САЛМАНОВ Олексій Валерійович,
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та організації
досудового слідства факультету № 1
Харківського національного університету внутрішніх справ
ORCID: https://orcid.org/0000-0001-9421-5085

ЩОДО ПРИНЦИПІВ НАЛЕЖНОСТІ ЦИФРОВИХ (ЕЛЕКТРОННИХ) ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Інформатизація суспільства та розвиток цифрових технологій призвели до необхідності розгляду нового виду доказів у кримінальних справах - цифрових (електронних) доказів, яких раніше не існувало. Складність їх використання в кримінальному судочинстві визначається тим, що вони мають складну технічну природу, включаючи абстрактні технічні та математичні моделі, а також специфічні умови виникнення, існування, копіювання та зберігання. Це ускладнює їхню однозначну класифікацію як матеріальних доказів або документів. Крім того, виникають проблеми з їх візуалізацією та гарантованим зберіганням. Проте в сучасному цифровому світі, який охоплює все більше аспектів суспільного життя, цифрові докази іноді є єдиною можливістю для досягнення справедливості. Тому правильна оцінка цифрових доказів в ході кримінального розслідування, щодо їхньої придатності та допустимості, стає основною метою в процесі доведення обвинувачень. [1].

Відомо, що з точки зору процесуальних норм будь-які інформаційні дані, перш ніж стати доказами, повинні бути оцінені з погляду їхньої придатності, припустимості, повноти та вірогідності. Докази характеризуються своєю вірогідністю та придатністю з точки зору їхнього вмісту, тоді як їхня припустимість та доречність визначаються в рамках процесуальних правил. Для того щоб інформація могла бути визнана доказом, вона повинна відповідати всім цим характеристикам. Без належності будь-якої з цих ознак, вона не може бути прийнята як доказ. [2]. М. Є. Шумило, обгрунтовуючи важливість розуміння доказів як складної юридичної конструкції системного характеру, зазначає, що для кваліфікованої юридичної роботи з доказами необхідно мати спеціальний процесуальний інструмент - юридичну конструкцію "склад доказу". Це допомагає аналізувати інформацію, яка подається на розгляд у суді, з точки зору її юриди-

чних "характеристик" - належності, припустимості, ступеня вірогідності, вагомості, переконливості та визначати можливості та способи її використання для формування та захисту власної юридичної позиції в суді. [3].

У юридичній науці допустимість доказів вважається однією з характеристик процесуальної форми, яка охоплює "сукупність умов, передбачених законодавством для вчинення процесуальних дій, їх послідовність, порядок реєстрації та оформлення процесуальних дій, процесуальні строки". Допустимість доказів стосується їхньої придатності для використання в кримінальному процесі з точки зору їхньої форми, як відмінності від питання їхньої належності, яка відноситься до їхньої змістовної придатності. Діалектика між формою та змістом полягає в тому, що форма набуває значення лише тоді, коли вона відповідає змістовній суті. [4]. Зміст без форми не може існувати. Форма судового доказу є важливою, оскільки залежить від об'єктивних властивостей фактів і обставин, що підлягають доказуванню, проміжних і побічних фактів, які впливають на формування доказів. Вважаэмо, що інститут допустимості доказів відображає пріоритет законодавця, який стоїть перед вибором між встановленням істини за будь-якою ціною та свідомою готовністю зменшити ймовірність досягнення цієї істини, щоб зменшити ризик обвинувачення невинного і обмежити сферу порушення конституційних прав громадян. [5].

Тож ми можемо виділити наступні принципи належності цифрових доказів, а саме:

1. Допустимість цифрових доказів - це завдання першочергового значення. Збір та зберігання доказів повинні відбуватися відповідно до процесуальних норм, які забезпечують їх можливе використання на судовому засіданні. Всупереч тому, наявність помилок та порушень у процесі збору і збереження може призвести до визнання доказів недопустимими.

2. Аутентичність цифрових доказів. Цей принцип гарантує, що дані, які отримані під час проведення надзвичайних ситуацій засобами спеціальної розвідки, повинні бути відповідними справі, і експерт повинен бути в змозі перевірити правдивість цих цифрових даних. Наприклад, перехоплення електронної пошти само по собі не дає достатньої підстави для визнання, що відправником є об'єкт дослідження. Електронного листа може бути надіслано кимось з оточення об'єкта, і підтвердження його автентичності можливе лише шляхом об'єднання різних даних (наприклад, пізніше об'єкт

підтвердив телефонним дзвінком, що саме він відправив це повідомлення). Більше того, повинен бути встановлений зв'язок між повідомленням і обліковим записом користувача або комп'ютером, з якого було відправлено це повідомлення, і особою, яка його відправила. Якщо повідомлення було дійсно відправлено, сліди повинні бути збережені як докази на різних комп'ютерах у різних інтернет-провайдерах, які це підтверджують.

