*УДК 343.14*
*DOI https://doi.org/10.24144/2788-6018.2024.05.125*

# ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В КРИМІНАЛЬНОМУ ПРОЦЕСІ ЗАРУБІЖНИХ КРАЇН

**Ніколенко Л.М.,**
*доктор юридичних наук, професор,*
*провідний науковий співробітник*
*науково-дослідної лабораторії публічної безпеки громади*
*факультету № 2,*
*Донецький державний університет внутрішніх справ,*
*ORCID: 0000-0002-3437-6968*

**Ніколенко Л.М. Використання електронних доказів в кримінальному процесі зарубіжних країн.**

В статті проаналізовано особливості використання електронних доказів в кримінальному процесі зарубіжних країн. Підкреслено, що на теперішній час електронні докази стали незамінними для кримінальних розслідувань і судових процесів у всьому світі. Наголошено на важливості правового регулювання кримінально-процесуальної форми цифрових технологій. Неналежний характер такого регулювання тягне за собою певні правові наслідки, в тому числі визнання електронних доказів неналежними або недопустимими.

Проаналізовано досвід деяких зарубіжних країн в сфері визнання та використання електронних доказів (США, Великої Британії, Китайської Народної Республіки та країн Європейського Союзу). Доведено, що кожна держава будує власний шлях та підхід до включення таких доказів у свої правові системи залежно від правових традицій, технологічної інфраструктури та міркувань конфіденційності.

З аналізу процесуальних кодексів відзначено, що процесуальна наука розробляє теорію щодо електронних доказів за галузевим принципом. Підкреслено, що в їх основі знаходяться загальні цифрові технології, тому це надає можливість вироблення єдиних міжгалузевих правил використання електронних доказів у будь-якому процесі.

Визначено, що в англосаксонській правовій системі відсутнє чітке розмежування доказів на види. Доказове право будується на типових проблемних ситуаціях.

Проаналізовано законодавство США, яке регулює використання електронних доказів у кримінальному процесі. Зазначено, що умовою їх прийняття є його автентичність та релевантність справі.

Зазначено, що у Великій Британії на всі електронні докази поширюються ті самі правила та закони, що застосовуються до документальних доказів.

Проаналізовано законодавство Європейського Союзу, яке регулює електронні докази та дозволяє посилити співпрацю між державами-членами в сфері використання електронних доказів.

Підкреслено, що держави продовжують адаптуватися до епохи цифрових технологій, розробка надійної правової бази та міжнародної співпраці будуть мати важливе значення для забезпечення ефективного та справедливого використання електронних доказів у прагненні до справедливості.

**Ключові слова:** електронні докази, поліція, кримінальний процес, Інтерпол, цифрова інформація, міжнародний досвід.

**Nikolenko L. The use of electronic evidence in the criminal process of foreign countries.**

It is emphasized that electronic evidence has become indispensable for criminal investigations and trials around the world. The importance of legal regulation of the criminal procedural form of digital technologies is emphasized. The improper nature of such regulation entails certain legal consequences, including the recognition of electronic evidence as improper or inadmissible.

The experience of some foreign countries in the field of recognition and use of electronic evidence (the USA, Great Britain, the People's Republic of China and the countries of the European Union) is analyzed. It has been proven that each state builds its own way and approach to incorporating such evidence into its legal systems depending on legal traditions, technological infrastructure and privacy considerations.

From the analysis of procedural codes, it was noted that procedural science develops a theory of electronic evidence according to the industry principle. It is emphasized that they are based on common digital technologies, therefore this provides an opportunity to develop uniform cross-

industry rules for the use of electronic evidence in any process.

It was determined that in the Anglo-Saxon legal system there is no clear division of evidence into types. Evidence law is based on typical problem situations.

The US legislation, which regulates the use of electronic evidence in the criminal process, is analyzed. It is noted that the condition for their acceptance is its authenticity and relevance to the case.

It is noted that in the UK, all electronic evidence is subject to the same rules and laws that apply to documentary evidence.

The legislation of the European Union, which regulates electronic evidence and allows to strengthen cooperation between member states in the field of using electronic evidence, is analyzed.

It is emphasized that as states continue to adapt to the age of digital technologies, the development of a reliable legal framework and international cooperation will be essential to ensure the effective and fair use of electronic evidence in the pursuit of justice.

**Key words:** electronic evidence, police, criminal process, Interpol, digital information, international experience.

**Постановка проблеми.** Розвиток цифрової ери змінив майже всі аспекти суспільного життя. Безумовно, дана тенденція впливає і на таку сферу суспільства та держави, як судочинство, причому, як на національному, так і на міжнародному рівні, проявляючи себе у вигляді досить широкого використання електронних доказів у кримінальному процесі. Розповсюдження електронних пристроїв та Інтернету запровадило величезну кількість нових джерел доказів, починаючи від електронних листів і публікацій у соціальних мережах до даних, що зберігаються в хмарних сховищах.

