ISSN 2072–8670 (Print)
НАУКА І ПРАВООХОРОНА
NAUKA I PRAVOOKHORONA
DOI (Issue): https: //doi.org/10.36486/np.2022.3(57)
Issue 3(57) 2022
УДК 343.140.01

Пономаренко Алла Василівна,
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник
ДНДІ МВС України, м. Київ, Україна
ORCID ID 0000-0002-6271-4485

ЗБИРАННЯ СТОРОНОЮ ОБВИНУВАЧЕННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ: ПРОБЛЕМИ СЬОГОДЕННЯ

Стаття присвячена дослідженню окремих правових проблем збирання стороною обвинувачення електронних доказів у кримінальному процесі України. Проаналізовано правові норми, якими регулюється збирання доказів, з метою виявлення колізій та неузгодженостей. Встановлено, що в КПК України відсутні дефініції "електронний доказ", у зв'язку з чим ці докази розглядаються як документи; не визначено порядок залучення спеціаліста до участі у процесуальних діях та підтвердження наявності у нього спеціальних знань і навичок. Зазначено про існування проблем під час огляду та фіксації електронних документів, розміщених у мережі Інтернет, недосконаліть положення щодо витребування електронних документів як способу збирання доказів. Обґрунтовується необхідність удосконалення положення, що стосується витребування електронних документів як способу збирання доказів.

Ключові слова: *електронний документ, фізичний носій інформації, мережа Інтернет; хмарні сервіси зберігання інформації, витребування електронних документів.*

Динамічний розвиток інформаційно-цифрових, а також комунікаційних технологій суттєво вплинув на сферу кримінальних процесуальних відносин в Україні. Завдяки технологічному прогресу в кримінальному процесі нашої держави з'явився новий вид доказів – електронний, який у порівнянні із класичним розумінням доказів має певні особливості збирання та використання у кримінальному проваджені.

Новизна зазначеного джерела доказування, недосконаліть нормативного регулювання та матеріально-технічної бази призвели до того, що під час проведення окремих слідчих (розшукових) та інших процесуальних дій, спрямованих на збирання та дослідження електронних доказів, сторона обвинувачення зазнає певних проблем, що ускладнюють доказування винуватості особи у скоєнні відповідного кримінального правопорушення та притягнення її до кримінальної відповідальності

Окремі питання збирання електронних доказів у кримінальному процесі України досліджували В.І. Завидняк, В.В. Лисенко, О.П. Метелев, А.В. Ратнова, О.С. Тарасенко, Є.С. Хижняк та інші. Однак в науці та практиці досі залишається багато дискусійних питань щодо збирання електронних доказів стороною обвинувачення, що потребує додаткового вивчення.

© Ponomarenko Alla, 2022

DOI (Article): https: //doi.org/10.36486/np.2022.3(57).18

Метою статті є дослідження та аналіз проблемних питань, що виникають у сторони обвинувачення під час збирання електронних доказів у кримінальному процесі України.

Одним із головних структурних елементів процесу доказування, від якого залежить подальша оцінка доказів, є збирання (формування) доказів. Цей процес полягає у здійсненні комплексної діяльності з виявлення, витребування, отримання, закріплення, збереження доказів у визначеному процесуальним законом порядку. Недотримання процесуальної форми збирання доказів може призвести до їх втрати чи визнання їх недопустимими у суді.

У кримінальному процесуальному законодавстві України передбачена можливість збору доказів як стороною захисту, так і стороною обвинувачення (слідчим, прокурором). Оскільки основний тягар збирання цих доказів покладено на останніх, то саме їх процесуальна діяльність у вказаній сфері є предметом цього дослідження.

Слідчий, прокурор у межах компетенції, визначеної у Кримінальному процесуальному кодексі України (далі – КПК України), уповноважені здійснювати досудове розслідування кримінальних правопорушень й нести відповідальність за законність та своєчасність здійснення процесуальних дій. Сторона обвинувачення використовує відповідний правовий механізм збирання доказів і здійснює це через проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів і ревізій та актів перевірок, проведення інших процесуальних дій, передбачених нормами кримінального процесуального законодавства (частина друга статті 93 КПК України).

