УДК 343.14+343.982 doi: 10.37025/1992-4437/2019-31-1-13

**В. Г. Хахановський,** *доктор юридичних наук, професор*
*Національна академія внутрішніх справ*
**V. Khakhanovskyi,** *DSc (Law), Professor*
*National Academy of Internal Affairs*
**М. В. Гуцалюк,** *кандидат юридичних наук,*
*старший науковий співробітник, доцент*
*Міжвідомчий науково-дослідний центр з проблем боротьби*
*з організованою злочинністю при РНБО України*
**M. Hutsaliuk,** *Ph.D in Law, Senior Researcher, Associate Professor*
*Interdepartmental Scientific Research Center*
*for Combating Organized Crime of the NSDC of Ukraine*

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ (ЦИФРОВИХ) ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ

## THE PECULIARITIES OF DIGITAL EVIDENCE USE IN CRIMINAL PROCEEDINGS

Метою статті є комплексний розгляд науково-методичного та нормативно-правового забезпечення використання електронних (цифрових) доказів у кримінальних провадженнях. У процесі дослідження розкрито сутність електронних (цифрових) доказів та їх значення у сфері забезпечення кібербезпеки. Проаналізовано міжнародні та вітчизняні нормативно-правові документи, в яких визначено такі докази, виявлено деякі неузгодженості, що стосуються розглядуваних питань. Обґрунтовано необхідність дотримання певних процедур вилучення та дослідження електронних (цифрових) доказів під час кримінальних проваджень і використання при цьому спеціальних знань. Наголошено, що виявлення та вилучення електронних (цифрових) доказів може проводити слідчий, інспектор-криміналіст Національної поліції в межах слідчих (розшукових) дій: під час огляду місця події, обшуку тощо. Констатовано, що, зважаючи на специфіку електронних (цифрових) доказів, до цієї роботи можуть залучатися працівники Департаменту кіберполіції Національної поліції, Експертної служби МВС України, науково-дослідних установ Міністерства юстиції України та ін. Засвідчено, що спеціальні знання в сфері цифрових доказів застосовують у лабораторних умовах, проводячи комп'ютерно-технічні експертизи. Застосування комплексного системного підходу до вирішення завдань дослідження, а також таких наукових методів, як прогнозування, синтез, аналіз, порівняння та узагальнення дали змогу отримати достовірні результати та висновки.

*Ключові слова:* електронні (цифрові) докази; кібербезпека; дані про рух інформації; спеціальні знання; кримінальне провадження; комп'ютерно-технічна експертиза.

Целью статьи является комплексное рассмотрение научно-методического и нормативно-правового обеспечения использования электронных (цифровых) доказательств в уголовных производствах. В процессе исследования раскрыта сущность электронных (цифровых) доказательств и их значение в сфере обеспечения кибербезопасности. Проанализированы международные и отечественные нормативно-правовые документы, в которых даны определения таким доказательствам, выявлены некоторые несогласованности, касающиеся рассматриваемых вопросов. Обоснована необходимость соблюдения определенных процедур изъятия и исследования электронных доказательств в уголовных производствах и использования при этом специальных знаний. Отмечено, что обнаружение и изъятие электронных (цифровых) доказательств может проводить следователь, инспектор-криминалист Национальной полиции в рамках следственных

(розыскных) действий: во время осмотра места происшествия, обыска и т. п. Констатировано, что с учетом специфики электронных (цифровых) доказательств к этой работе могут привлекаться работники Департамента киберполиции Национальной полиции, Экспертной службы МВД Украины, научно-исследовательских учреждений Министерства юстиции Украины и др. Подтверждено, что специальные знания в сфере цифровых доказательств применяют в лабораторных условиях, проводя компьютерно-технические экспертизы. Применение комплексного системного подхода к решению задач исследования, а также таких научных методов, как прогнозирование, синтез, анализ, сравнение и обобщение позволили получить достоверные результаты и выводы.

*Ключевые слова:* электронные (цифровые) доказательства; кибербезопасность; данные о движении информации; специальные знания; уголовное производство; компьютерно-техническая экспертиза.

