

**КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА.
СУДОВА ЕКСПЕРТИЗА. ОПЕРАТИВНО-РОЗШУКОВА
ДІЯЛЬНІСТЬ**

УДК 343.14:340.13

Ангеленюк Анна-Марія Юріївна,
кандидат юридичних наук,
старший науковий співробітник
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0001-5947-5105

**ШЛЯХИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ПРОЦЕСУАЛЬНОГО
ЗАКОНОДАВСТВА ЩОДО ЗБИРАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ**

У статті зосереджено увагу на актуальності збирання електронних доказів у кримінальному провадженні під час розслідування злочинів. У межах порівняльного методу наведено окремі положення нормативно-правових актів національного законодавства та Європейського Союзу, які стосуються збирання електронних доказів та спрямовані на удосконалення цього процесу. Надано пропозиції до кримінального процесуального законодавства України, що сприятимуть підвищенню якості збирання електронних доказів, враховуючи використання міжнародної правової допомоги.

Ключові слова: доказування, збирання, правова основа, запит, електронні докази, міжнародна правова допомога.

В умовах сьогодення під час розслідування кримінальних проваджень окреме місце займають електронні докази, що частково пов'язано з використанням електронно-технічних інновацій у сучасному світі, які набувають широкого застосування у різних сферах діяльності людини. Так, наприклад, у межах державних інституцій діють електронні сервіси з метою покращення надання послуг; у сфері торгівлі створені електронні платформи для продажу товарів чи послуг; у містах широко застосовуються системи автономного відеоспостереження; розширено функції індивідуальних технічних засобів, мобільних пристроїв тощо. Не стало винятком і використання електронно-технічних інновацій під час злочинної діяльності, що вплинуло на способи вчинення кримінальних правопорушень та приховування їх слідів, зокрема у кіберпросторі [1]. Як наслідок, правоохоронні органи та суди дедалі частіше досліджують докази, зафіксовані в електронній формі [2, с. 116].

Слід зауважити, що у низці випадків через недосконалість правової основи збирання електронних доказів, їх може бути визнано недопустимими у кримінальному провадженні [3, с. 210]. Особливо вирішення зазначеної проблеми є актуальним та потрібним під час розслідування злочинів, вчинених окупаційними військами на території України, так як електронні докази цієї категорії злочинів надалі можуть

© Anheleniuk Anna-Mariia, 2023

DOI (Article): [https://doi.org/10.36486/np.2023.4\(62\).18](https://doi.org/10.36486/np.2023.4(62).18)

Issue 4(62) 2023

<https://naukaipravohorona.com/>

представляться у міжнародних судових інституціях та бути основними підставами для визнання вини обвинувачених осіб [2, с. 117–118].

Відтак, розслідування злочинів у сучасних умовах вимагає вдосконалення кримінального процесуального законодавства щодо збирання електронних доказів у кримінальному провадженні, формування шляхів здійснення якого в Україні є метою статті.

У своїх роботах електронним доказам у кримінальному судочинстві приділяли увагу Н. М. Ахтирська, М. В. Гуцалюк, О. В. Сіренко, В. Г. Хахановський та інші. Серед авторів, які досліджували питання електронних доказів у кримінальному процесі на дисертаційному рівні, можна назвати А. В. Ратнову, А. В. Скрипника, А. В. Столітнього. Однак у науці досліджено лише окремі аспекти збирання електронних доказів.

Ураховуючи появу в кримінальному процесуальному полі більшої кількості електронних доказів, а також міжнародні тенденції розвитку правових засад та удосконалення порядку збирання електронних доказів під час розслідування злочинів, потрібно надалі розвивати наукові напрацювання щодо цього в Україні. Таким чином, слід внести відповідні зміни до законодавства нашої держави, які б підсилили правову основу практичного використання електронних доказів, удосконалили б порядок їх збирання, а також підвищили б їх ефективність у кримінальному процесі під час розслідування кримінальних правопорушень.

Загалом слід відзначити позитивний законотворчий процес щодо удосконалення законодавства з питань застосування цифрових технологій в Україні.

