпотужніші суперкомп'ютери не зможуть зламати зашифровану інформацію, що гарантує конфіденційність правових баз даних і судових матеріалів.

Ще однією інновацією, яка може суттєво змінити юридичну практику, є використання доповненої та віртуальної реальності у судових процесах. Завдяки технологіям VR (Virtual Reality) адвокати, прокурори та судді зможуть візуально відтворювати місце злочину, що дасть змогу більш детально аналізувати докази та приймати виважені рішення. Подібні технології вже тестуються у деяких країнах і демонструють значний потенціал у підвищенні ефективності кримінального судочинства.

Відзначимо, що під технологією VR слід розуміти використання віртуальної реальності для створення іммерсивних інтерактивних досвідів [15]. Іммерсивний інтерактивний досвід – це форма взаємодії, в якій людина повністю занурюється в штучне або змінене середовище, що створює ефект присутності та глибокого залучення.

Окрім цього, значного поширення набувають біометричні технології у правозастосуванні, зокрема системи розпізнавання облич та голосу, які допомагають у кримінальних розслідуваннях та спрощують процес ідентифікації особи в судових установах. Використання таких технологій підвищує рівень безпеки та дозволяє автоматизувати багато рутинних процесів у правоохоронних структурах.

Розвиток технологій неможливий без відповідного рівня компетентності серед фахівців, які працюють у сфері правозастосування. Тому важливим кроком є впровадження навчальних програм з ІКТ для юристів та правоохоронців. Вивчення принципів роботи електронного судочинства, механізмів кіберзахисту та алгоритмів штучного інтелекту має стати обов'язковою частиною професійної підготовки правників.

Юристам важливо вивчати криптографію, цифрову експертизу та автоматизоване правозастосування. Це дозволить юристам ефективніше використовувати цифрові інструменти у своїй роботі та краще розуміти їхні правові аспекти.

Не менш важливим є впровадження курсів цифрової безпеки, оскільки правозастосовці працюють із чутливою інформацією, що може стати ціллю для кібератак. Навчальні програми мають включати теми з управління ризиками, виявлення загроз та роботи з безпечними електронними платформами, що використовуються у судовій та правоохоронній практиці.



Оскільки кіберзлочинність та цифрове правосуддя мають глобальний характер, важливу роль у розвитку цієї сфери відіграє співпраця між країнами. Україна вже бере активну участь у міжнародних ініціативах у сфері кібербезпеки, однак подальше зміцнення спільних ініціатив із міжнародними організаціями, такими як Інтерпол, Європол та ООН, дозволить покращити механізми протидії кіберзлочинам та гармонізувати правові стандарти у сфері цифрового правозастосування.

Особливо важливим є створення глобальних стандартів цифрової юриспруденції, які встановлять єдині підходи до електронного судочинства, регулювання штучного інтелекту у правовій сфері та використання цифрових доказів у судових процесах.

Важливою складовою міжнародної співпраці є обмін найкращими практиками між державами, що дозволить запозичити успішні технологічні рішення та адаптувати їх до національного правового середовища.

Перспективи розвитку ІКТ у правозастосуванні визначаються сукупністю технологічних, правових та освітніх ініціатив. Гармонізація законодавства, запровадження новітніх цифрових технологій, підвищення рівня цифрової грамотності серед фахівців та розширення міжнародної співпраці сприятимуть створенню ефективною та безпечною системи цифрового правосуддя, здатної відповідати викликам сучасності.

**Висновки.** Інформаційно-комунікаційні технології стали невід'ємною частиною сучасного правозастосування, змінюючи підходи до правосуддя та правоохоронної діяльності. Цифровізація юридичних процесів підвищує ефективність, прозорість і доступність правосуддя, але супроводжується викликами у сфері нормативного регулювання, кібербезпеки та етики.

Ключові напрями цифровізації включають електронне судочинство, автоматизацію юридичних послуг, використання штучного інтелекту для аналізу судових рішень і блокчейн-технологій для захисту цифрових доказів. Big Data та Predictive Analytics допомагають прогнозувати злочинність і покращувати розслідування, а розвиток LegalTech забезпечує дистанційний доступ до юридичних послуг.

Водночас існують ризики. Недосконале законодавство створює правові прогалини, що можуть використовуватися зловмисниками. Використання штучного інтелекту викликає питання відповідальності за автоматизовані рішення та проблему алгоритмічної дискримінації.

Кібербезпека залишається пріоритетом. Використання електронних баз і судових реєстрів вимагає ефективного захисту, зокрема багаторівневої автентифікації, шифрування та моніторингу кіберзагроз.

Соціальні аспекти цифровізації також важливі. Цифровий розрив може обмежити доступ до правосуддя для вразливих груп, а недостатня цифрова



грамотність ускладнює впровадження технологій, що потребує навчальних програм.

