УДК 343.98
DOI https://doi.org/10.32844/2618-1258.2025.5.44

СУСЛІКОВА І.С.

ПРОБЛЕМИ ДОКАЗУВАННЯ У СПРАВАХ ПРО КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У ФІНАНСОВІЙ СФЕРІ, ВЧИНЕНІ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

PROBABILITY PROBLEMS IN CASES OF CRIMINAL OFFENCES IN THE FINANCIAL SPHERE COMMITTED WITH THE USE OF DIGITAL TECHNOLOGIES

Метою наукової статті є комплексний аналіз проблем доказування у кримінальних провадженнях щодо правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, з урахуванням сучасної слідчої та судової практики, а також обґрунтування науково й практично виважених підходів до вдосконалення процесу збирання, фіксації та оцінки цифрових доказів в умовах цифровізації та воєнного стану**.** Узагальнення теоретичних положень і аналіз судової практики свідчать, що доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, має підвищений рівень складності та істотно відрізняється від доказування у «класичних» фінансових злочинах. Ця специфіка зумовлена цифровою природою доказової інформації, багатоступеневістю фінансових операцій, використанням анонімізованих технологій і транснаціональних інструментів, що ускладнює встановлення персоніфікованого зв'язку між протиправними діями та конкретною особою, а також доведення суб'єктивної сторони кримінального правопорушення. Встановлено, що ключовими проблемами доказування у зазначеній категорії справ є ідентифікація суб'єкта злочину у цифровому середовищі, доведення фактичного контролю над фінансовими та цифровими інструментами, забезпечення допустимості й належності електронних доказів, а також відтворення причинно-наслідкового зв'язку між цифровими діями і заподіяною майновою шкодою. Судова практика, зокрема позиції Верховного Суду, підтверджує необхідність дотримання підвищених стандартів доказування, що вимагає від органів досудового розслідування комплексного поєднання процесуальних, криміналістичних і технічних засобів доказування та активного використання спеціальних знань і експертних досліджень. Зроблені у статті висновки дають підстави стверджувати, що підвищення ефективності доказування у справах про фінансові правопорушення, вчинені з використанням цифрових технологій, можливе лише за умови вдосконалення методик збирання й фіксації цифрових доказів, розвитку спеціалізації слідчих і прокурорів, стандартизації експертного забезпечення та узгодження слідчої практики з сучасними підходами суду до оцінки електронних доказів. Це, у свою чергу, сприятиме підвищенню якості досудового розслідування та забезпеченню ефективного кримінально-правового захисту фінансових інтересів держави і громадян.

Ключові слова: *кібершахрайство, фінансова сфера, воєнний стан, досудове розслідування, цифрові докази, криптовалюта.*

The purpose of the scientific article is a comprehensive analysis of the problems of evidence in criminal proceedings regarding offenses in the financial sector committed using digital technologies, taking into account modern investigative and judicial practice, as well as substantiation of scientifically and practically sound approaches to improving the process of collecting, recording and evaluating digital evidence in the context of digitalization and martial law. A generalization of theoretical provisions and

© СУСЛІКОВА І.С. – доктор філософії з економіки, фахівець І категорії відділу міжнародних зв'язків (Державний податковий університет) https://orcid.org/0000-0003-3399-020X

an analysis of judicial practice indicate that the evidence in cases of criminal offenses in the financial sector committed with the use of digital technologies has an increased level of complexity and differs significantly from the evidence in "classical" financial crimes. This specificity is due to the digital nature of evidentiary information, the multi-stage nature of financial transactions, the use of anonymized technologies and transnational instruments, which complicates the establishment of a personalized connection between illegal actions and a specific person, as well as proving the subjective side of the criminal offense. It has been established that the key problems of proof in this category of cases are the identification of the subject of the crime in the digital environment, proving actual control over financial and digital instruments, ensuring the admissibility and relevance of electronic evidence, as well as reproducing the causal relationship between digital actions and the property damage caused. Judicial practice, in particular the positions of the Supreme Court, confirms the need to comply with increased standards of proof, which requires pre-trial investigation bodies to comprehensively combine procedural, forensic and technical means of proof and actively use special knowledge and expert research. The conclusions made in the article give grounds to argue that increasing the efficiency of proof in cases of financial offenses committed using digital technologies is possible only if the methods of collecting and recording digital evidence are improved, the specialization of investigators and prosecutors is developed, expert support is standardized, and investigative practice is harmonized with modern court approaches to the assessment of electronic evidence. This, in turn, will contribute to improving the quality of pre-trial investigation and ensuring effective criminal-legal protection of the financial interests of the state and citizens.