Робота з приводу використання електронних доказів у кримінальному процесі, передусім, розпочалась із їх фактичної наявності під час доказування вчинення злочинів у кіберпросторі, де будь-яких інших доказів (не електронних) може не існувати. Проте, враховуючи сучасні виклики і тенденції у сфері кримінально-процесуальних відносин, не слід пов'язувати електронні докази лише з кіберзлочинністю, а розуміти, що використання електронних технологій на сьогодні вийшли за її межі та стосуються решти кримінальних правопорушень також.

Серед нормативно-правових актів, що стосуються цифрової сфери, необхідно виділити Стратегію кібербезпеки України, затверджену Указом Президента України від 26 серпня 2021 року (далі – Стратегія), у якій серед стратегічних цілей необхідно виокремити «Прагматичне міжнародне співробітництво» та «Ефективну протидію кіберзлочинності» як такі, що найбільш актуальні під час збирання електронних доказів та розслідування кримінальних правопорушень в Україні.

Окрім того, слід зауважити, що у Стратегії одним із чинників та передумов, які формують загрози кібербезпеки України, визначено недостатню урегульованість цифрової складової розслідування кримінальних правопорушень.

Забезпечення досягнення стратегічних цілей, відповідно до положень Стратегії, має здійснюватися в Україні так:

1) шляхом розвитку міжнародного співробітництва (в межах якого Україною підписано Другий додатковий протокол до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці

між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах);

2) шляхом удосконалення на законодавчому рівні питань, що стосуються електронних доказів (використовуючи при цьому кращі практики Сполучених Штатів Америки, а також держав-членів Європейського Союзу (далі – ЄС) з цих питань) [1].

Також слід звернути увагу на внесення змін і доповнень до законодавства України у 2022 році, відповідно законів України «Про внесення змін до Кримінального процесуального кодексу України та «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» [4], які вирішили частину проблемних питань, пов'язаних зі збиранням електронних доказів під час розслідування злочинів, а саме:

1) введено статтю 245-1 «Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису», яка закріпила порядок здійснення цієї процесуальної дії під час розслідування кримінальних правопорушень;

2) надано можливість у разі необхідності виготовляти постанову слідчого, прокурора в електронній формі (з використанням електронного підпису) або в Інформаційно-телекомунікаційній системі досудового розслідування та інше.

Отже, в Україні на законодавчому рівні закріплені основні напрями роботи, що стосуються розвитку цифрових технологій. Проте законодавство, яке безпосередньо стосується застосування електронних доказів під час розслідування кримінальних правопорушень, потребує надалі вдосконалення, що має спрямовуватися на покращення реагування правоохоронних органів на кримінальні правопорушення та виконання завдань кримінального процесу загалом, у тому числі під час воєнного стану.

Цікавими та корисними під час дослідження питань збирання електронних доказів у кримінальному провадженні є напрацювання країн ЄС.

Увагу привертають напрями роботи ЄС, які стосуються уніфікації підходів до збирання електронних доказів, що є цінним досвідом для перейняття у глобальному сенсі для світової спільноти. Дійсно, відсутність єдиного підходу до збирання електронних доказів може призвести до правової невизначеності як для постачальників послуг, так і для правоохоронних органів чи суду. Наприклад, у постачальників послуг, які створені або пропонують послуги в різних державах, можуть виникати різноманітні чи навіть суперечливі зобов'язання, відповідно це призводить до того, що такі постачальники послуг підлягають різним санкціям у разі порушень. Значення таких розбіжностей надалі у межах кримінального провадження зростатиме, оскільки у повсякденному житті суспільства все більше використовуються комунікаційні та інформаційні послуги. Такі розбіжності, безперечно, становлять перешкоду для належного збирання електронних доказів учинення кримінальних правопорушень під час досудового розслідування, у тому числі у разі взаємодії між країнами у межах міжнародної правової допомоги.

Наступними питаннями, що потребують вдосконалення та стосуються електронних доказів, є швидкість їх отримання, а також можливості їх збереження. Пришвидшення процесу отримання електронних доказів, а також їх зберігання пов'язано саме із формою

електронних доказів, які переважно нестійкі до впливу фізичних чинників: легко модифікуються, знищуються тощо [5, с. 15]. Відповідно для правоохоронних органів та суду ЄС важливо мати ефективні інструменти для швидкого отримання електронних доказів та їх збереження під час розслідування кримінальних правопорушень.