Серед засобів збирання доказів важливе значення мають слідчі (розшукові) дії, які відповідно до статті 223 КПК України спрямовані на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні. Як слушно зауважує Ю.В. Терещенко, саме слідчі (розшукові) дії та їх результати є підґрунтям для побудови доказової бази, їх проведення становить зміст досудового розслідування [1, с. 113–115].

У процесі проведення деяких слідчих (розшукових) дій, практичні працівники правоохоронних органів України стикаються з низкою проблем, пов'язаних зі збиранням електронних доказів. Насамперед це стосується відсутності в КПК України дефініції "електронний доказ", у зв'язку з чим ці докази на підставі частини другої статті 84 та пункту 1 частини другої статті 99 КПК розглядаються як документи. Вищий антикорупційний суд наголосив, що у зв'язку з відсутністю вказаного поняття у КПК України, він "керується положеннями Закону України "Про електронні документи та електронний документообіг", частина перша статті 5 якого містить дефініцію цього джерела доказів та визначає, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа". Цей суд зазначив, що "електронний документ є інформацією, а матеріальний носій, на якому він зберігається, – лише способом фіксування та зберігання вказаної інформації [2].

© Ponomarenko Alla, 2022

За слушним твердженням О.Г. Козицької, електронні докази мають спільні риси з традиційними доказами, але водночас мають низку унікальних характеристик:

1) їх не видно неозброєним оком: вилучити їх подекуди може лише спеціаліст;

2) вони є нестійкими, за певних обставин інформація в пам'яті пристрою може бути змінена або втрачена;

3) їх можна копіювати без втрати якості необмежену кількість разів, і будь-яка наступна копія не буде відрізнятися від оригіналу;

4) можуть як бути створені людиною, так і бути результатом функціонування інформаційної системи;

5) вільно переміщуються в електронній мережі без технічного носія та не мають нерозривного зв'язку з матеріальним носієм;

6) потребують специфічного порядку збирання, перевірки й оцінки [3, с. 420].

Окрім відсутності понятійного апарату, слідчі, прокурори мають певні труднощі під час дослідження змісту електронних доказів. Зокрема, це стосується електронних документів, які зберігаються на фізичних носіях інформації, у відкритому доступі в мережі Інтернет, а також у хмарних сервісах зберігання інформації тощо.

Г. Чигрина аргументовано стверджує, що для більшості суб'єктів доказування (слідчих, прокурорів) проблемою є виявлення та вербалізація у процесуальних документах та інших матеріалах кримінального провадження (протоколах обшуку, огляду місця події, допиту; постановах про призначення експертиз, клопотаннях, листах-запитах тощо) процесів, пов'язаних зі збиранням та використанням електронних документів та іншої комп'ютерної інформації [4 с. 135].

Так, під час проведення огляду електронних документів виникають труднощі, зумовлені тим, що цей документ є певним комп'ютерним кодом, який може бути прочитаний лише за допомогою відповідного обладнання та програмного забезпечення. З цього приводу А.В. Коваленко звертає увагу на те, що будь-які дії з електронними документами мають здійснюватися за допомогою сертифікованого службового обладнання з використанням ліцензійного програмного забезпечення. Використання несертифікованого обладнання або неліцензійного програмного забезпечення може призвести до викривлення інформації, отриманої з електронного документа через апаратні та/або програмні збої і помилки [5, с. 184].

Складність проведення огляду електронних документів полягає також у тому, що досить часто необхідно залучати спеціаліста чи експерта, які мають спеціальні знання у сфері комп'ютерних технологій. Спеціаліст може надати безпосередню технічну допомогу в огляді та вилученні комп'ютерної техніки, допомогти належним чином описати в протоколі кожний оглянутий пристрій, при необхідності зберегти чи розкодувати, а у деяких випадках вибрати найбільш доцільну програму, яка допоможе представити інформацію у необхідній формі. Водночас питання щодо залучення спеціаліста до участі у процесуальних діях на досудовому слідстві є досить дискусійним.

