Електронні докази у кримінальному провадженні: досвід реалізації у зарубіжних країнах

Сенченко Надія Миколаївна[1], Чумаченко Валерія Юріївна [2]

Опубліковано	Секція	УДК
30.04.2025	Право	343.14:341.4

DOI: https://doi.org/10.5281/zenodo.15395747

Анотація. Стаття розглядає важливість протидії кіберзлочинності на глобальному рівні та ключову роль електронних доказів у кримінальних провадженнях. Аналізується стан законодавчого регулювання електронних доказів у різних країнах (ЄС, США, Велика Британія, Китай), висвітлюються проблеми відсутності єдиного визначення та складності міжнародної співпраці. Окрему увагу приділено новим регламентам ЄС (2023/1543, 2023/1544), спрямованим на гармонізацію отримання електронних доказів. Підкреслено необхідність балансу між ефективністю правоохоронної діяльності та захистом права на приватність. Розглянуто значення адаптації законодавства України щодо електронних доказів у контексті євроінтеграції.

Ключові слова: кіберзлочинність, цифрова криміналістика, транскордонна співпраця, регламенти ЄС, захист приватних даних.

Electronic evidence in criminal proceedings: experience of implementation in foreign countries

Annotation. In 2017, amendments were made to the Civil Procedure Code, the Commercial Procedure Code, and the Code of Administrative Procedure of Ukraine, which included “electronic evidence” as a means of evidence. The adoption of the Law of Ukraine “On Amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine “On Electronic Communications” to Increase the Efficiency of Pre-Trial Investigation “On Hot Pursuit” and “Countering Cyberattacks” of March 15, 2022 No. 2137-IX significantly improved the regulatory and legal regulation of the process of providing evidence using electronic evidence. However, some issues remain unresolved in the legal field that require further regulation to ensure the effective application of new legislative norms in the practical activities of law enforcement agencies. Given the need to work with electronic documents in most criminal proceedings,

[1] кандидат юридичних наук, доцент, доцент кафедри кримінального права та правосуддя, Національний університет «Чернігівська політехніка». ORCID: http://orcid.org/0000-0002-3767-8937

[2] здобувач вищої освіти І курсу магістратури, юридичного факультету, Національний університет «Чернігівська політехніка». ORCID: https://orcid.org/0009-0007-7429-2690

there is an urgent need to develop uniform rules for handling this type of evidence, as well as to prepare forensic recommendations for practitioners. When working with electronic documents, subjects of evidence must understand the features of these documents, be able to extract them without damaging or changing the information, and also have in-depth knowledge of the tactics of conducting individual investigative (search) and other procedural actions aimed at collecting and studying electronic evidence. The relevance of this study is also due to the lack of a legislative and scientific definition of electronic documents in criminal proceedings, a clear list of their mandatory details and determining their place in the evidence system.

The article considers the importance of combating cybercrime at the global level and the key role of electronic evidence in criminal proceedings. The state of legislative regulation of electronic evidence in different countries (EU, USA, UK, China) is analyzed, the problems of the lack of a single definition and the complexity of international cooperation are highlighted. Special attention is paid to the new EU regulations (2023/1543, 2023/1544), aimed at harmonizing the receipt of electronic evidence. The need for a balance between the effectiveness of law enforcement activities and the protection of the right to privacy is emphasized. The importance of adapting Ukrainian legislation on electronic evidence in the context of European integration is considered.

Keywords: cybercrime, digital forensics, cross-border cooperation, EU regulations, protection of private data.

