УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2025-1/146

ЦИФРОВА ЕРА КРИМІНАЛЬНОГО ПРОЦЕСУ: МОЖЛИВОСТІ ІТ-СИСТЕМ У ДОСУДОВОМУ РОЗСЛІДУВАННІ

THE DIGITAL ERA OF THE CRIMINAL PROCESS: OPPORTUNITIES OF IT SYSTEMS IN PRE-TRIAL INVESTIGATION

Шаблистий В.В., д.ю.н., професор,
директор
Навчально-науковий інститут права та інноваційної освіти
Дніпровського державного університету внутрішніх справ,
ORCID ID: 0000-0003-0210-1772

У статті констатовано, що сучасний кримінальний процес перебуває під значним впливом ІТ- системи, що зумовлює трансформацію його ключових стадій, зокрема досудового розслідування. Ця стадія, як одна з центральних у кримінальному провадженні, дедалі активніше інтегрує цифрові інструменти для збору, обробки й аналізу доказової бази. Застосування ІТ-систем сприяє підвищенню ефективності слідчих дій, прискорює ідентифікацію підозрюваних і дозволяє автоматизувати рутинні процедури. Водночас впровадження таких технологій супроводжується низкою викликів, пов'язаних із недостатньою законодавчою регламентацією, захистом персональних даних, забезпеченням кібербезпеки та обмеженим рівнем цифрової компетентності працівників правоохоронних органів, що ускладнює адаптацію кримінального процесу до інноваційних реалій.

У статті розглянуто процес цифровізації досудового розслідування в Україні, зокрема впровадження інформаційно-телекомунікаційних систем у кримінальний процес. Проаналізовано правові аспекти використання ІТ-технологій у слідчих діях, їхній вплив на ефективність кримінального провадження та можливі ризики, зокрема проблеми нормативної регламентації, захисту персональних даних і кібербезпеки. Окрему увагу приділено питанням визнання електронних доказів, їхньої допустимості та необхідності вдосконалення кримінального процесуального законодавства. Визначено перспективи застосування штучного інтелекту, аналізу великих даних і блокчейн-технологій у кримінальному процесі. Також акцентовано на міжнародних аспектах цифрового правосуддя, необхідності гармонізації українського законодавства з міжнародними стандартами та інтеграції вітчизняних інформаційних систем із глобальними базами даних для ефективної боротьби з кіберзлочинністю.

Доведено, що цифровізація кримінального провадження є невідворотним процесом, що потребує комплексного підходу, включаючи законодавчі зміни, технічні удосконалення та розвиток спеціалізованих підрозділів цифрової криміналістики. Вирішення цих завдань сприятиме підвищенню ефективності кримінального судочинства та забезпеченню належного рівня правового захисту в умовах сучасних викликів.

Ключові слова: кримінальний процес, досудове розслідування, цифровізація, електронні докази, ІТ-системи, кібербезпека, кримінальне судочинство, штучний інтелект.

The article states that the modern criminal process is under the significant influence of the IT system, which causes the transformation of its key stages, in particular the pre-trial investigation. This stage, as one of the central ones in criminal proceedings, is increasingly integrating digital tools for collecting, processing and analyzing evidence. The use of IT systems helps to increase the efficiency of investigative actions, accelerates the identification of suspects and allows for the automation of routine procedures. At the same time, the implementation of such technologies is accompanied by a number of challenges associated with insufficient legislative regulation, personal data protection, ensuring cybersecurity and a limited level of digital competence of law enforcement officers, which complicates the adaptation of the criminal process to innovative realities.

The article examines the process of digitalization of pre-trial investigation in Ukraine, particularly the implementation of information and telecommunication systems in criminal proceedings. The legal aspects of using IT technologies in investigative actions, their impact on the efficiency of criminal proceedings, and potential risks, including regulatory issues, personal data protection, and cybersecurity, are analyzed. Special attention is given to the recognition of electronic evidence, its admissibility, and the need to improve criminal procedural legislation. The prospects of applying artificial intelligence, big data analysis, and blockchain technologies in criminal proceedings are identified. The article also highlights the international aspects of digital justice, the necessity of harmonizing Ukrainian legislation with international standards, and the integration of national information systems with global databases for effective counteraction to cybercrime.