3. Комплетність отриманих цифрових доказів. Цей принцип вимагає, щоб подані цифрові докази представляли повний спектр подій, які мали місце. Наявність чіткої та повної картини подій необхідна для визначення того, яким чином були залишені цифрові сліди. Очевидно, що невивчена частина або неповність доказів може залишити недоліки, що є набагато більш небезпечним, ніж відсутність доказів зовсім. Наприклад, якщо з IP-адреси користувача комп'ютера була здійснена DDoS-атака на державний хост gov.ua, що призвело до збою в роботі державних установ, детальний аналіз цифрових слідів на жорсткому диску комп'ютера розкрив, що сталася інфікування вірусною програмою операційної системи. Це призвело до автоматичної DDoS-атаки, яку виконав комп'ютер без втручання користувача. Пізніше виявилося, що весь пул (окремий сегмент) IP-адрес провайдера в конкретному місці був заражений.

Таким чином, ураховуючи всю різноманітність процесів, які можуть відбуватися на комп'ютері та в телекомунікаційній мережі, досить важливим є завдання щодо знаходження відповідності частини доказів із їх першоджерелом та мати уявлення про всю картину подій, що відбулися.

4. Достовірність отриманих цифрових доказів. Основна ідея цього принципу полягає в тому, що всі зібрані докази повинні бути надійними, і це повністю залежить від методології та інструментів, використаних для отримання цифрових доказів, з основною увагою на використання наукового підходу. Важливо зауважити, що методи, які використовуються, повинні бути достовірними та визнаними в кіберпросторі. Крім того, слід наголосити на важливості дотримання процесуальних процедур та регламентації отримання цифрових доказів.

5. Зрозумілість та обґрунтованість. Цей останній принцип гарантує, що спеціаліст (експерт) на судовому засіданні здатний чітко, зрозуміло та логічно пояснити, які методи він використовував при дослідженні цифрових доказів і як була збережена цілісність даних. Докази мають бути представлені у доступній формі та виглядати правдоподібно.

Отже, ми вважаємо, що наведені характеристики цифрових доказів є засобом гарантування прийняття законних і обґрунтованих процесуальних рішень у кримінальному провадженні, а також засобом захисту прав і свобод громадян, уникнення покарання невинуватих і встановлення вини осіб, які вчинили злочин. Важливо відзначити, що цей перелік не є вичерпним, і дослідження в цьому напрямку є доцільним.

Висновки. В Україні на сьогодні відсутня єдина судова практика щодо допустимості та належності цифрових (електронних) доказів, отриманих як з матеріальних носіїв інформації, так і з мережі Інтернет. Існує актуальна потреба в урегулюванні цього питання як на законодавчому рівні, так і за допомогою відповідних судових роз'яснень. З урахуванням специфіки цифрових (електронних) доказів, забезпечення їхньої достовірності в кримінальному провадженні передбачає оперативність проведення слідчих (розшукових) дій, обов'язкову участь фахівця, фахову підготовку всіх учасників процесу доказування і відмову від порушень рекомендацій щодо роботи з цифровими доказами.

Список використаної літератури: 1. Кримінальний процесуальний кодекс України від 18.04.2010 № 4651-VI (редакція від 05.01.2022). Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text **2.** Закон України «Про адвокатуру та адвокатську діяльність» № 3022-IX від 10.04.2023 (редакція від 03.08.2023). Відомості Верховної Ради (ВВР), 2013, № 27, ст.282. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text **3.** Шумило.М. поняття доказів у кримінальному процесі: пролегомени до розуміння «невловного»... феномену доказового права[The concept of evidence in criminal proceedings: prolegomena to understand the «elusive» phenomenon of evidentiary law] (2015) 3/ Visnyk kryminalnoho sudochynstva Pp.95-103. **4.** Закон України «Про нотаріат» № 3037-IX від 11.04.2023 (Редакція від 09.06.2023) Відомості Верховної Ради України (ВВР), 1993, № 39, ст.383. URL: https://zakon.rada.gov.ua/laws/show/3425-12#Text **5.** Салманов, О. В. Процесуальний порядок проведення слідчих (розшукових) дій, що обмежують недоторканність житла чи іншого володіння особи (Doctoral dissertation, спеціальність 12.00. 09. Харків. 2020)