Вступ

У 2017 році до Цивільного процесуального кодексу, Господарського процесуального кодексу та Кодексу адміністративного судочинства України були внесені зміни, які віднесли «електронні докази» до засобів доказування. Прийняття Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та «протидії кібератакам» від 15 березня 2022 року № 2137-IX суттєво покращило нормативно-правове регулювання процесу доказування за допомогою електронних доказів. Проте в правовому полі залишаються невирішеними окремі питання, що потребують подальшого врегулювання для забезпечення ефективного застосування нових норм законодавства у практичній діяльності правоохоронних органів. З огляду на необхідність роботи з електронними документами у більшості кримінальних проваджень постає гостра потреба у виробленні єдиних правил поводження з цим видом доказів, а також у підготовці криміналістичних рекомендацій для практичних працівників. При роботі з електронними документами суб'єкти доказування повинні розуміти особливості цих документів, вміти здійснювати їх вилучення без пошкодження чи зміни інформації, а також володіти глибокими знаннями щодо тактики проведення окремих слідчих (розшукових) та інших процесуальних дій, спрямованих на збирання та дослідження електронних доказів. Актуальність цього дослідження зумовлена також відсутністю законодавчого та наукового визначення електронних документів у кримінальному провадженні, чіткого переліку їх обов'язкових реквізитів та визначення місця у системі доказів. Для України, яка прагне набуття членства в Європейському Союзі, важливим є запровадження підходів, визначених законодавчими актами ЄС, що особливо актуально в умовах необхідності посилення власної спроможності протистояти викликам війни, що створює значні труднощі для національної правоохоронної та судової системи. Водночас переговорний процес щодо вступу України до ЄС передбачає широке наближення національного законодавства до acquis ЄС, що потребує врахування стандартів

регулювання кримінального судочинства, зокрема у сфері використання електронних доказів. Окрім цього важливо дослідити досвід інших зарубіжних країн щодо застосування електронних доказів у кримінальних провадженнях.

Окремі проблемні питання електронних доказів у кримінальному провадженні досліджували у своїх працях вчені Ю.Ю. Орлов, О.В. Сіренко, Д.С. Степанець, Eoghan Casey, Esther George, Nigel Jones та ін.

Метою статті є дослідження змісту та особливостей правового регулювання та використання електронних доказів у кримінальному судочинстві зарубіжних країн.

Результати

Світове співтовариство усвідомлює важливість протидії кіберзлочинності на глобальному рівні. Уряди багатьох держав ухвалили кримінальне законодавство, створили спеціалізовані підрозділи для боротьби з кіберзлочинністю та сприяють розвитку цифрової криміналістики. Для забезпечення ефективної протидії злочинам у кіберпросторі державні органи повинні мати глибоке розуміння масштабів, видів та наслідків таких правопорушень. Водночас безмежний характер Інтернету, швидкий розвиток технологій та постійне вдосконалення методів, що використовуються кіберзлочинцями, ускладнюють завдання органів кримінальної юстиції щодо всебічного розуміння проблеми. Тому уряди повинні створити умови, за яких інформаційні технології приносять користь суспільству та окремим особам у безпечному середовищі. Первинно електронні документи розглядалися як ключовий елемент у протидії кіберзлочинності, проте сьогодні вони стали невід’ємною частиною майже кожного кримінального правопорушення, де їх можна ефективно використовувати для розслідування, що зумовлює необхідність вивчення питань щодо застосування електронних документів у всіх видах кримінальних правопорушень. Аналіз закордонних наукових публікацій та нормативно-правових актів свідчить, що найчастіше використовуються терміни "electronic evidence" (в перекладі з англійської – "електронний доказ") або "digital evidence" (у перекладі – "цифровий доказ"), тоді як поняття "електронний документ" практично не застосовується. Водночас в європейських країнах відсутнє чітке юридичне визначення електронних доказів. Загальною тенденцією є адаптація принципів та правил, встановлених для традиційних доказів, до електронних, що стосується збору, обміну та оцінки доказової сили.

Поняття електронних доказів у кримінальному провадженні, згідно з думкою Н. М. Ахтирської, охоплює дані, які підтверджують факти, інформацію або концепції в такій формі, що дозволяє їх обробку за допомогою комп'ютерних систем, включаючи програми, виконувані цими системами, або інші дії [1, с. 125]. Джерелами електронних доказів можуть бути різноманітні електронні пристрої, зокрема комп'ютери, периферійні пристрої, мобільні телефони, цифрові камери, комп'ютерні мережі, а також Інтернет. В. В. Мурадов визначає електронні докази як сукупність інформації, що зберігається в електронному вигляді на різноманітних типах електронних носіїв та в електронних засобах, і таку позицію підтримують і такі науковці, як О. І. Котляревський та Д. М. Киценко [2, с. 8]. Часто терміни «електронні докази» і «цифрові докази» розглядаються як синонімічні. І. О. Крицька використовує поняття «цифрових джерел доказової інформації», до яких відносяться програми, файли баз даних, аудіо- і відеозаписи [3, с. 302]. Джерелами таких доказів є пристрої для зберігання даних, зокрема постійні запам'ятовуючі пристрої, накопичувачі на жорстких магнітних дисках (вінчестери, дискети), мобільні носії (оптичні диски, флеш-карти), а також NAS-системи [4, с. 209-210]. Оскільки існують різні підходи до використання термінів у науковому середовищі, ми схиляємось до використання терміна «електронні докази» в контексті кримінального провадження як більш відповідного і загальноприйнятого.