The purpose of the article is to overview scientific, methodological and regulatory support for the use of electronic (digital) evidence in criminal proceedings. The research reveales the essence of electronic (digital) evidence and their value in cybersecurity. National and international regulatory documents, in wich such evidence was defined, were analyzed; there were found some inconsistencies in them on the researched issues. The need for adherence to certain procedures for the seizure and research of electronic (digital) evidence during criminal proceedings, together with the use of special knowledge is justified by the authors of the article. It is emphasized that detection and seizure of electronic (digital) evidence can be carried out by investigator or forensic inspector of the National Police of Ukraine within the framework of investigative actions (in particular, during the inspection of the crime scene, perquisition, etc.) It is also stated, that concidering the specificity of electronic (digital) evidence, employees of the Cyberpolice Department of the National Police of Ukraine, representatives of the Expert Service of the Ministry of Internal Affairs of Ukraine, specialists of research institutions of the Ministry of Justice of Ukraine and others may be involved in this work. It has been proven, that special knowledge in the field of digital evidence are applied in laboratory conditions during conducting computer-technical expertise. The use of a comprehensive systematic approach, as well as such scientific methods as forecasting, synthesis, analysis, comparison and generalization, provided reliable results and conclusions in the researched issues.

Keywords: electronic (digital) evidence; cybersecurity; data about the movement of information; special knowledge; criminal proceedings; computer-technical expertise.

Цифрові технології активно втілюються у повсякденне життя. А отже урядові установи, банки, торговельні організації, окремі громадяни дедалі більше залежать від надійної роботи інформаційних інфраструктур, поєднаних глобальною мережею Інтернет. Проте зі збільшенням кількості користувачів цієї мережі постійно виникають загрози протиправного використання інформаційних технологій. Відповідно необхідною умовою стабільного функціонування сучасних інформаційних сервісів є їх надійний кіберзахист (Bychkova et al., 2019, s. 15). Суспільство має бути впевнене в тому, що на кіберзлочинців чекає викриття та заслужене покарання.

Успішне розслідування кіберзлочинів неможливе без отримання (збирання) електронних (цифрових) доказів*, на яких ґрунтується доказова база для ухвалення вмотивованих і справедливих рішень. Крім того, такими доказами дедалі частіше послуговуються під час розслідування традиційних злочинів.

Окремі аспекти використання електронних (цифрових) доказів під час розслідування кримінальних правопорушень вивчали, зокрема, В. Д. Гавловський, Ю. Ю. Орлов, Д. М. Цехан, С. С. Чернявський. У цьому напрямі працювали й закордонні дослідники, такі як А. Сегер (Seger A.), Н. Джонс (Nigel Jones), С. Мейсон (S. Mason), Д. Сенг (D. Seng), Г. Кім, С. Лі (S. Lee) та ін. (див., наприклад, Mason, 2016; Mason, & Seng, 2017; Kim, & Lee, 2005). Разом із тим, зважаючи на новизну проблеми, є нагальна потреба комплексного дослідження науково-методичного та нормативно-правового забезпечення викори-

* Терміни «електронні докази», «цифрові докази», «докази в електронній формі» в межах цієї статті застосовуються як синоніми.

стання таких доказів у кримінальних провадженнях, що й становить мету цієї статті та зумовлює актуальність обраної тематики.

Слід наголосити, що промислова розробка засобів для аналізу електронних доказів активно розвивається з початку 2000-х рр. Тоді й вийшов друком перший номер журналу «Digital investigation» («Цифрові розслідування»), в якому висвітлювалися різноманітні технологічні рішення та наукові пропозиції у цій сфері.

Вирізняють докази в електронній формі, що багато в чому схожі з традиційними, такі унікальні характеристики:

вони, як правило, невидимі «неозброєним оком», а тому для їх виявлення послуговуються спеціальним програмним та апаратним інструментарієм;

також вони здебільшого нестійкі до впливу фізичних чинників, оскільки легко модифікуються, знищуються тощо;

їх відносно легко копіювати, найчастіше не втрачаючи якості.

Тому вбачається слушною думка М. М. Соколова, що «наділення електронних доказів самостійним процесуальним статусом та розроблення їх загального визначення сприятимуть установленню дійсних обставин справи та повному й всебічному з'ясуванню обставин справи» (Sokolov, 2017).