It has been proven that the digitalization of criminal proceedings is an inevitable process that requires a comprehensive approach, including legislative changes, technical improvements, and the development of specialized digital forensics units. Solving these tasks will contribute to increasing the efficiency of criminal justice and ensuring an adequate level of legal protection in the face of modern challenges.

Key words: criminal process, pre-trial investigation, digitalization, electronic evidence, IT systems, cybersecurity, criminal justice, artificial intelligence.

Постановка проблеми. Сучасний кримінальний процес перебуває під значним впливом інформаційно-телекомунікаційних технологій (далі – ІТ- системи), що зумовлює трансформацію його ключових стадій, зокрема досудового розслідування. Ця стадія, як одна з центральних у кримінальному провадженні, дедалі активніше інтегрує цифрові інструменти для збору, обробки й аналізу доказової бази. Застосування ІТ-систем сприяє підвищенню ефективності слідчих дій, прискорює ідентифікацію підозрюваних і дозволяє автоматизувати рутинні процедури. Водночас впровадження таких технологій супроводжується низкою викликів, пов'язаних із недостатньою законодавчою регламентацією, захистом персональних даних, забезпеченням кібербезпеки та обмеженим рівнем цифрової компетентності працівників правоохоронних органів, що ускладнює адаптацію кримінального процесу до інноваційних реалій.

Перспективні технології, такі як штучний інтелект, аналіз великих даних (Big Data) і блокчейн, відкривають нові можливості для розслідування кримінальних правопорушень, зокрема через підвищення точності аналізу та забезпечення прозорості даних. Проте їхнє використання в правовому полі потребує чіткого визначення процесуального статусу електронних доказів, а також розробки механізмів їхньої верифікації та захисту від маніпуляцій чи фальсифікації. Зростання кіберзлочинності додатково актуалізує необхідність адаптації правоохоронних структур до нових загроз шляхом удосконалення діяльності спеціалізованих підрозділів із цифрової криміналістики.

Ще одним важливим аспектом є проблема міждержавної взаємодії у сфері обміну цифровими доказами. Інтеграція національних інформаційних систем із міжнародними базами даних має потенціал значно підвищити ефективність розслідування транскордонних злочинів.

Однак відсутність належної координації між правоохоронними органами різних держав і розбіжності в нормативному регулюванні ускладнюють оперативний доступ до необхідної інформації. Це підкреслює потребу в гармонізації законодавчих норм і розробці єдиних міжнародних стандартів для використання ІТ-систем у кримінальному процесі.

Таким чином, цифровізація досудового розслідування є об'єктивним і невідворотним процесом, що вимагає системного підходу до вирішення пов'язаних із нею проблем. Для забезпечення ефективного, прозорого та справедливого кримінального судочинства необхідно вдосконалити нормативно-правову базу, підвищити професійну кваліфікацію слідчих у сфері цифрових технологій і розвинути відповідну технічну інфраструктуру. Лише за умови комплексного та збалансованого впровадження ІТ-систем можна досягти якісного прогресу в цій галузі.

Аналіз останніх досліджень. Останні дослідження у сфері використання інформаційно-телекомунікаційних технологій у кримінальному процесі демонструють їхню значну роль у підвищенні ефективності досудового розслідування. Науковці звертають увагу на проблеми правового регулювання цифрових доказів, питання кібербезпеки та можливості застосування штучного інтелекту у галузі кримінального судочинства. Зокрема, важливий внесок у розвиток цієї тематики зробили такі дослідники, як Бондар В.С., Гавловський В.Д., Гуцалюк М.В., Дабіжа Д.В., Кисельов А.О., Круль С.М., Лишак О.А., Орлов Ю.Ю., Тетерятник Г.К., Федчак І.А., Хахановський В.Г., Чернявський С.С., які у своїх працях розглядали питання діджиталізації, електронного судочинства та автоматизації слідчих дій.

Метою написання статті є аналіз можливостей ІТ-систем у досудовому розслідуванні та оцінка їхнього впливу на ефективність кримінального процесу.

Виклад основного матеріалу. Останні роки в Україні характеризуються активним упровадженням інформаційних і цифрових технологій, що в сучасному контексті отримали назву «діджиталізація», у повсякденне життя суспільства з метою його вдосконалення та прогресивного розвитку.

Відповідно до світових тенденцій і спираючись на досвід міжнародних партнерів, у червні 2021 року Верховна Рада України ухвалила Закон України № 1498-IX «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування» (далі – Законом України № 1498-IX) [1].