Комітет безпеки Європейського Союзу визначає електронні докази як дані, що зберігаються в електронному вигляді, наприклад, IP-адреси, електронні листи, фотографії або імена користувачів, які мають значення для кримінального процесу. Зазвичай такі дані знаходяться у постачальників послуг, а правоохоронні та судові органи змушені звертатися до них для отримання необхідної інформації. У національному законодавстві Австрії, Болгарії, Чеської Республіки, Італії, Швеції та інших держав офіційне визначення електронних доказів відсутнє. Законодавство Португалії також не містить визначення терміна "електронний доказ", однак у цій країні використовується наукове визначення, згідно з яким електронний доказ — це будь-який тип інформації, що має доказове значення та зберігається на цифровому пристрої або передається в цифровій чи двійковій формі. У Німеччині електронні докази визначають як інформацію, що зберігається або передається у цифровій формі та має значення для кримінального розслідування. У Франції електронні докази охоплюють будь-яку доказову інформацію, створену, збережену або передану в цифровій формі за допомогою електронних пристроїв, яка є важливою для досудового розслідування кримінальних правопорушень. До електронних доказів належать різні типи даних в електронній формі, зокрема електронні листи, текстові повідомлення, фотографії, відео з мережі Інтернет, а також інші категорії даних, такі як інформація про абонентів або дані про трафік онлайн-акаунтів. Електронні докази мають таку саму юридичну силу, як і паперові, вони підписуються і не потребують прив’язки до конкретного технологічного засобу. Жодна з досліджуваних країн не передбачає спеціальних юридичних кодексів для роботи з електронними доказами. Аналіз законодавства цих держав показує, що електронні докази зазвичай прирівнюються до традиційних доказів, причому найбільш схожі вони з документами у паперовій формі [5, с. 169].

Німеччина, Бельгія, Іспанія, Фінляндія, Франція, Ірландія, Італія, Люксембург, Португалія та Румунія визнають електронні документи рівнозначними паперовим документам та надають їм юридичне значення в судовому процесі [6, с. 286]. Незважаючи на відсутність єдиного визначення терміна «електронний доказ», держави-члени Європейського Союзу та Ради Європи успішно співпрацюють у питаннях збору, збереження та використання електронних доказів. Хоча в Європейській конвенції про взаємодопомогу у кримінальних справах немає чіткого визначення поняття «докази», це не стає перешкодою для співробітництва між європейськими країнами. Теоретично запровадження єдиного визначення електронних доказів могло б спростити процедуру їх обміну, що сприяло б ефективнішій взаємодії між державами-членами. На сьогоднішній день не існує універсальної міжнародної чи європейської правової бази, яка б регулювала питання електронних доказів. У більшості випадків держави покладаються на норми національного законодавства при зборі, збереженні, використанні та обміні такими доказами. Національні кримінальні закони були ухвалені задовго до появи інтернету та технологій, здатних створювати електронні докази, тому деякі країни адаптували своє законодавство до нових умов, тоді як інші продовжують застосовувати традиційні кримінальні закони, поширюючи їх також на електронні докази, що призводить до значних відмінностей у національних правових системах та підходах до обробки транскордонних електронних доказів, що створює певні труднощі у цій сфері. Згідно з дослідженням ООН щодо кіберзлочинності, навіть у країнах зі схожими правовими традиціями правила, що стосуються доказів, істотно відрізняються, що ускладнює міжнародне співробітництво у боротьбі з кіберзлочинністю [7, с. 192]