Насамперед це пов'язано з відсутністю в КПК України порядку залучення спеціаліста, що може викликати сумніви у допустимості висновку спеціаліста як джерела доказів. Також підлягає критиці стаття 71 КПК України, у якій визначено, що спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними

© Ponomarenko Alla, 2022
DOI (Article): https: //doi.org/10.36486/np.2022.3(57).18

знаннями та навичками застосування технічних або інших засобів. При цьому законодавець не уточнює, яким чином підтверджується наявність знань і навичок спеціаліста. За слушним твердженням В. Клочкова, І. Старости, відсутність чіткого визначення "спеціаліста" може стати підґрунтям зловживання з боку сторони обвинувачення таким процесуальним інструментом. Для отримання такого висновку може залучатись особа, яка насправді не є спеціалістом (перевірити його знання і навики можливості не має); спеціаліст може залучатись в тих випадках, коли насправді у ньому необхідності не має, таким чином слідчий або прокурор можуть безпідставно сформувати собі додаткову доказову базу [6].

З цього приводу ми поділяємо думку Г. Чигриної про те, що з метою усунення непорозумінь щодо фаховості спеціаліста, які можуть виникнути під час подальшого судового розгляду кримінального провадження, при вирішенні питання про допуск спеціаліста до участі у процесуальних діях на досудовому слідстві необхідно до матеріалів справи долучати копії дипломів та свідоцтво про ІТ-освіту, а також виписки із трудової книжки цього спеціаліста за останні 3–5 років, завірені підписами відповідальних осіб та печаткою роботодавця [4, с. 136]. Отже, зазначене вказує на необхідність законодавчого урегулювання питання щодо залучення спеціаліста до участі у процесуальних діях стосовно збирання стороною обвинувачення електронних доказів.

З метою пошуку та вилучення електронних документів для формування доказової бази, огляду підлягають такі об'єкти:

1) фізичні носії інформації (моноблоки, мобільні телефони, комп'ютери, ноутбуки, флеш-накопичувачі, жорсткі диски, сервери);

2) мережа Інтернет;

3) хмарні сервіси зберігання інформації.

Огляд електронних документів, розміщених на фізичному носії інформації, здійснюється, як правило, після їх вилучення під час проведення обшуку. При цьому, як слушно зауважує Є.С. Хижняк, огляд та дослідження фізичного носія електронного документа не є дослідженням самого електронного документа. У такому разі фізичний носій може бути лише речовим доказом [7, с. 81]. З цього приводу Верховний суд України у постанові від 10 вересня 2020 року у справі № 751/6069/19 звертає увагу на те, що "матеріальний носій – лише спосіб збереження інформації, який має значення тільки коли електронний документ виступає речовим доказом. Головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення" [8].

Окрему увагу варто приділити огляду електронних документів, розміщених в мережі Інтернет. Останнім часом такі документи стають одним з головних джерел інформації, що має орієнтуюче або доказове значення під час розслідування кримінальних проваджень. Існує проблема процесуальної фіксації цих документів як доказів. Це пов'язано з тим, що інформація, яка розповсюджується через вебсайт в мережі Інтернет, може бути легко змінена, видалена або відредагована власником, або інтернет-провайдерами, в розпорядженні яких знаходяться сервери.

© Ponomarenko Alla, 2022

При цьому доведення модифікації такої інформації практично неможливе, оскільки найчастіше сервери, на яких розміщені електронні документи, розташовані закордоном, що значно ускладнює процес отримання доступу до них. Така ж ситуація складається з хмарними сховищами, в яких дані зберігаються на численних розподілених у мережі серверах, наданих у користування клієнтам зазвичай третьою стороною. На відміну від моделі збереження даних на власних серверах, дані зберігаються і обробляються в так званій "хмарі", яка, по суті, є одним великим віртуальним сервером.

Найголовнішим завданням сторони обвинувачення при отриманні електронних доказів з мережі Інтернет чи з хмарних сервісів зберігання інформації є своєчасне закріплення фактичних даних для подальшої їх оцінки та використання як джерела доказів. Проте, як свідчить правозастосовна практика, суб'єкти доказування, маючи навички володіння комп'ютером на рівні простого користувача, відчувають труднощі у роботі з мережевими ресурсами, їх спеціалізованою термінологією, механізмом роботи та грамотним відображенням у процесуальній формі.