Як випливає з назви цього законодавчого акта, його прийняття ознаменувало початок створення в Україні новаторської ІТ-системи досудового розслідування, яка офіційно запрацювала з 15 грудня 2021 року.

Згідно з положеннями закону та частиною 1 статті 106-1 Кримінального процесуального кодексу України (далі – КПК України), зазначена система призначена для створення, накопичення, зберігання, пошуку, обробки та передачі матеріалів і відомостей у межах кримінального провадження [2]. Іншими словами, усі матеріали кримінальних проваджень, внесених до Єдиного реєстру досудових розслідувань після 15 грудня 2021 року, формуються та ведуться в електронному вигляді, а не на паперових носіях.

Безумовно, таке нововведення має позитивну мету – зменшення обсягу паперової роботи для правоохоронних органів, яка в сучасних умовах є надмірно трудомісткою та не завжди виправданою через значні затрати часу й ресурсів.

За даними статистики, оприлюдненими на офіційному сайті Офісу Генерального прокурора, у грудні 2024 року в Україні було зареєстровано 492 479 кримінальних проваджень [3]. При цьому середній обсяг одного провадження становить щонайменше 1000 сторінок, що є доволі значним показником.

Спільним наказом Тимчасово виконуючого повноваження Директора Національного антикорупційного бюро України, Генерального прокурора, Голови Ради суддів України та Голови Вищого антикорупційного суду від 15 грудня 2021 року № 175/390/57/72 було затверджено положення про систему «іКейс». Принагідно зауважити, що функціонування ІТ-системи досудового розслідування «іКейс», сприяє значній автоматизації процесів досудового розслідування в цілому, а також окремих процедур, що стосуються організаційних, управлінських, аналітичних, інформаційно-телекомунікаційних та інших потреб користувачів системи [4]. Це, зокрема, полегшило доступ сторони захисту до матеріалів кримінального провадження відповідно до статті 221 КПК України, а також дозволить слідчому судді оперативно розглядати клопотання та скарги сторін провадження на етапі досудового розслідування в розумні строки, без необхідності фізичного витребування матеріалів від органу досудового розслідування чи прокуратури, що суттєво економить час [2].

Крім того, Законом України № 1498-IX передбачено, що Офіс Генерального прокурора, орган, до складу якого входить орган досудового розслідування, а також орган, відповідальний за затвердження положення про систему, що діє в судах, зобов'язані протягом шести місяців із дня набрання законом чинності розробити та затвердити положення про ІТ-систему досудового розслідування [1].

Проте, варто звернути увагу на зауваження представників правозахисної спільноти України, які висловлюють занепокоєння щодо відсутності чіткого порядку залучення адвокатів як учасників кримінального процесу до роботи з системою «іКейс» під час виконання ними своїх процесуальних обов'язків [5, с. 461].

Також необхідно відзначити окремі процесуальні порушення, пов'язані з нововведеннями, які допускаються деякими слідчими [6, с. 375]. Зокрема, відповідно до абзацу 2 частини 3 статті 290 КПК України, на стадії надання доступу до матеріалів кримінального провадження іншій стороні окремі слідчі вдаються до імітації цього процесу в електронному форматі (наприклад, надсилаючи скан-копії на електронну пошту адвоката або копіюючи їх на USB-накопичувачі) [2]. При цьому слідчий звітує про ознайомлення сторони з матеріалами та вимагає письмового підтвердження цього факту відповідно до частини 9 статті 290 КПК України, чим порушує право сторони на доступ до фізичних оригіналів матеріалів справи.

Вбачається, що надання електронних копій матеріалів кримінального провадження слідчими будь-якого органу досудового розслідування (за винятком Національного антикорупційного бюро України) слід розглядати лише як надання копій, а не як повноцінне відкриття матеріалів у розумінні статті 290 КПК України, яка передбачає доступ саме до оригінальних документів [2].

Запровадження нових інформаційних технологій і технічних рішень у різні сфери життя є неминучим процесом і може вважатися беззаперечним кроком уперед. Проте, як і в разі будь-яких інновацій, до їх інтеграції необхідно підходити з максимальною відповідальністю, щоб уникнути руйнування вже наявних механізмів і запобігти можливим зловживанням із боку тих, хто ці технології застосовуватиме [7].