У межах Європейського Союзу Європейська Комісія у 2023 році розробила та оприлюднила пакет нормативних актів, що отримав підтримку Європейського Парламенту та Ради ЄС. Ці акти запроваджують нові підходи до отримання електронних доказів через пряме звернення до приватних постачальників послуг зв’язку, зберігання даних та інтернет-інфраструктури, що знаходяться в іншій державі-члені ЄС, без

необхідності залучення національних органів держави, де розташований постачальник послуг. Аналітики A. Juszczak та E. Sason зазначають, що реалізація такого підходу можлива за умови високого рівня взаємної довіри між державами-членами. Важливо також враховувати, що держави-члени зберігають широкі повноваження у визначенні змісту доказів, їхньої належності та особливостей застосування, тоді як норми права ЄС встановлюють лише мінімальні стандарти, яких повинні дотримуватися держави-члени в межах національних систем кримінальної юстиції. Новий пакет законодавчих актів ЄС щодо електронних доказів включає два нормативні акти, ухвалені 12 липня 2023 року. Перший — 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 [9]. Другий — Директива 2023/1544, яка встановлює гармонізовані правила щодо визначення призначених установ та призначення законних представників з метою збору електронних доказів у кримінальному провадженні [10].

Регламент 2023/1543, що регулює Європейські ордери на пред'явлення та Європейські ордери на збереження електронних доказів у кримінальному провадженні, а також для виконання покарань у вигляді позбавлення волі, встановлює пряму дію в національних правових системах держав-членів. Він визначає правила та гарантії для національних органів, покладаючи на постачальників послуг, що діють в межах інших держав-членів, зобов'язання щодо збереження та надання електронних доказів для використання в кримінальному провадженні на запити компетентних органів інших держав-членів Європейського Союзу. Згідно з положеннями Протоколу № 22, який стосується неучасті Данії у Просторі свободи, безпеки та справедливості ЄС, цей регламент є обов'язковим для всіх держав-членів, за винятком Данії. Регламент 2023/1543, спираючись на статтю 82(1) Договору про функціонування Європейського Союзу, вводить два нових правових інструменти, призначені для використання державами-членами з метою отримання електронних доказів у кримінальному провадженні: Європейський ордер про пред'явлення та Європейський ордер про збереження [9]. Обидва інструменти визначаються як рішення, видані або підтверджені судовим органом держави-члена та адресовані призначеній установі або законному представнику постачальника послуг, який надає послуги в Союзі та розташований в іншій державі-члені, з метою отримання електронних доказів або їх збереження для подальшого запиту на пред'явлення. На підставі Європейського ордеру про збереження судові органи держави-члена мають право заборонити постачальникам послуг, зареєстрованим на території іншої держави-члена, видаляти або змінювати дані. Водночас Європейський ордер про пред'явлення дозволяє органам влади негайно або у визначений час вимагати збережену інформацію безпосередньо від постачальників послуг [11, с. 442].

Регламент 2023/1543 встановлює умови видачі документів, їх оформлення постачальниками послуг, вимоги до повідомлень та підстави для відмови з боку держави-члена, що виконує ордер, процедуру виконання, заходи відповідальності, права осіб, чиї дані запитуються, процедуру перегляду у випадку конфлікту зобов'язань з законодавством третьої країни, положення щодо стандартизованих сертифікатів та децентралізованої ІТ-системи, а також норми, що регулюють розподіл витрат. Варто зазначити, що Регламент не надає вичерпного переліку правил, які повністю регулюють застосування Європейського ордера про пред'явлення та Європейського ордера про збереження, натомість у багатьох випадках відсилає до положень національного законодавства держав-членів. Сфера застосування Регламенту 2023/1543 обмежена ордерами, що видаються в рамках кримінального провадження та з метою виконання покарань у вигляді позбавлення волі або тримання під вартою на строк не менше чотирьох місяців, винесених рішенням за участі сторони захисту. Провадження in

absentia виключені з дії цього Регламенту відповідно до статті 2 [9]. Накази можуть бути видані також у кримінальному провадженні проти юридичної особи, що унеможливлює їх використання як превентивних заходів або засобів постійного спостереження, що вимагає наявності конкретного кримінального провадження, тобто застосування таких інструментів можливе виключно в межах кримінальної справи до моменту її завершення. Регламент не поширюється на справи про взаємну правову допомогу, де застосовуються інші відповідні інструменти.