На наше переконання, під час роботи із зазначеними джерелами інформації суб'єктам доказування доцільно при фіксації інформації з Інтернет-сайтів зазначати час та часовий пояс; з'ясовувати не особистість користувача, а облікові дані апаратної частини і програмного забезпечення відповідного джерела поширення інформації; при вилученні інформації із серверів вилучати лише необхідні дані, а не весь дисковий масив.

У протоколі огляду вебсторінки в мережі Інтернет обов'язково мають вказуватись реквізити електронного документа, його призначення, стислий зміст та інші викладені в ньому обставини, які мають значення для розслідування. До протоколу проведення слідчих (розшукових) дій також можуть додаватись роздруківки чи скріншоти екрану як додатки. Роздруківка Інтернет-сторінки, файлу полягає у друці їх вмісту на папері. Паперова роздруківка, окрім інформації про зміст електронного документа, може також містити дату, час друку, інтернет-адресу сторінки, кількість друкованих сторінок, їх нумерацію тощо.

Наступною слідчою (розшуковою) дією, яка є важливим засобом збирання електронних доказів, є обшук, метою якого є відшукання та вилучення речей і документів, які мають значення для кримінального провадження.

Донедавна на законодавчому рівні не було врегульоване питання щодо доступу слідчого, прокурора до змісту кореспонденції, інших персональних даних, які зберігаються в мобільних пристроях, комп'ютерах. Слідча й судова практика застосовували різні варіанти, у тому числі через санкціонування вилучення телефонів під час обшуку, через накладення арешту на тимчасово вилучене майно, через призначення експертизи або й через доступ до змісту телефону без спеціального санкціонування. Проте після 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 [9], питання обшуку комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку було урегульовано в межах загальної процедури обшуку житла або іншого володіння особи.

© Ponomarenko Alla, 2022
DOI (Article): https: //doi.org/10.36486/np.2022.3(57).18

Необхідно звернути увагу на те, що у попередній редакції статті 236 КПК України слідчий, прокурор під час проведення обшуку мав право відкривати закриті приміщення, сховища, речі, якщо особа, присутня при обшуку, відмовляється їх відкривати або обшук здійснюється за відсутності відповідних осіб. Після внесення змін до статті 236 КПК України законодавець надав право слідчому, прокурору долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх відкрити чи зняти (деактивувати) систему логічного захисту або обшук здійснюється за відсутності осіб, зазначених у частині третій цієї статті. Крім того, слідчий, прокурор мають право при виявленні доступу чи можливості доступу до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, яка на них міститься, має значення для встановлення обставин у кримінальному провадженні, здійснювати пошук, виявлення та фіксацію комп'ютерних даних на місці проведення обшуку.

Звертаємо увагу на те, що особи, які володіють інформацією про зміст комп'ютерних даних та особливості функціонування комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку, можуть повідомити про це слідчого, прокурора під час здійснення обшуку, відомості про що вносяться до протоколу обшуку (частина шоста статті 236 КПК України).

Окрім проведення слідчих (розшукових) дій, сторона обвинувачення може збирати електронні докази шляхом їх витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб. Водночас на практиці трапляються випадки, коли під час здійснення досудового розслідування фізична або юридична особа відмовляє у наданні запитуваних документів. Замість таких документів сторона обвинувачення отримує на свою вимогу лист про згоду їх видати, але лише на підставі ухвали слідчого судді, суду про тимчасовий доступ до речей і документів. Така ситуація зумовлена недосконалістю положень КПК України в частині правового регулювання порядку витребування та отримання стороною обвинувачення речей, документів та їх копій, що призводить до затягування розслідування.

Ми поділяємо думку А.В. Ратнової про те, що витребування електронних документів має здійснюватися у формі вимоги про витребування документів та речових доказів з дотримання вимог КПК України та надсилатись до належного суб'єкта супровідним листом. Крім того, доцільно запровадити строки розгляду такої вимоги стороною, у якої витребовуються документи та санкції у випадку необґрунтованої відмови чи неповного надання відповіді [10, с. 128]. Вважаємо, невиконання такої вимоги є підставою для звернення сторони обвинувачення з клопотанням про застосування інших заходів забезпечення кримінального провадження.