Цифрова трансформація суспільства, зростання кіберзлочинів та, як слідство, збільшення доказового значення цифрових слідів злочинів, актуалізує необхідність використання електронних доказів у діяльності правоохоронних органів.

Так, експерти «Cybersecurity Ventures» стверджують, що у 2024 році збитки від кіберзлочинності сягнуть 9,5 трильйонів доларів США, тоді як наступного року ця цифра може збільшитися до 10,5 трильйонів доларів США [1].

Електронні докази стали незамінними для кримінальних розслідувань і судових процесів у всьому світі. Важливість правового регулювання кримінально-процесуальної форми цифрових технологій не можна недооцінювати. Неналежний характер такого регулювання тягне за собою певні правові наслідки, в тому числі визнання електронних доказів неналежними або недопустимими.

Кожна держава будує власний шлях та підхід до включення таких доказів у свої правові системи залежно від правових традицій, технологічної інфраструктури та міркувань конфіденційності.

У 2017 році до Цивільного процесуального кодексу України, Господарського процесуального кодексу України та Кодексу адміністративного судочинства України були здійснено зміни щодо включення електронних доказів до засобів доказування. Аналогічних змін до Кримінального процесуального кодексу України (далі – КПК України) здійснено не було, що спричиняє неоднакове тлумачення електронних доказів як на досудовому, так і на судовому етапі кримінального провадження.

У зв'язку з цим, підвищений інтерес викликає зарубіжний досвід, де на законодавчому рівні закріплено можливість використання електронних доказів у кримінальному процесі. Тому дана проблематика потребує негайного дослідження та аналізування.

**Стан дослідження.** Питання електронних доказів у кримінальному процесі досліджували: В.В. Вапнярчук, Ю.М. Грошевий, М.В. Гуцалюк, І.Г. Каланча, А.В. Коваленко, О.П. Метелев, В.В. Мурадов, Ю.Ю. Орлов, В.С. Петренко, А.В. Ратнова, А.В. Скрипник, А.В. Столітній, С.С. Чернявський, О.Г. Шило та інші поважні вчені. Поряд з цим, із врахуванням динаміки розвитку електронних технологій питання електронних доказів в кримінальному процесі потребує подальшого дослідження, що свідчить про актуальність даної статті.

**Метою статті** є наукове осмислення використання електронних доказів у кримінальному процесі, вивчення зарубіжного досвіду, а також останніх законодавчих інновацій щодо електронних доказів.

**Виклад основного матеріалу.** КПК України не містить особливого порядку використання електронних доказів. Тим часом, основний порядок доказування був сформований більш ніж півстоліття тому і зорієнтований на отримання традиційних засобів доказування. Отже, в умовах використання як засобів доказування електронних слідів і способів відображення юридично значущої інформації, що міститься в них, настільки специфічні, що традиційні процесуальні форми доказування в сучасних умовах вже не актуальні та застаріли. З аналізу процесуальних кодексів слід відзначити, що процесуальна наука розробляє теорію щодо електронних доказів за галузевим принципом. Це можна пояснити тим, що деякі електронні докази з'являються у кримінальному процесі пізніше, ніж у господарському або цивільному. Але ж в їх основі зна-

ходяться загальні цифрові технології, тому це надає можливість вироблення єдиних міжгалузевих правил використання електронних доказів у будь-якому процесі. Деякі зарубіжні країни використовують саме такій підхід.

В англосаксонській правовій системі відсутнє чітке розмежування доказів на види. Доказове право будується на типових проблемних ситуаціях. Доказове право США, по суті, є закріпленням найважливіших та знакових судових рішень, узагальненою практикою і носить заборонний характер, тобто вказує, в яких випадках доказ не може бути визнаним допустимим. Тому для американських юристів немає істотного значення чи є електронні докази самостійним видом доказів [2, с. 2].

Федеральні правила про докази (Federal Rules of Evidence), прийняті в 1975 році, вважаються основним нормативним актом щодо регулювання доказів у США. У ст. 401 Федеральних правил про докази відзначається, що належними визнаються докази, які в будь-якому вигляді здатні зробити наявність будь-якого факту, який вплине на кваліфікацію вчиненого, більш вірогідним або менш вірогідним, ніж за відсутності цих доказів. Стаття 402 Федеральних правил про докази тлумачить цифрові докази (digital evidence) як дані (data) та носій, на якому зберігаються дані (media storing the data) [3]. Таке широке визначення поняття доказів вже давно дозволило у кримінальному процесі США застосувати електронні докази.