У Конвенції про кіберзлочинність (2001 р.), яку ратифіковано із застереженнями Законом України від 7 вересня 2005 № 2824-IV, поняття електронного доказу не окреслене, проте у цьому документі подано кілька інших, пов'язаних з ним визначень, а саме:

комп'ютерна система – будь-який пристрій чи група взаємно поєднаних або пов'язаних пристроїв, один чи більше з яких відповідно до певної програми виконує автоматичне оброблення даних;

комп'ютерні дані – будь-яке представлення фактів, інформації або концепцій у формі, придатної для оброблення в комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою;

дані про рух інформації – будь-які пов'язані з комунікацією за допомогою комп'ютерної системи комп'ютерні дані, створені комп'ютерною системою, що становила частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги.

Згідно зі ст. 14 цієї Конвенції кожна сторона вживає таких законодавчих та інших заходів, які можуть бути необхідні для визначення повноважень і процедур з метою конкретних кримінальних розслідувань, застосовує такі повноваження і процедури для збирання доказів в електронній формі щодо кримінального правопорушення (*Konventsiia pro kiberzlochynnist,* 2001).

Для імплементації Конвенції про кіберзлочинність в Україні група експертів Ради Європи ще в 2016 р. надала відповідні рекомендації щодо врегулювання застосування електронних доказів у кримінальному судочинстві, але в процесі вдосконалення норм чинного законодавства вони до сьогодні так і не були використані.

Зокрема в Україні положення Конвенції про кіберзлочинність щодо процедурних питань збереження комп'ютерних даних та розкриття даних про рух інформації, попри завдання, поставлене рішенням РНБО України від 29 грудня 2016 р. № 32 щодо внесення в установленому порядку на розгляд Верховної Ради України законопроектів щодо імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 р. № 2824-IV, та запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі опера-

тивно-розшукової діяльності (*Pro rishennia Rady,* 2016), досі не імплементовано повним обсягом.

З огляду на те, що сьогодні більша частина світової торгівлі здійснюється онлайн, важливим елементом цього процесу є відповідний ступінь визначеності щодо прийняття, оброблення та юридичного визнання електронних даних, які поширюються кіберпростором, оминаючи державні кордони. Тому в 2016 р. англійські вчені запропонували ухвалити Міжнародну конвенцію з електронних доказів (Mason, 2016), активне обговорення якої триває.

В Україні як юридичну категорію електронні докази започатковано в 2017 р. у Цивільному, Господарському процесуальних кодексах України (далі – ЦПК України, ГПК України) та Кодексі адміністративного судочинства України (далі – КАС України). Натепер накопичено певну судову практику їх використання (Studennykov, 2019).

Так, згідно зі ст. 100 ЦПК України, ст. 96 ГПК України та ст. 99 КАС України електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи, зокрема, електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, наприклад, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (у тому числі в Інтернеті).

Задовольняючи великий попит працівників правоохоронних органів (слідчих, оперативних підрозділів, працівників Експертної служби МВС та ін.), група науковців розробила методичні рекомендації щодо методів використання електронних (цифрових) доказів (Hrebeniuk et al., 2017).

Водночас дотепер поняття «електронні докази» не визначено Кримінальним процесуальним кодексом України (далі – КПК України), що на практиці незрідка ускладнює їх визнання належними та допустимими. А отже убачається доцільним внести зміни до КПК України, доповнивши, зокрема, § 4 «Речові докази і документи» гл. 4 «Докази і доказування» ст. $98^1$ у такій редакції:

*«Стаття $98^1$. Електронні докази*

*Електронними доказами є інформація в електронній (цифровій) формі, що отримана в передбаченому цим Кодексом порядку та має значення для кримінального провадження.*

*Електронні докази отримують за допомогою електронних пристроїв із комп'ютерних носіїв інформації, комп'ютерних мереж, у тому числі через Інтернет.».*

Певні неузгодженості трапляються і через нерозуміння різниці між електронним документом та електронним доказом, наслідком чого є відмова суду приймати до розгляду, наприклад, електронне листування, оскільки бракує обов'язкових реквізитів. Крім того, через відсутність відповідної процедури незрозуміло, яким чином електронний документ, навіть засвідчений електронним підписом, перевіряють перед поданням до суду, що потребує певної судової експертизи або друкування на папері інформації з бази даних, загальний обсяг якої може сягати десятків томів. Тому крім надання визначення електронного доказу в КПК України, на нашу думку, слід додатково, можливо в підзаконних нормативних актах, визначити порядок роботи з електронними доказами, зокрема окреслити необхідні носії інформації, докази з яких суддя зможе проаналізува-

ти, програмне забезпечення для такого аналізу та обумовити, за потреби, інші технічні і технологічні аспекти.

У ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», розробленому Технічним комітетом стандартизації «Банківські та фінансові системи і технології» Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ»), цифровий доказ визначений як інформація або дані, збережені або передані в бінарному вигляді, на які можна покладатися як на докази.

Наказом ДП «УкрНДНЦ» «Про прийняття національних нормативних документів, гармонізованих з європейськими та міжнародними нормативними документами, скасування національних нормативних документів, змін до національних нормативних документів» від 6 грудня 2017 р. № 400 цей стандарт з 1 січня 2019 р., а відповідно й настанови набули чинності.

Запровадження цього стандарту, який надає настанови щодо специфічної діяльності з оброблення потенційних цифрових доказів для підтримання їх цілісності, щоб забезпечити їх допустимість у законодавчих та дисциплінарних судових процесах, а також в інших інстанціях, потребує, зазначено у вступній його частині, узгодження з національними законами, правилами і нормативними документами. Проте деякі терміни, використані у цьому стандарті, в кримінальному судочинстві України не застосовуються, серед них, зокрема, «здобуття» (acquisition) як процес створення копії даних у межах визначеного алгоритму (ідентифікація, збирання, здобуття, збереження), який доцільно замінити на фіксацію. Ці та інші неузгодженості з кримінальним процесуальним законодавством України ускладнюють використання стандарту. Не сприяє його повноцінному впровадженню й те, що про нього через певні обмеження (надається він лише зацікавленим особам і тільки на платних умовах, забороняється його копіювати і поширювати навіть в електронному вигляді) нічого не знають у практичних підрозділах.

У зазначеному стандарті йдеться і про компетентних осіб, які пройшли відповідне навчання та «мають достатнє технічне та законодавче розуміння для належного оброблення потенційних цифрових доказів». У вітчизняній теорії кримінального процесу та криміналістики це розуміють як використання спеціальних знань.

Певні непорозуміння пов'язані і з тим, що через специфічність цифрову інформацію, слушно зазначає Д. М. Цехан, складно віднести, дотримуючись теорії кримінального процесу, до певної групи доказів. А тому науковець пропонує започаткувати категорію цифрового доказу, під яким розуміти фактичні дані в цифровій (дискретній) формі, зафіксовані на будь-якому типі носія і доступні для сприйняття людиною після оброблення ЕОМ, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (Tsekhan, 2013, s. 259).

Виявляти та вилучати такі докази в межах слідчих (розшукових) дій (зокрема під час огляду місця події, обшуку тощо) можуть слідчий, інспектор-криміналіст Національної поліції. З огляду на їх специфіку до цієї роботи залучають працівників Департаменту кіберполіції Національної поліції, Експертної служби МВС України, науково-дослідних установ Міністерства юстиції України. Досліджують електронні (цифрові) докази в лабораторних умовах під час комп'ютерно-технічної експертизи.

Як засвідчує практика, через певну некомпетентність трапляються непоодинокі випадки вилучення з місць події значної кількості комп'ютерної техніки та носіїв інформації, що жодним чином не стосуються справи, спричиняючи тим самим тривале (до кількох років) проведення експертизи та блокування роботи експертів.

*Висновки*. Термінологічний апарат у сфері електронних (цифрових) доказів у межах вітчизняного законодавства потребує узгодження для його гармонізації з європейськими та міжнародними нормами. До того ж на часі адаптування ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» до чинного законодавства України, а також прискорення імплементації положень Конвенції Ради Європи «Про кіберзлочинність» в частині обов'язкового зберігання та надання на вимогу правоохоронних органів операторами та провайдерами телекомунікацій необхідної для розслідування кіберзлочинів інформації. При цьому варто передбачити вивчення методології роботи з цифровими доказами при підготовці фахівців і забезпечити широке її використання у практичній діяльності правоохоронних органів, прокуратури та судів.

**References**


Bychkova, S. S., Volokh, O. K., Havlovskyi, V. D., Hrebeniuk, M. V., Hutsaliuk, M. V., Demydenko, V. O. … Khakhanovskyi, V. H., Tsyplynskyi, Yu. I. (2019). *Naukovo-praktychnyi komentar Zakonu Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy»*. Kyiv: Natsionalna akademiia prokuratury Ukrainy.