Отримання електронних доказів через суди часто займає багато часу, що призводить до ситуацій, коли потрібні відомості можуть бути уже недоступними. У разі відсутності узгоджених правил співпраці з постачальниками послуг різних країн-членів ЄС з'явилися випадки прийняття постачальниками послуг прямих запитів щодо отримання відомостей, якщо це не суперечить нормам їх національного законодавства. Як наслідок, країни-члени ЄС все більше покладаються на добровільну пряму взаємодію з постачальниками послуг.

Отже, наявна законодавча база ЄС має прогалини, що створює проблеми для правоохоронних органів та судів, а також для постачальників послуг, які прагнуть задовольнити юридичні запити щодо електронних доказів, бо через правову невизначеність не хочуть мати потенційні конфлікти з органами влади чи судом.

Враховуючи зазначені вище проблеми, які стосуються збирання електронних доказів у кримінальному провадженні, в ЄС запропонували вирішити, створивши спеціальні правила щодо транскордонного судового співробітництва для збереження та виготовлення електронних доказів, що враховуватимуть особливий характер електронних доказів та міститимуть зобов'язання для постачальників послуг відповідати безпосередньо на запити, які надходять від органів влади іншої держави-члена ЄС [6]. Так, 17 серпня 2023 року набули чинності Внутрішні правила ЄС, які застосовуватимуться з 2026 року, відповідно до яких передбачено:

- створення європейського ордеру на пред'явлення документів;
- створення європейського наказу про збереження даних;
- гарантування правового захисту, включаючи гарантії права на захист персональних даних;
- створення децентралізованої ІТ-системи;
- зобов'язання постачальників послуг стосовно призначення установи або призначення законного представника в ЄС;
- забезпечення юридичної визначеності щодо діяльності підприємств та постачальників послуг [7].

Отже, використовуючи практику країн-членів ЄС, в Україні необхідно надати перевагу застосуванню консолідованих підходів до збирання електронних доказів.

Позитивним моментом є те, що Україна має напрацювання у напрямі взаємодії з країнами-членами ЄС. Так, Україною підписано Другий додатковий протокол до Конвенції про кіберзлочинність, схвалений Радою Європи 17 листопада 2021 року. Зазначений протокол скерований на забезпечення ефективності заходів кримінального правосуддя та збір доказів в електронній формі, а також передбачає вищий рівень оперативності та доцільність прискореної процедури в межах міжнародного співробітництва [2, с. 121].

Згідно з Другим додатковим протоколом до Конвенції про кіберзлочинність,

передбачені: розширення прямого співробітництва з постачальниками послуг; взаємодія між органами з питань розкриття збережених комп'ютерних даних та інших можливостей підвищення ефективності роботи з електронними доказами, зокрема у надзвичайних ситуаціях. Окрім того, за положеннями протоколу підставою для відмови у міжнародному співробітництві не можуть бути: відсутність такого ж складу правопорушення в законодавстві запитуваної держави; інше термінологічне визначення діяння; віднесення діяння до іншої категорії тяжкості [8, с. 192; 9].

На сьогодні необхідною є ратифікація зазначеного протоколу, а також внесення змін у Кримінальний процесуальний кодекс України (далі – КПК), враховуючи світові тенденції розвитку використання електронних доказів.

Так, з метою удосконалення міжнародного співробітництва та спрощення його використання у надзвичайних ситуаціях, можна:

1) доповнити статтю 544 КПК частиною 3-1 такого змісту: «Кожна сторона може шукати взаємної допомоги у швидкому порядку, якщо вона вважає, що існує надзвичайна ситуація»;

2) додати у частину 5 статті 548 КПК після слів «отримання українською стороною оригіналу запиту» слова «крім випадків направлення та виконання запиту під час надання надзвичайної взаємодопомоги. У випадку існування надзвичайної ситуації та інших умов при яких запит підлягає виконанню, запитувана сторона повинна негайно відповісти на запит».