Перед прийняттям електронного доказу судом учасник процесу має довести його автентичність за допомогою стандартної процедури автентифікації електронного документу або сторона має надати опис процесу створення або систему, яка використовується для одержання результату, та продемонструвати, що система або процес дають точний результат [4].

Електронні докази повинні бути релевантними справі, а саме: вони надають будь-яку можливість зробити факт більш або менш вірогідним, ніж це було б без доказів; факт має значення при вирішенні позову; докази є прийнятними, якщо вони не визнані неприйнятними відповідно до Конституції Сполучених Штатів, федерального закону, інших федеральних правил доказів або правил встановлених Верховним судом США [3].

Законодавче регулювання електронних доказів у Великій Британії регламентується Законом про поліцію та кримінальні докази 1984 р. Згідно ст. 19 вказаного Закону поліція може витребувати будь-яку інформацію, в тому числі в електронній формі. Головна умова полягає в тому, щоб електронна доказова інформація мала відношення до скоєння або запобігання злочинам, а також коли її вилучення сприяє запобіганню приховування, втрати, підробки або знищення доказів у будь-якій формі [5].

На всі цифрові докази поширюються ті самі правила та закони, що застосовуються до документальних доказів [6]. Крім того, це питання регулюється також Статутом про використання комп'ютера із протиправною метою (Computer Misuse Act), який містить кримінально-правові норми щодо комп'ютерних злочинів та інших, які вчиняються з використанням комп'ютера як знаряддя злочину, кримінально-процесуальні положення обшуку, вилучення електронних доказів, повноваження правоохоронних органів [7]. Взагалі у Великій Британії не виділяється такого окремого виду доказів як електронні докази, а йдеться лише про процедури та правила подання електронних документів.

Романо-германська система права розуміє електронні докази як інформацію, створену, збережену чи передану у цифровому вигляді, що дозволяє спростувати факт, що оскаржується під час судового розгляду, свідчить про найефективніше використання їх під час провадження у кримінальних справах [8].

На рівні Європейського Союзу (далі – ЄС) для використання електронних доказів у кримінальному процесі було вироблено стандарти, які впроваджують держави-члени. У своєму звіті Європейська Комісія зазначила, що електронні докази становлять основу доказової бази у близько 85% кримінальних справ, і в 65% з цих випадків докази потрібно отримати від іншої держави-члена [1].

ЄС ухвалив свої нормативні акти присвячені електронним доказам: Регламент 2023/1543 про Європейські ордери на пред'явлення та Європейські ордери на збереження електронних доказів у кримінальному провадженні та для виконання покарань у вигляді позбавлення волі після розгляду кримінальної справи (далі – Регламент), який встановлює правила та гарантії для національних органів, які зобов'язують постачальників послуг, розташованих в іншій державі-члені, зберігати та надавати електронні докази для їхнього використання в кримінальному провадженні на запити компетентних органів інших держав-членів ЄС [9] та Директиву 2023/1544, що встановлює гармонізовані правила визначення призначених установ і призначення законних представників із метою збору електронних доказів у кримінальному провадженні (далі – Директива) [10].

До електронного доказу, згідно п. 8 ст. 3 Регламенту 2023/1543, відносяться три групи даних: дані абонента, дані трафіку та дані змісту, які зберігаються постачальником послуг або від його імені в електронній формі під час отримання відповідними постачальниками послуг Європейського ордеру про пред'явлення

або Європейського ордеру про збереження. Зокрема, до даних абонента належить інформація, яка дозволяє його ідентифікувати як користувача послуг, а саме зареєстроване ним ім'я, дата народження, адреса, банківські дані на оплату рахунків, телефон, імейл адреса; вид наданих йому послуг, тривалість тощо. До даних трафіку належать дані, пов'язані з наданням послуги, яку пропонує постачальник послуг, наприклад, джерело та призначення повідомлення або інший тип взаємодії, місцезнаходження пристрою, дата, час, тривалість, розмір, маршрут, формат, використовуваний протокол і тип стиснення, а також інші метадані. Дані змісту – інформація про будь-які дані в цифровому форматі, такі як текст, голос, відео, зображення та звук [9].

Цікавий досвід Китайської Народної Республіки (далі – КНР) щодо використання електронних доказів. У 2012 р. електронні докази були прирівняні до існуючих доказів у КПК КНР, хоча кримінально-процесуальний закон не розкривав це поняття [11].