Hrebeniuk, M. V., Havlovskyi, V. D., Hutsaliuk, M. V., Khakhanovskyi, V. H., Stepanets, D. S., Kyrychok, V. M. … Samoilov, S. V. (2017). *Vykorystannia elektronnykh (tsyfrovykh) dokaziv u kryminalnykh provadzhenniakh:* metod. rekomendatsii. Kyiv: MNDTs pry RNBO Ukrainy. 76 s.

Kim, H., & Lee, S. (2005). Digital evidence collection process in integrity and memory information gathering. DOI: 10.1109/SADFE.2005.9.

Konventsiia pro kiberzlochynnist. (2001). Uziato z https://zakon.rada.gov.ua/laws/show/994_575.

Mason, S. (2016). A Convention on Electronic Evidence: helping to provide for certainty in international trade. doi: https://doi.org/10.14296/deeslr.v13i0.2321.

Mason, S., & Seng, D. (2017). Electronic Evidence: Fourth Edition. doi: 10.14296/517.9781911507079.

Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 r. «Pro zahrozy kiberbezpetsi derzhavy ta nevidkladni zakhody z yikh neitralizatsii». Ukaz Prezydenta Ukrainy № 32. (2017). Uziato z http://www.rnbo.gov.ua/documents/437.html.

Sokolov, M. (2017). «Tsyfrovi» arhumenty. Uziato z https://zib.com.ua/ua/print/130861-yak_uregulovano_elektronni_dokazi_v_novih_procesualnih_kodek.html.

Studennykov, S. (2019). Elektronni dokazy v protsesualnomu pravi: yak tse pratsiuie v ukrainskykh realiiakh. *Sudebno-yurydycheskaia hazeta*. 8 apr. Uziato z https://sud.ua/ru/news/publication/138354-elektronni-dokazi-v-protsesualnomu-pravi-yak-tse-pratsyuye-v-ukrayinskikh-realiyakh.

Tsekhan, D. M. (2013). Tsyfrovi dokazy: poniattia, osoblyvosti ta mistse u systemi dokazuvannia. *Naukovyi visnyk Mizhnarodnoho humanitarnoho un-tu* (s. 256–260).


**Список використаних джерел**


Бичкова, С. С., Волох, О. К., Гавловський, В. Д., Гребенюк, М. В., Гуцалюк, М. В., Демиденко, В. О. … Хахановський, В. Г., Циплинський, Ю. І. (2019). *Науково-практичний коментар Закону України «Про основні засади забезпечення кібербезпеки України»*. Київ: Національна академія прокуратури України.

Гребенюк, М. В., Гавловський, В. Д., Гуцалюк, М. В., Хахановський, В. Г., Степанець, Д. С., Киричок, В. М. … Самойлов, С. В. (2017). *Використання електронних (цифрових) доказів у кримінальних провадженнях:* метод. рекомендації. Київ: МНДЦ при РНБО України. 76 с.

Kim, H., & Lee, S. (2005). Digital evidence collection process in integrity and memory information gathering. DOI: 10.1109/SADFE.2005.9.

Конвенція про кіберзлочинність. (2001). Узято з https://zakon.rada.gov.ua/laws/show/994_575.

Mason, S. (2016). A Convention on Electronic Evidence: helping to provide for certainty in international trade. doi: https://doi.org/10.14296/deeslr.v13i0.2321.

Mason, S., & Seng, D. (2017). Electronic Evidence: Fourth Edition. doi: 10.14296/517.9781911507079.

Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації». Указ Президента України № 32. (2017). Узято з http://www.rnbo.gov.ua/documents/437.html.

Соколов, М. (2017). *«Цифрові» аргументи.* Узято з https://zib.com.ua/ua/print/130861-yak_uregulovano_elektronni_dokazi_v_novih_procesualnih_kodek.html.

Студенников, С. (2019). Електронні докази в процесуальному праві: як це працює в українських реаліях. *Судебно-юридическая газета.* 8 апр. Узято з https://sud.ua/ru/news/publication/138354-elektronni-dokazi-v-protsesualnomu-pravi-yak-tse-pratsyuye-v-ukrayinskikh-realiyakh.

Цехан, Д. М. (2013). Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного ун-ту* (с. 256–260).

Стаття надійшла до редакції 29.04.2019