Наведені пропозиції до статей 544 та 548 КПК України слід розглядати як частину комплексної законотворчої роботи щодо збирання електронних доказів у кримінальному процесі.

Підсумовуючи наведене вище, слід зазначити, що на сьогодні основними шляхами удосконалення кримінального процесуального законодавства щодо збирання електронних доказів є правові. Так, у положеннях КПК, перш за все, необхідно закріпити поняття електронних доказів як джерел права; доповнити та деталізувати порядок їх збирання, фіксації та зберігання. Також слід створити правову основу для прямого співробітництва з постачальниками послуг; пришвидшення форм співробітництва для розкриття інформації про абонентів (трафіків); пришвидшення взаємодопомоги у надзвичайних ситуаціях; діяльності, що стосується міжнародного співробітництва, якщо така не охоплена міжнародними договорами, в тому числі організації відеоконференцій, роботи спільних слідчих груп та спільних розслідувань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стратегія кібербезпеки, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL : <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 12.10.2023).

2. Гуцалюк М.В., Антонюк П.Є. Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. Інформація і право № 2 (41). 2022. С. 116–122. URL: https://ippi.org.ua/sites/default/files/15_22.pdf (дата звернення: 12.10.2023).

3. Сіренко О.В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2019. Вип. 14. С. 208–214.

© Anhelenuk Anna-Mariia, 2023

DOI (Article): [https://doi.org/10.36486/np.2023.4\(62\).18](https://doi.org/10.36486/np.2023.4(62).18)

Issue 4(62) 2023

<https://naukaipravohorona.com/>

4. 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»: Закон України від 15 березня 2022 року № 2137-IX. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#n17> (дата звернення: 12.10.2023).

5. Хахановський В. Г., Гуцалюк М.В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. Криміналістичний вісник. 2019. № 1 (31). С. 13–19.

6. Regulation (EU) 2023/1543 – adopted by the co-legislators on 12 July 2023 – concerning European Production Orders and European Preservation Orders for electronic evidence (e-evidence) in criminal proceedings and for the execution of custodial sentences following criminal proceedings. An official website of the European Union. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (дата звернення: 12.10.2023).

7. Directive 2023/1544 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. An official website of the European Union. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en (дата звернення: 12.10.2023).

8. Ахтирська Н.М. Одержання доказів в електронній формі в світлі Другого додаткового протоколу Конвенції про кіберзлочинність Криміналістика і судова експертиза. Вип. 67. 2022. С. 188–200. URL: <https://doi.org/10.33994/kndise.2022.67.21> (дата звернення: 12.10.2023).

9. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: <https://rm.coe.int/1680a49dab> (дата звернення: 12.10.2023).

REFERENCES

1. Stratehiia kiberbezpeky, zatverdzhena Ukazom Prezydenta Ukrainy. “The cyber security strategy approved by the Decree of the President of Ukraine dated August 26, 2021, No. 447/2021”. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>. (Date of Application: 12.10.2023) [in Ukrainian].

2. Hutsaliuk, M.V., Antoniuk, P.Ye. (2022). Protsesualna spromozhnist vykorystannia elektronnoi (tsyfrovoi) informatsii yak dokazu v kryminalnomu provadzhenni. “Procedural ability to use electronic (digital) information as evidence in criminal proceedings. Information and law”. URL: https://ippi.org.ua/sites/default/files/15_22.pdf. (Date of Application: 12.10.2023) [in Ukrainian].

3. Sirenko, O.V. (2019). Elektronni dokazy u kryminalnomu provadzhenni. Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka). “Electronic evidence in criminal proceedings. International Legal Bulletin: Current Problems of Modernity (Theory and Practice)”. Iss. 14. P. 208-214 [in Ukrainian].

4. Zakon Ukrainy Pro vnesennia zmin do Kryminalnoho protsesualnoho kodeksu Ukrainy ta Zakonu Ukrainy «Pro elektronni komunikatsii» shchodo pidvyshchennia efektyvnosti dosudovoho rozsliduvannia «za hariachymy slidamy» ta protydii kiberatakam». “On amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine ‘On Electronic Communications’ regarding increasing the effectiveness of pretrial investigation ‘on hot tracks’ and countering cyberattacks”: Law of Ukraine dated March 15, 2022, No. 2137-IX. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#n17>. (Date of Application: 12.10.2023) [in Ukrainian].