Міжнародний досвід демонструє ефективні рішення, зокрема Predictive Policing та Інтернет-суди. Україна може використати цей досвід для розробки Єдиної судової інформаційної системи та цифрових правових платформ.

Перспективи цифровізації пов'язані з вдосконаленням законодавства, розвитком технологічної інфраструктури та цифрової грамотності. Важливо гармонізувати нормативну базу з міжнародними стандартами, зокрема GDPR і вимогами кібербезпеки.

Необхідно впроваджувати інноваційні технології, зокрема квантове шифрування, доповнену реальність у судових процесах, біометричні системи та штучний інтелект для правоохоронних органів.

Таким чином, цифровізація правозастосування має значний потенціал, але потребує збалансованого підходу, що поєднує технологічний розвиток, правове регулювання та міжнародну співпрацю. Інформаційно-комунікаційні технології повинні не лише підвищувати ефективність правосуддя, а й гарантувати дотримання прав громадян у цифровому суспільстві.

### *Література*

1. Берназюк О.О. Роль та місце цифрових технологій у сфері публічного управління. *Інформаційне право*. 2017. № 10. URL: <http://pgp-journal.kiev.ua/archive/2017/10/35.pdf>
2. Ведмідь П.В. Роль інформаційно-комунікаційних технологій у забезпеченні ефективності державного управління. *Публічне управління і адміністрування в Україні*. 2020. Вип. 18. С. 32-36.
3. Динник І.П. Сучасні інформаційно-комунікаційні технології та їх потенціал впливу на взаємодію держави і громадянського суспільства в умовах децентралізації. *Інвестиції: практика та досвід*. 2019. № 4. С. 152-157.
4. Єфанова Н.В. Аналіз нормативно-правового забезпечення у сфері інформаційно-комунікаційної інфраструктури в Україні. *Політичні та правові аспекти державного управління*. 2018. №1. С. 117-124.
5. Костюк П.П. Використання технології блокчейн для забезпечення інформаційної безпеки. *Сучасний захист інформації*. 2020. № 3(43). С. 22-28.
6. Куйбіда В.С., Карпенко О.В., Риженко О.В. Інформаційно-комунікативна діяльність органів публічної влади: монографія. Київ: ЦП Компринт. 2019. 358 с.
7. Маньгора В.В., Михальчук Ю.О. Використання цифрових технологій у праві: перспективи та виклики. *Інформація і право*. 2023. № 4(47). С. 147-158.
8. Романів Х.Б. Роль інформаційно-комунікаційних технологій у формуванні професійної правосвідомості студентів-юристів. *Інформація і право*. 2020. № 3(34). С. 110-118.
9. Сидоренко Т.М., Заболотна В.А. Застосування інформаційно-комунікаційних технологій у діяльності освітніх установ. *Економіка. Менеджмент. Бізнес*. 2023. № 1-2(41). С. 50-55.
10. Сучасні інформаційно-комунікаційні технології: навч. посіб. / Г.Г. Швачич та ін. Дніпро: НМетАУ, 2017. 230 с.
11. Хаванов А.В. Інформаційно-комунікаційні технології у боротьбі з корупцією та їх вплив на економічну безпеку. *Причорноморські економічні студії*. 2024. Вип. 87. С. 51-54.



12. Черніков Д.Ю. Інформаційно-комунікаційні технології як ефективний інструмент протидії корупції. *Молодий вчений*. 2018. № 11(63). С. 948-950.

13. Шматковська Т., Коробчук Т., Борисюк О. Сучасні інформаційно-комунікаційні технології в системі обліково-аналітичного забезпечення щодо моделювання бізнес-процесів. *Економіка та суспільство*. 2023. Вип. 53. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/2678/2593>.

14. Шмирова О.В., Зелінська В.А. Роль інформаційно-комунікаційних технологій на сучасному етапі інформатизації освіти. *Молодий вчений*. 2017. № 5(45). С. 455-458.

15. Чукурна О.П., Тардаскіна Т.М. Менеджмент в цифровій економіці: навч. посіб. Одеса: «Астропринт», 2024. 376 с.

### References:

1. Bernazyuk, O.O. (2017). Rol ta mistse tsyfrovyyh tekhnolohii u sferi publichnogo upravlinnia [The role and place of digital technologies in the field of public administration]. *Informatsiine pravo – Information Law*, 10. URL: <http://pgp-journal.kiev.ua/archive/2017/10/35.pdf> [In Ukrainian].