Водночас у кримінальному процесуальному законодавстві України відсутнє чітке визначення електронних доказів як самостійної категорії. Законодавець обмежується загальним визначенням доказів, відповідно до якого це фактичні дані, отримані у передбаченому КПК України порядку, на підставі яких встановлюються обставини, що мають значення для кримінального провадження. При цьому процесуальними джерелами доказів згідно з части-

ною 2 статті 84 КПК України є показання, речові докази, документи та висновки експертів [2]. Отже, електронні докази формально не виділені як окремий вид, що створює певні труднощі у їхньому використанні.

Дослідники, зокрема Орлов Ю.Ю. та Чернявський С.С., пропонують законодавчо закріпити поняття електронних доказів як самостійного джерела доказової інформації. Вони визначають електронні відображення як цілісну систему відомостей або комп'ютерних інструкцій в інформаційній мережі чи на технічному носії, що можуть бути використані для встановлення фактів у кримінальному провадженні [8]. Подібний підхід підтримується і на міжнародному рівні. Так, Рада Європи визначає електронні докази як будь-які докази, отримані з даних, що містяться на цифрових пристроях або вироблені ними, функціонування яких залежить від програмного забезпечення та комп'ютерних мереж.

Електронні докази мають низку специфічних особливостей, що відрізняють їх від традиційних джерел доказової інформації. Вони невидимі неозброєним оком, а їх вилучення часто потребує спеціальних технічних засобів і залучення фахівців. Крім того, електронні докази є нестійкими, оскільки можуть бути змінені або втрачені через технічні фактори, такі як перезапис даних, розрядка пристрою чи фізичне пошкодження носія. Водночас вони можуть копіюватися без втрати якості, що створює як переваги у збереженні та передачі, так і ризики підробки, через що важливо забезпечувати їхню автентичність. Окрему роль відіграє їх походження: електронні докази можуть бути створені людиною (наприклад, електронні листи, повідомлення) або автоматично згенеровані системами (логи серверів, дані про з'єднання тощо). Крім того, вони не прив'язані до матеріального носія, можуть вільно переміщуватися у цифровому середовищі, що ускладнює їхню фіксацію та збереження. Саме тому процес збирання, перевірки й оцінки електронних доказів вимагає залучення спеціалістів та застосування методів цифрової криміналістики, адже без належної процедури їх належності може бути поставлена під сумнів, що здатне суттєво вплинути на судовий розгляд і результати кримінального провадження.

Ключовою проблемою використання електронних доказів у кримінальному процесі є забезпечення їхньої належність та допустимості. Для цього необхідно дотримуватись низки принципів, серед яких законність збору інформації, цілісність отриманих даних, належне документування всіх процесуальних дій із цифровими носіями, залучення відповідних експертів та спеціалістів [9]. Важливим аспектом є використання технологій захисту даних, зокрема цифрових підписів та криптографічних механізмів, які можуть підтверджувати автентичність електронних доказів [10, с. 22-23].

Проте для ефективного використання електронних доказів у правовій сфері необхідно чітко визначити їхній процесуальний статус, а також розробити надійні механізми верифікації та захисту від підробки чи маніпуляцій. Важливо запровадити уніфіковані стандарти збору, аналізу та оцінки таких доказів, що гарантуватиме їхню допустимість, допустимість і належність у судових процесах [11, с. 164]. Крім того, варто вдосконалити законодавчі норми, які регулюють відповідальність за фальсифікацію або незаконне використання електронних доказів, оскільки правова невизначеність може спричинити зловживання. Зростання кіберзлочинності ще більше підкреслює потребу в адаптації правоохоронних органів до нових викликів, зокрема шляхом удосконалення діяльності спеціалізованих підрозділів із цифрової криміналістики.

Слід констатувати, що проблема міждержавної взаємодії у сфері обміну цифровими доказами залишається одним із ключових викликів сучасного кримінального процесу. Інтеграція національних інформаційних систем із міжнародними базами даних здатна значно підвищити ефективність розслідування транскордонних злочинів, проте її реалізація ускладнена відсутністю єдиних механізмів координації між правоохоронними органами різних країн та розбіжностями в нормативно-правовому регулюванні. Це обумовлює необхідність гармонізації законодавчих норм і розробки універсальних міжнародних стандартів використання цифрових технологій у кримінальному судочинстві. Водночас актуальним залишається питання науково-технічного вдосконалення процесів верифікації цифрових доказів, розробки надійних алгоритмів захищеного обміну інформацією та створення ефективних методів автоматизованого аналізу великих обсягів даних для ідентифікації цифрових слідів злочинної діяльності [12]. Подальші дослідження у цих напрямах є критично важливими для підвищення рівня безпеки та ефективності міжнародного співробітництва у сфері боротьби з кіберзлочинністю.