Згідно з Регламентом 2023/1543, визначення «електронного доказу» охоплює три категорії даних: відомості про абонента, дані трафіку та зміст [9]. Дані, що зберігаються в електронному форматі постачальником послуг або від його імені, підлягають наданню за Європейським ордером про пред'явлення або збереження. До відомостей про абонента належить інформація, що ідентифікує користувача послуг, зокрема його зареєстроване ім'я, дата народження, адреса, банківські реквізити для оплати, номер телефону, електронна адреса, вид наданих послуг та їх тривалість. Дані трафіку включають інформацію щодо надання послуги постачальником, таку як джерело та призначення повідомлення, місцезнаходження пристрою, дата, час, тривалість, розмір, маршрут, формат, використовуваний протокол, тип стиснення та інші метадані. Зміст включає будь-яку цифрову інформацію, як-от текст, голос, відео, зображення та звук. Персональна та територіальна сфера дії Регламенту 2023/1543 поширюється на суб'єктів, що надають послуги в межах Європейського Союзу, згідно зі статтею 2, частина 1, а саме: «постачальники послуг, що забезпечують електронні комунікаційні та інші інформаційні послуги, які дають змогу користувачам спілкуватися між собою або здійснюють обробку чи зберігання даних від імені користувачів, наприклад, телекомунікаційні компанії та компанії соціальних мереж». До цих суб'єктів належать провайдери IP-телефонії, послуг обміну миттєвими повідомленнями, електронної пошти, ринкові майданчики, інші хостинг-послуги, онлайн-ігри та платформи азартних ігор.

Згідно з Регламентом 2023/1543, встановлення статусу постачальника послуг, що діє в межах Європейського Союзу, вимагає аналізу двох взаємопов'язаних критеріїв. Первинний критерій полягає в доступності послуг на території держави-члена, тоді як вторинний критерій передбачає наявність суттєвого зв'язку з цією державою, що встановлюється на основі конкретних фактичних показників. Наявність такого зв'язку підтверджується, якщо постачальник послуг має організацію, що фізично розташована в межах Союзу. У випадках відсутності такої організації, суттєвий зв'язок також може бути визнаний, якщо постачальник послуг має значну кількість користувачів в одній або декількох державах-членах, або якщо його діяльність спрямована на одну або декілька держав-членів ЄС. Для визначення такого зв'язку Регламент передбачає ряд критеріїв оцінки, включаючи використання місцевої мови або валюти, можливість замовлення товарів або послуг, наявність додатків у місцевих магазинах додатків, а також здійснення рекламної діяльності. Важливо зазначити, що проста присутність в Інтернеті, наприклад, через веб-сайт або електронну адресу, сама по собі не є достатньою для підтвердження того, що постачальник послуг надає послуги в межах Союзу, відповідно до положень цього Регламенту.

Європейський ордер на пред'явлення, як інструмент судової практики, може бути санкціонований судовим органом, зокрема судом або органом обвинувачення, у випадках, коли запит стосується даних абонента та конкретних видів даних трафіку. Ордер спрямований на отримання відомостей, необхідних для ідентифікації користувача, таких як IP-адреси та номери доступу. У певних обставинах, ордер може бути виданий іншим компетентним органом держави видачі, що діє як слідчий орган, уповноважений національним законодавством на збір доказів у кримінальному провадженні. Однак, у таких випадках, наказ підлягає підтвердженню судовим органом,

який здійснює перевірку його відповідності умовам Регламенту та, за потреби, національному законодавству. Європейський ордер про збереження, на відміну від попереднього, не передбачає диференціації залежно від категорій даних. Тому, цей ордер може бути виданий щодо будь-яких видів даних, як судовим органом, так і будь-яким іншим компетентним органом держави-члена, що видає рішення. Для ефективного функціонування обох видів ордерів, кожна держава-член повинна визначити один або кілька центральних органів, наділених повноваженнями приймати рішення щодо необхідності отримання інформації за такими ордерами [12, с. 822-823].