2. Vedmid, P.V. (2020). Rol informatsiino-komunikatsiinykh tekhnolohii u zabezpechenni efektyvnosti derzhavnoho upravlinnia [The role of information and communication technologies in ensuring the efficiency of public administration]. *Publichne upravlinnia i administruvannia v Ukraini – Public Administration and Governance in Ukraine*, 18, 32-36 [In Ukrainian].

3. Dynnyk, I.P. (2019). Suchasni informatsiino-komunikatsiini tekhnolohii ta ikh potentsial vplyvu na vzaємodiiu derzhavy i hromadianskoho suspilstva v umovakh detsentralizatsii [Modern information and communication technologies and their potential impact on the interaction between the state and civil society in the context of decentralization]. *Investytsii: praktyka ta dosvid – Investments: Practice and Experience*, 4, 152-157 [In Ukrainian].

4. Yefanova, N.V. (2018). Analiz normatyvno-pravovoho zabezpechennia u sferi informatsiino-komunikatsiinoi infrastruktury v Ukraini [Analysis of regulatory and legal support in the field of information and communication infrastructure in Ukraine]. *Politychni ta pravovi aspekty derzhavnoho upravlinnia – Political and Legal Aspects of Public Administration*, 1, 117-124 [In Ukrainian].

5. Kostiuk, P.P. (2020). Vykorystannia tekhnolohii blockchain dlia zabezpechennia informatsiinoi bezpeky [The use of blockchain technology to ensure information security]. *Suchasnyi zakhyst informatsii – Modern Information Security*, 3(43), 22-28 [In Ukrainian].

6. Kuibida, V.S., Karpenko, O.V., Ryzhenko, O.V. (2019). *Informatsiino-komunikatyvna diialnist orhaniv publichnoi vlady: monohrafiia [Information and communication activities of public authorities]*. Kyiv: TsP Komprynt [In Ukrainian].

7. Manhora, V.V., Mykhalchuk, Yu.O. (2023). Vykorystannia tsyfrovyykh tekhnolohii u pravi: perspektyvy ta vyklyky [The use of digital technologies in law: Prospects and challenges]. *Informatsiia i pravo – Information and Law*, 4(47), 147-158 [In Ukrainian].

8. Romaniv, Kh.B. (2020). Rol informatsiino-komunikatsiinykh tekhnolohii u formuvanni profesiinoi pravosvidomosti studentiv-yurystiv [The role of information and communication technologies in forming the professional legal awareness of law students]. *Informatsiia i pravo – Information and Law*, 3(34), 110-118 [In Ukrainian].

9. Sydorenko, T.M., Zabolotna, V.A. (2023). Zastosuvannia informatsiino-komunikatsiinykh tekhnolohii u diialnosti osvितnikh ustanov [The application of information and communication technologies in the activities of educational institutions]. *Ekonomika. Menedzhment. Biznes – Economics. Management. Business*, 1-2(41), 50-55 [In Ukrainian].

10. Shvachych, H.H. et al. (2017). *Suchasni informatsiino-komunikatsiini tekhnolohii: navch. posib. [Modern Information and Communication Technologies]*. Dnipro: NMetAU [In Ukrainian].



11. Khavanov, A.V. (2024). Informatsiino-komunikatsiini tekhnolohii u borotbi z koruptsiieiu ta ikh vplyv na ekonomichnu bezpeku [Information and communication technologies in the fight against corruption and their impact on economic security]. *Prychornomorski ekonomichni studii – Black Sea Economic Studies*, 87, 51-54 [In Ukrainian].

12. Chernikov, D.Yu. (2018). Informatsiino-komunikatsiini tekhnolohii yak efektyvnyi instrument protydii koruptsii [Information and communication technologies as an effective tool for combating corruption]. *Molodyi vchenyi – Young Scientist*, 11(63), 948-950 [In Ukrainian].

13. Shmatkovska, T., Korobchuk, T., Borysiuk, O. (2023). Suchasni informatsiino-komunikatsiini tekhnolohii v systemi oblikovo-analitychnoho zabezpechennia shchodo modeliuvannia biznes-protseviv [Modern information and communication technologies in the accounting and analytical support system for business process modeling]. *Ekonomika ta suspilstvo – Economy and Society*, 53. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/2678/2593>[In Ukrainian].

14. Shmyrova, O.V., Zelinska, V.A. (2017). Rol informatsiino-komunikatsiinykh tekhnolohii na suchasnomu etapi informatyzatsii osvity [The role of information and communication technologies at the present stage of education informatization]. *Molodyi vchenyi – Young Scientist*, 5(45), 455-458 [In Ukrainian].

15. Chukurna, O.P., Tardaskina, T.M. (2024). *Menedzhment v tsyfrovii ekonomitsi: navch. posib.* [Management in the Digital Economy]. Odesa: Astroprynt [In Ukrainian].