Висновок. Запровадження ІТ-системи досудового розслідування в Україні є важливим кроком на шляху цифрової трансформації кримінального процесу. Використання системи «іКейс» сприяє підвищенню ефективності роботи слідчих органів, оптимізації процесу обробки кримінальних проваджень і забезпеченню оперативного доступу до матеріалів справи. Однак впровадження таких інновацій супроводжується певними викликами, зокрема відсутністю чіткої правової регламентації статусу електронних доказів, процедур їх збирання та використання, а також ризиками фальсифікації та маніпуляцій.

Необхідно вдосконалити кримінальне процесуальне законодавство, закріпивши електронні докази як окрему категорію доказової бази та розробивши стандартизовані механізми їх перевірки та верифікації. Важливим напрямом подальшого розвитку є також забезпечення захисту електронних даних, створення ефективних алгоритмів боротьби з кіберзлочинністю та інтеграція національних цифрових систем із міжнародними базами даних.

Таким чином, цифровізація кримінального провадження є невідворотним процесом, що потребує комплексного підходу, включаючи законодавчі зміни, технічні удосконалення та розвиток спеціалізованих підрозділів цифрової криміналістики. Вирішення цих завдань сприятиме підвищенню ефективності кримінального судочинства та забезпеченню належного рівня правового захисту в умовах сучасних викликів.

ЛІТЕРАТУРА:

1. Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування : Закон України від 1 червня 2021 року № 1498-IX. *Відомості Верховної Ради України* (ВВР). 2021. № 31. Ст. 253. URL: https://zakon.rada.gov.ua/laws/show/1498- 20#Text

2. Кримінальний процесуальний кодекс України: Закон України від 12.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/go/4651-17

3. Офіс Генерального прокурора. Офіційний веб-сайт. URL: https://www.gp.gov.ua/

4. Про інформаційно-телекомунікаційну систему досудового розслідування «іКейс: Наказ Національного антикорупційного бюро України, Офісу Генерального прокурора, Вищого антикорупційного суду, Ради суддів України від 15.12.2021 № 175/390/57/72.

5. Черниченко І.В., Маслюк О.В. Переваги застосування «іКейс» у кримінальному провадженні України. *Юридичний науковий електронний журнал*. 2024. № 7. С. 460-462.

6. Демура М. До питання про цифрову трансформацію кримінального провадження в умовах воєнного стану. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2022. Спеціальний випуск № 2 (121). С. 374-381

7. Навчальний посібник для підготовки до державного екзамену з дисциплін «Кримінальний процес», «Криміналістика» / В. В. Шаблистий, А. Ф. Волобуєв, Г. Л. Д'яковський та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 332 с.

8. Орлов Ю.Ю., Чернявський С.С. Електронне відображення як джерело доказів у кримінальному провадженні. *Юридичний часопис Національної академії внутрішніх справ.* 2017. № 1(13). С. 12–24.

9. Солдатенко О. А. Трансформація кримінального процесу в епоху цифрових технологій: виклики та перспективи. Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності : матер. Міжнар. наук.-практ. конф. (м. Дніпро, 08 грудня 2023 р.). Дніпро : ДДУВС, 2024. С. 269-272

10. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації / Авт. колектив: А.В. Захарко, А.Г. Гаркуша, В.В. Рогальська, І.В. Краснобрижий, О.В. Брягін. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. 73 с.

11. Шиян А.Г. Процесуальні джерела доказів у кримінальному провадженні: новели кримінального процесуального законодавства України. Актуальні проблеми експертного забезпечення досудового розслідування: матеріали наук.-практ. семінару (м. Дніпро, 29 травня 2020 р.). Дніпро: ДДУВС, 2020. С. 163-166

12. Запобігання комп'ютерним кримінальним правопорушенням : наук.-практ. посібник / С. В. Бабанін. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 80 с.