Важливим регуляторним актом Європейського Союзу, що стосується питань електронних доказів, є Директива 2023/1544, затверджена 12 липня 2023 року [10]. Акт встановлює уніфіковані норми для ідентифікації уповноважених установ та призначення законних представників з метою збору електронних доказів у контексті кримінальних розслідувань. Директива визначає юридичні основи для компетентних органів країн-членів ЄС стосовно їхніх повноважень у межах інших країн ЄС, щоб забезпечити належне виконання розпоряджень, виданих органами цих держав для збору електронних доказів відповідно до Регламенту 2023/1543. Основне зобов'язання для країн-членів викладене у статті 3 цієї Директиви, згідно з яким країни повинні забезпечити, щоб постачальники послуг, що функціонують на ринку ЄС, призначали щонайменше одну уповноважену особу, відповідальну за отримання та виконання рішень, виданих компетентними органами для збору доказів у кримінальних справах, включаючи електронні. Проте, зважаючи на специфіку цього нормативного акта ЄС, кожна держава-член може самостійно визначати, яким чином вона реалізовуватиме це зобов'язання, зберігаючи певну свободу дій у процесі його виконання.

В англосаксонській правовій системі не існує чіткого поділу доказів на різні категорії. Доказове право США формується на основі типових проблемних ситуацій і закріплює основні судові рішення, що стали знаковими, а також узагальнену практику. При цьому система доказового права має заборонний характер, оскільки визначає, в яких випадках доказ не може бути визнаний допустимим. Для американських юристів не має великого значення, чи є електронні докази окремим видом доказів. Основним нормативним актом, що регулює доказування в США, є Федеральні правила доказів, прийняті в 1975 році. Згідно з статтею 401 цих правил, належними вважаються докази, які можуть вплинути на ймовірність існування певного факту, що має значення для кваліфікації вчиненого діяння, роблячи його більш або менш вірогідним, залежно від того, чи є ці докази. Стаття 402 Федеральних правил роз’яснює поняття цифрових доказів як дані та носії, на яких ці дані зберігаються [13]. Таке широке трактування доказів дозволило широко застосовувати електронні докази у кримінальному процесі США. Перед тим, як суд прийме електронне доказування, учасник процесу повинен довести його автентичність, використовуючи стандартну процедуру автентифікації електронного документа. Також сторона повинна надати опис процесу створення або системи, яка використовується для отримання результату, та підтвердити, що ця система чи процес забезпечують точність отриманих даних. Електронні докази мають бути релевантними для конкретної справи, тобто вони повинні давати можливість зробити факт більш або менш ймовірним, ніж це було б без таких доказів. Факт має бути значущим для вирішення справи, і докази є прийнятними, якщо вони не суперечать вимогам Конституції Сполучених Штатів, федеральному законодавству, іншим федеральним правилам доказування або рішенням, встановленим Верховним судом США [14].

Законодавче регулювання електронних доказів у Великій Британії визначається Законом про поліцію та кримінальні докази 1984 року. Згідно з його статтею 19, поліція має право отримувати будь-яку інформацію, у тому числі в електронній формі, якщо вона має відношення до розслідування або попередження злочинів, а також коли її

вилучення може запобігти приховуванню, знищенню, втраті або підробці доказів у будь-якому вигляді [15]. Для цифрових доказів діють ті самі норми, що й для традиційних документальних доказів. Окрім цього, питання регулювання електронних доказів охоплюється також Статутом про використання комп'ютера із протиправною метою, який встановлює кримінальні норми щодо комп'ютерних злочинів та інших правопорушень, вчинених з використанням комп'ютерної техніки як знаряддя злочину. Він містить також кримінально-процесуальні норми, що стосуються обшуку та вилучення електронних доказів, а також визначає повноваження правоохоронних органів. Важливо відзначити, що у Великій Британії не існує окремої категорії доказів під назвою "електронні докази". Натомість, мова йде про встановлені процедури та правила щодо подання електронних документів у рамках загального законодавства.