В Україні на державному рівні проголошено та здійснюються різноманітні заходи щодо цифрового розвитку, цифрових трансформацій і цифровізації суспільних відносин. З цією метою, в роботу органів публічної влади впровад-

© Ponomarenko Alla, 2022

жуються новітні технології, що призвело до започаткування електронного документообігу, електронного кримінального провадження та електронного суду.

Незважаючи на новації, кримінальне процесуальне законодавство України досить повільно реформується, на відміну він інших процесуальних галузей, де, зокрема, широко розвивається інститут електронних доказів. Недосконаліть вітчизняного нормативного регулювання питань збирання слідчим, прокурором електронних доказів перешкоджає ефективному розслідуванню кримінальних правопорушень, що підриває довіру населення до правоохоронних органів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Терещенко Ю.В*. Слідчі (розшукові) дії як різновид процесуальних дій. Митна справа. 2014. № 1 (21). С. 112–117.

2. Ухвала Вищого антикорупційного суду від 01.07.2021 у справі № 707/146/17. URL: https://reyestr.court.gov.ua/Review/98133827 (дата звернення: 03.08.2022).

3. *Козицька О.Г*. Щодо поняття електронних доказів у кримінальному провадженні. Юридичний науковий електронний журнал. 2020. № 8. С. 418–421.

4. *Чигрина Г*. Електронні документи: залучення спеціаліста до збирання та використання під час кримінального провадження URL: http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf (дата звернення: 03.08.2022).

5. *Коваленко А.В*. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. Вісник Національної академії правових наук України. Харків: Право. 2017. № 1 (88). С. 182–191.

6. *Клочков В., Староста І*. Про деякі проблеми досудового розслідування кримінальних проступків. URL: http://klochkov.partners/ ua/news/o-nekotoryh-problemah-dosudebnogo-rassledovaniya-ugolovnyhprostupkov/ (дата звернення: 03.08.2022).

7. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних правопорушень. Держава та регіони. Серія: Право. 2017. № 4 (58). С. 80–85.

8. Постанова Першої судової палати Касаційного кримінального суду Верховного Суду від 10.09.2020 у справі № 751/6069/19. URL: https://reyestr.court.gov.ua/Review/91722819 (дата звернення: 03.08.2022).

9. 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 15.03.2022 № 2137–IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 03.08.2022).

10. *Ратнова А.В*. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні: дис. ... д-ра філософії. Львів. 2021. 248 с.

REFERENCES

1. *Tereshchenko Yu.V*. (2014). Slidchi (rozshukovi) dii yak riznovyd protsesualnykh dii. Mytna sprava. "Investigative (search) actions as a type of procedural actions". Customs business. No 1 (21). P. 112–117. [In Ukrainian].

2. Ukhvala Vyshchoho antykoruptsiinoho sudu. "Resolution of the High Anti-Corruption Court dated 07/01/2021 in case No 707/146/17". URL: https://reyestr.court.gov.ua/Review/98133827 (Date of Application: 03.08.2022). [In Ukrainian].

3. *Kozytska O.H*. (2020). Shchodo poniattia elektronnykh dokaziv u kryminalnomu provadzhenni. Yurydychnyi naukovyi elektronnyi zhurnal. "Regarding the concept of electronic evidence in criminal proceedings". Legal scientific electronic journal. No 8. P. 418–421. [In Ukrainian].

4. *Chyhryna H*. Elektronni dokumenty: zaluchennia spetsialista do zbyrannia ta vykorystannia pid chas kryminalnoho provadzhennia. "Electronic documents: involvement of a specialist in collection and use during criminal proceedings". URL:http://www.jurnaluljuridic.in.ua/archive/2017/3/30.pdf (Date of Application: 03.08.2022). [In Ukrainian].

5. *Kovalenko A.V*. (2017). Osoblyvosti taktyky ohliadu elektronnykh dokumentiv pid chas dosudovoho rozsliduvannia posiahan na zhyttia ta zdorovia zhurnalista. "Peculiarities of the tactics of

© Ponomarenko Alla, 2022

reviewing electronic documents during the pre-trial investigation of attacks on the journalist's life and health". Bulletin of the National Academy of Legal Sciences of Ukraine. Kharkiv: Pravo. No 1 (88). P. 182–191. [In Ukrainian].