Положення «Про вирішення деяких питань щодо збирання, отримання та аналізу електронних даних у кримінальних справах» визначає електронні докази, як інформацію, зібрану в рамках кримінальної справи, збережену та передану в електронній формі, яка може бути доказом у кримінальній справі. Стаття 2 вказаного Положення відносить до електронних доказів у кримінальній справі: веб-сайти, блоги (онлайн-щоденники), мікроблоги, сторінки в соціальних мережах, ідентифікатори додатку (наприклад, WeChat), форуми, онлайн-диски (онлайнові сховища). Також значення мають комунікації в мережі Інтернет та мережах зв'язку, наприклад, мобільних повідомленнях, електронних листах, повідомленнях з месенджерів, повідомленнях у групах. Особливо важливим є ідентифікаційна інформація, отримана при реєстрації користувача на сайті, електронних транзакціях, журналах реєстрації [12]. Положення також визначає порядок отримання таких доказів тільки двома слідчими та з дотриманням процесуальної форми та технічних стандартів.

Слід підкреслити, що важливу роль у розробці правил щодо електронних доказів грають міжнародні організації. Так, Інтерпол у 2019 р. провів зустріч присвячену електронним доказам, де були не тільки виявлені основні проблеми, використання електронних доказів в процесі доказування, а й вироблені рекомендації як законодавчим, так і правоохоронним органам. Наприклад, при проведенні обшуку та виїмки, їх ідентифікації за допомогою методів, що гарантують їхню цілісність, рекомендується поводитися з ними, як і з усіма іншими традиційними доказами. Необхідно враховувати, що деякі електронні пристрої вимагають особливих процедур збору, пакування та транспортування або тому, що вони схильні до пошкодження електромагнітними полями, або тому, що їх вміст може змінитися під час обігу та резервування [13].

**Висновки.** Використання електронних доказів у кримінальному процесі є складною сферою права, яка продовжує розвиватися. Хоча вони пропонують потужні інструменти для правоохоронних органів, вони також створюють значні проблеми, пов'язані з конфіденційністю, достовірністю та транскордонною співпрацею. Оскільки країни продовжують адаптуватися до епохи цифрових технологій, розробка надійної правової бази та міжнародної співпраці будуть мати важливе значення для забезпечення ефективного та справедливого використання електронних доказів у прагненні до справедливості.

В умовах прагнення України стати повноправним членом ЄС ухвалення нормативних актів на рівні ЄС щодо електронних доказів буде сприяти ефективному транскордонному співробітництву держав-членів ЄС у кримінальних справах, що, враховуючи ріст кіберзлочинів стає все більше актуальним. У процесі вступу до ЄС Україна має не лише посилити співпрацю з державами-членами у кримінальних справах, а також забезпечити відповідність національного законодавства acquis ЄС у сфері кримінального судочинства, що вимагає врахування досвіду європейських країн.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Official Cybercrime Report 2023. Cybersecurity Venture. URL: https://www.esentire.com/resources/library/2023-official-cybercrimereport.
2. Rothstein P.F. Evidence: State and Federal Rules. St. Paul, 1991. 669 p.
3. Federal Rules of Evidence. Washington, 2013. URL: https://www.courts.wa.gov/court_rules/?fa=court_rules.list&group=ga&set=ER.
4. General Principles for Digital Evidence. 2021. URL: https://www.ciinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf.
5. Police and Criminal Evidence Act. 1984. URL: https://www.legislation.gov.uk.
6. Digitally Stored Evidence Standard Operating Procedure. Police Service of Scotland Standard Operating Procedure (SOP). 2018. URL: https://www.scotland.police.uk/spa-media/ercbdgot/indecent-images-childrendigital-media-sop.pdf.
7. Computer Misuse Act. 1990. URL: https://www.uwe.ac.uk/study/it-services/information-security-toolkit/information-security-policies/computer-related-

legislation#ab2846d51-b7e6-4539-94e0-c88b59754c18.
8. Electronic evidence guide. A basic guide for police officers, prosecutors and judges. Version 2.1, Strasbourg. 2020. URL: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf.
9. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj.
10. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32023L1544.
11. Criminal Procedure Law of the People's Republic of China. 2012. URL: https://www.lawinfochina.com/display.aspx?lib=law&id=9247&CGid#:~:text=Article%202%20The%20objectives%20of,by%20law%20and%20combating%20crimes%2C.
12. The provisions of the Supreme People's Court of the People's Republic of China, the Supreme People's Procuratorate of the People's Republic of China and the Ministry of Public Security of the People's Republic of China. 2016. URL: https://splcgk.court.gov.cn/gzfwww// spyw/spywDetails?id=84ba1d7cbc0540d59fe49341f8b1ef85.
13. Guidelines for digital forensics first responder. Best practices for search and seizure of electronic and digital evidence. 2021. URL: https://www.interpol.int/content/download/16243/ file/Guidelines to Digital Forensics First Responders_V7.pdf.