Досвід Китайської Народної Республіки у сфері використання електронних доказів викликає значний академічний і практичний інтерес, зокрема через унікальні демографічні та технологічні умови країни. З населенням понад 1,4 мільярда осіб, що робить її другою за чисельністю державою світу, КНР стикається з безпрецедентними викликами та можливостями у впровадженні цифрових інновацій у правову систему. Проте саме цей масштаб став каталізатором для розвитку передових механізмів роботи з електронними даними, які поєднують штучний інтелект, Big Data та сувору законодавчу базу. У 2012 році електронні докази були прирівняні до традиційних доказів у рамках Кримінально-процесуального кодексу КНР, хоча цей закон не надавав чіткого визначення поняття електронних доказів. У документі «Про вирішення деяких питань щодо збирання, отримання та аналізу електронних даних у кримінальних справах» електронні докази визначені як інформація, яка була зібрана в межах кримінальної справи, збережена і передана в електронному вигляді і яка може бути використана як доказ у кримінальному процесі. Відповідно до статті 2 цього документу, до електронних доказів у кримінальних справах відносяться веб-сайти, блоги, мікроблоги, сторінки в соціальних мережах, ідентифікатори додатків, форуми, онлайн-диски та інші онлайн-сховища. Важливими також є комунікації в Інтернеті, включаючи мобільні повідомлення, електронні листи, повідомлення через месенджери та в групах. Особливу цінність становить ідентифікаційна інформація, яка збирається під час реєстрації користувача на сайтах, при здійсненні електронних транзакцій, а також журнали реєстрації. Положення також встановлює, що отримання таких доказів можливе лише за участю двох слідчих, з дотриманням процесуальних вимог і технічних стандартів [16].

Електронні докази можуть містити інформацію, яка стосується таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції, що є особистим правом, яке належить до основних природних прав людини. Відповідно до статті 8 Конвенції про захист прав людини і основоположних свобод, кожна особа має право на повагу до свого приватного та сімейного життя, житла і кореспонденції. Державні органи не мають права втручатися в здійснення цього права, за винятком випадків, коли втручання відбувається відповідно до закону і є необхідним у демократичному суспільстві для захисту національної та громадської безпеки, економічного добробуту країни, запобігання заворушенням чи злочинам, а також для захисту здоров'я, моралі або прав і свобод інших осіб. Водночас електронні документи стають важливим елементом у рішеннях Європейського суду з прав людини. Так, у справах, таких як «P. and S. v. Poland» (30.10.2012), «Eon v. France» (14.03.2013) та «Shuman v. Poland» (03.06.2014), ЄСПЛ розглядав порушення процедури збору електронних доказів, що стосуються таємниці приватного та сімейного життя, що стало підставою для вирішення спорів [17]. Наприклад, у справі «M.N. and Others v. San Marino» (заява № 28005/12 від 07 липня 2015 року) суд зазначив, що вилучення даних, таких як банківські відомості, отримані з виписок, чеків, фідуціарних розпоряджень та електронних листів, може бути

трактовано як втручання в приватне життя і листування, що підпадає під захист, встановлений статтею 8 Конвенції [18]. У справі «Copland v. the United Kingdom» (заява № 62617/00, рішення від 3 квітня 2007 року) ЄСПЛ підкреслив, що електронні листи, відправлені з робочого місця, повинні також захищатися згідно зі статтею 8 Конвенції, так само як і інформація, отримана через моніторинг приватного використання Інтернету. Заявниця в цьому випадку не була попереджена про можливість відстеження її дзвінків, тому вона обґрунтовано очікувала приватності дзвінків, здійснених з робочого телефону, так само як і щодо електронної пошти та використання Інтернету. ЄСПЛ визнав порушення статті 8 Конвенції в зв'язку з моніторингом телефонних дзвінків, електронної пошти та Інтернету працівниками без відповідного законодавчого обґрунтування цього втручання. Однак суд не виключає, що в певних випадках моніторинг може бути визнано «необхідним у демократичному суспільстві» і мати законну мету, хоча у конкретній справі, через відсутність законності втручання, питання необхідності не було розглянуте [19].