6. *Klochkov V., Starosta I.* Pro deiaki problemy dosudovoho rozsliduvannia kryminalnykh prostupkiv. "About some problems of pre-trial investigation of criminal misdemeanors". URL: http://klochkov.partners/ ua/news/o-nekotoryh-problemah-dosudebnogo-rassledovaniya-ugolovny-hprostupkov/ (Date of Application: 03.08.2022). [In Ukrainian].

7. *Khyzhniak Ye.S.* (2017). Osoblyvosti ohliadu elektronnykh dokumentiv pid chas rozsliduvannia kryminalnykh pravoporushen. "Peculiarities of reviewing electronic documents during the investigation of criminal offenses". State and regions. Series: Law. No 4 (58). P. 80–85. [In Ukrainian].

8. Postanova Pershoi sudovoi palaty Kasatsiinoho kryminalnoho sudu Verkhovnoho Sudu. "Resolution of the First Judicial Chamber of the Criminal Court of Cassation of the Supreme Court dated September 10, 2020 in case No 751/6069/19". URL: https://reyestr.court.gov.ua/Review/ 91722819 (Date of Application: 03.08.2022). [In Ukrainian].

9. 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 pre-trial investigation "on hot tracks" and countering cyberattacks: Law of Ukraine dated 03.15.2022 No 2137–IX". URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (Date of Application: 03.08.2022) [In Ukrainian].

10. *Ratnova A.V.* (2021). Kryminalni protsesualni ta kryminalistychni osnovy vykorystannia elektronnykh dokumentiv u dokazuvanni. "Criminal procedural and forensic basics of using electronic documents in evidence: dissertation". ... Doc. Philosophy. Lviv. 248 p. [In Ukrainian].

UDC 343.140.01

Ponomarenko Alla,
Candidate of Juridical Sciences, Senior Researcher,
Leading Researcher, State Research Institute MIA Ukraine,
Kyiv, Ukraine,
ORCID ID 0000-0002-6271-4485

COLLECTION OF ELECTRONIC EVIDENCE BY THE PROSECUTION SIDE IN THE CRIMINAL PROCESS OF UKRAINE: PROBLEMS OF TODAY

The article is devoted to the study of certain legal problems of the collection of electronic evidence by the prosecution side in the criminal process of Ukraine. The author points out that in the process of conducting some investigative (search) actions, practical workers of law enforcement agencies of Ukraine face a number of problems related to the collection of electronic evidence. First of all, this concerns the absence of a definition of "electronic evidence" in the Criminal Procedure Code of Ukraine. Therefore, these evidences are considered as documents. In addition to the absence of the specified concept, investigators and prosecutors have certain difficulties when studying the content of electronic evidence. This applies to electronic documents stored on physical data carriers, publicly available on the Internet, as well as in cloud storage services, etc.

During the review of electronic documents, difficulties arise due to the fact that this document is a certain computer code that can only be read with the help of the

© Ponomarenko Alla, 2022

appropriate hardware and software. The difficulty of reviewing electronic documents also lies in the fact that quite often it is necessary to involve a specialist or an expert who has certain knowledge in the field of computer technologies.

It is emphasized that the Code of Criminal Procedure of Ukraine does not specify the procedure for involving a specialist to participate in procedural actions, and it does not specify how the specialist's knowledge and skills are confirmed. The author supports the opinion that it is necessary to attach to the case materials copies of diplomas and certificates of IT education, as well as extracts from the work book of this specialist for the last 3–5 years, certified by the signatures of the responsible persons and the seal of the employer.

The author believes that despite digital innovations, the criminal procedural legislation of Ukraine is being reformed quite slowly, unlike other procedural branches where, in particular, the institute of electronic evidence is widely developing. The imperfection of the domestic regulatory regulation of the collection of electronic evidence by investigators and prosecutors hinders the effective investigation of criminal offenses, which undermines the public's trust in law enforcement agencies.

Keywords: electronic document, physical carrier of information, Internet; cloud services for information storage, retrieval of electronic documents.

Отримано 04.10.2022

© Ponomarenko Alla, 2022