5. Khakhanovskiy, V.H., Hutsaliuk, M.V. (2019). Osoblyvosti vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh. “Peculiarities of using electronic (digital) evidence in criminal proceedings”. Kryminalistychnyi visnyk. No. 1 (31) P. 13-19 [in Ukrainian].

6. Regulation (EU) 2023/1543 – adopted by the co-legislators on 12 July 2023 – concerning European Production Orders and European Preservation Orders for electronic evidence (e-evidence) in criminal proceedings and for the execution of custodial sentences following criminal proceedings.

© Anheliniuk Anna-Mariia, 2023

DOI (Article): [https://doi.org/10.36486/np.2023.4\(62\).18](https://doi.org/10.36486/np.2023.4(62).18)

An official website of the European Union. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en. (Date of Application: 12.10.2023) [in English].

7. Directive 2023/1544 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. An official website of the European Union. URL: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en. (Date of Application: 12.10.2023) [in English].

8. *Akhtyrskya, N.M.* (2022). Oderzhannia dokaziv v elektronii formi v svitli Druhoho dodatkovoho protokolu Konventsii pro kiberzlochynnist Kryminalistyka i sudova ekspertyza. "Receipt of evidence in electronic form in light of the Second Additional Protocol to the Convention on Cybercrime Forensics and Forensics". Iss. 67. P. 188-200. URL: <https://doi.org/10.33994/kndise.2022.67.21>. (Date of Application: 12.10.2023) [in Ukrainian].

9. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: <https://rm.coe.int/1680a49dab>. (Date of Application: 12.10.2023) [in English].

UDC 343.14:340.13

Anheleniuk Anna-Mariia,Candidate of Juridical Sciences, Senior Researcher,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0001-5947-5105

IMPROVING CRIMINAL PROCEDURAL LEGISLATION FOR COLLECTING ELECTRONIC EVIDENCE

The article emphasizes the importance of collecting electronic evidence in criminal proceedings for investigating crimes. It highlights the features of using electronic evidence in modern conditions, including proving the commission of war crimes.

Within the framework of the comparative method some provisions of legal acts of the national legislation and the European Union, which relate to the collection of electronic evidence and are aimed at improving this process, are presented. Among such legal acts, the following have been analyzed: 1) Ukraine's Cyber Security Strategy, one of the objectives of which is «Pragmatic International Cooperation» and «Effective Counteraction to Cybercrime»; 2) European Union Directive establishing harmonized rules on the identification of designated institutions and appointment of legal representatives for the purpose of collecting electronic evidence in criminal proceedings; 3) Second Additional Protocol to the Convention on Cybercrime.

The author proposes amendments and additions to Articles 544 and 548 of the Criminal Procedure Code of Ukraine to enhance the quality of electronic evidence collection. It is recommended to consolidate the concept of electronic evidence in the provisions of the Criminal Procedure Code, include electronic evidence in the list of sources of law, and supplement and detail the procedure for collecting, recording, and storing electronic evidence. Given the procedure for the functioning of international legal assistance, in particular in proving

© Anheleniuk Anna-Mariia, 2023

DOI (Article): [https://doi.org/10.36486/np.2023.4\(62\).18](https://doi.org/10.36486/np.2023.4(62).18)

Issue 4(62) 2023

<https://naukaipravohorona.com/>

crimes with the help of electronic evidence, it is emphasized that Ukraine should create a legal framework for: 1) direct cooperation with service providers; 2) acceleration of forms of cooperation in the case of disclosure of information about subscribers (traffic); 3) acceleration of mutual assistance in emergency situations; 4) activities related to international cooperation, if not covered by international treaties (for example, organization of videoconferences, joint investigation teams and joint investigations).

Keywords: evidence, collection, legal basis, request, electronic evidence, international legal assistance.

Отримано 21.11.2023