Висновки

Таким чином, дослідження показало, що електронні докази стали невід'ємним елементом сучасної кримінальної юстиції, особливо у контексті боротьби з кіберзлочинністю. Незважаючи на відсутність єдиного міжнародного або навіть європейського визначення, більшість країн адаптують традиційні правові норми до цифрового середовища, визнаючи електронні докази рівнозначними паперовим. Проте розбіжності у термінології, процедурах збору, зберігання та обміну такими доказами ускладнюють міжнародне співробітництво. Ініціативи ЄС, такі як Регламент 2023/1543 та Директива 2023/1544, спрямовані на гармонізацію підходів, але їх ефективність залежить від взаємної довіри між державами та врахування національних особливостей. Важливим аспектом залишається баланс між ефективністю правоохоронної діяльності та захистом прав на приватність під час збирання електронних доказів у зарубіжних країнах, що підкреслюється практикою ЄСПЛ.

У контексті прагнення України стати повноправним членом Європейського Союзу, прийняття нормативних актів ЄС щодо електронних доказів відіграватиме важливу роль у забезпеченні ефективної транскордонної співпраці серед держав-членів Союзу в кримінальних справах, що стає все більш актуальним на тлі зростання кіберзлочинності. В процесі інтеграції до ЄС Україні необхідно не лише посилити взаємодію з іншими державами-членами у питаннях кримінального правосуддя, але й адаптувати своє національне законодавство до acquis ЄС у сфері кримінального судочинства, що вимагає врахування досвіду європейських країн.

Список використаних джерел

1. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету*. 2016. № 36(2). С. 123–125.
2. Мурадов В. В. Електронні докази: криміналістичний аспект використання. *Порівняльне правознавство*. 2013. № 3-2. С. 313–315.
3. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. № 1. С. 301–304.
4. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. № 14. С. 208–214.

5. Ратнова А. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 Право. Львів, 2021. 248 с.
6. Fredesvinda I. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*. 2007. No. 1 (4). P. 285–289.
7. Mifsud Bonnici J. P., Tudorica M., Cannataci J. A. The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. *Law, Governance and Technology Series*. 2018. No. 39. P. 189–234.
8. Juszczak A., Sason E. The Use of Electronic Evidence in the European Area of Freedom, Security and Justice. An Introduction to the New EU Package on E-evidence. *EUCRIM*. 2023. No. 2. P. 182–200.
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 proceeding. *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj (дата звернення: 01.04.2025).
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. *EUR-Lex*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32023L1544 (дата звернення: 01.04.2025).
11. Чорнозуб Л. Використання цифрових доказів у кримінальному судочинстві держав-членів Європейського Союзу: нові правові інструменти. *Юридичний науковий електронний журнал*. 2024. № 3. С. 441–444.
12. Ніколенко Л. Використання електронних доказів в кримінальному процесі зарубіжних країн. *Аналітично-порівняльне правознавство*. 2024. № 5. С. 820–824.
13. Federal Rules of Evidence. *LII / Legal Information Institute*. URL: https://www.law.cornell.edu/rules/fre (дата звернення: 01.04.2025).
14. General Principles for Digital Evidence. *Conference of International Investigators*. URL: https://www.ciinvestigators.org/wp-content/uploads/2021/11/CII-General-Principles-for-Digital-Evidence-21stCII.pdf (дата звернення: 01.04.2025).
15. Police and Criminal Evidence Act 1984. *Legislation.gov.uk*. URL: https://www.legislation.gov.uk/ukpga/1984/60/contents (дата звернення: 01.04.2025).
16. Criminal Procedure Law of the People's Republic of China. *WIPO - World Intellectual Property Organization*. URL: https://www.wipo.int/wipolex/en/text/337115 (дата звернення: 01.04.2025).
17. Фулей Т. Застосування практики Європейського суду з прав людини при здійсненні правосуддя : Науково-метод. посіб. для суддів. 2-ге вид. випр., допов. Київ, 2015. 208 с.
18. M.N. and Others v. San Marino. *HUDOC - European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=001-155819 (дата звернення: 01.04.2025).
19. Copland v. the United Kingdom. *HUDOC - European Court of Human Rights*. URL: https://hudoc.echr.coe.int/eng?i=002-2765 (дата звернення: 01.04.2025).