Key words: *cyber fraud, financial sphere, martial law, pre-trial investigation, digital evidence, cryptocurrency.*

Актуальність теми. Актуальність дослідження проблем доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, зумовлена стрімкою цифровізацією фінансових відносин, активним впровадженням дистанційних банківських сервісів, електронних платіжних інструментів і криптоактивів, що суттєво трансформувало як механізм вчинення кримінальних правопорушень, так і характер доказової інформації у кримінальному провадженні. Фінансові правопорушення дедалі частіше вчиняються у кіберпросторі, набувають латентного та транснаціонального характеру, що ускладнює застосування традиційних підходів до збирання, фіксації та оцінки доказів.

Особливої гостроти зазначена проблематика набула в умовах воєнного стану в Україні. Збройна агресія рф супроводжується зростанням обсягів цифрових фінансових операцій, масштабними соціальними виплатами, благодійними та волонтерськими зборами, що створює сприятливе середовище для вчинення фінансових правопорушень із використанням цифрових технологій. Водночас воєнний соціально-психологічний контекст підвищує вразливість потерпілих, а обмеженість ресурсів правоохоронних органів ускладнює ефективне документування кримінально протиправної діяльності.

Практика досудового розслідування та судового розгляду свідчить, що основні труднощі у справах цієї категорії пов’язані не стільки з установленням факту заподіяння майнової шкоди, скільки з доведенням причетності конкретної особи до її спричинення, встановленням суб’єктивної сторони кримінального правопорушення, допустимістю та належністю цифрових доказів, а також доведенням причинно-наслідкового зв’язку між діями у цифровому середовищі та фінансовими наслідками. Значна частина доказової інформації існує в електронній формі, є динамічною та залежною від технічних умов її збереження, що створює ризики втрати або визнання таких доказів недопустимими.

Аналіз судової практики, зокрема позицій Верховного Суду, засвідчує формування підвищених стандартів доказування у справах про фінансові правопорушення, вчинені з використанням цифрових технологій. Суди послідовно наголошують на необхідності доведення автентичності, цілісності цифрових доказів, а також фактичного контролю особи над фінансовими та цифровими інструментами. Це, у свою чергу, вимагає від органів досудового розслідування якісно нового, науково обґрунтованого підходу до організації доказування.

У зв’язку з цим, комплексне дослідження проблем доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій,

є своєчасним і необхідним. Таке дослідження має важливе теоретичне значення для розвитку кримінального процесу та криміналістики, а також істотну практичну цінність для вдосконалення діяльності органів досудового розслідування і суду в умовах цифровізації та воєнного стану.

Аналіз останніх досліджень і публікацій. Проблематика доказування у кримінальних провадженнях щодо правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, у сучасній науковій літературі розглядається переважно у трьох взаємопов'язаних напрямах: 1) дослідження кіберзлочинності та кібершахрайства як явищ, що трансформують традиційні моделі посягань на власність; 2) розроблення криміналістичних підходів до виявлення та фіксації цифрових слідів, зокрема електронних документів і даних електронних комунікацій; 3) аналіз процесуальних стандартів допустимості, належності та оцінки електронних доказів у кримінальному судочинстві. У межах зазначених напрямів особливу увагу науковців привертають питання автентичності й цілісності електронної інформації, ідентифікації суб'єкта правопорушення у цифровому середовищі, а також меж застосування спеціальних знань під час формування доказової бази.

У вітчизняній науці кримінального процесу та криміналістики окремі аспекти електронних (цифрових) доказів, їх процесуальної природи, порядку отримання, фіксації та використання у доказуванні досліджували М. А. Погорецький, Т. Г. Фоміна, І. Г. Каланча, А. В. Гутник, А. Я. Хитра та інші автори, які сформували теоретичні підходи до розуміння електронної інформації як джерела доказів і акцентували на необхідності дотримання процесуальних гарантій її перевірюваності. Криміналістичні та методичні засади розслідування фінансових правопорушень у цифровому середовищі, у тому числі шахрайства з використанням електронних платіжних інструментів, висвітлювалися у працях А. Є. Жиліна, А. В. Рейнгольда, К. О. Чаплинського, а також у дослідженнях, присвячених виявленню та документуванню злочинної діяльності у сфері інформаційних технологій. Значний масив праць стосується й загальнотеоретичних положень доказування та кримінально-правової протидії економічним і службовим правопорушенням, які формують концептуальне підґрунтя аналізу (зокрема у роботах В. В. Голіни, М. І. Хавронюка, В. Я. Тація, Ю. В. Бауліна, С. С. Чернявського).

Водночас аналіз наукових публікацій засвідчує, що попри значний доробок у сфері кіберзлочинності та електронних доказів, низка питань зберігає дискусійний або недостатньо розроблений характер. Зокрема, потребують подальшого комплексного осмислення процесуальні стандарти доказування у справах про фінансові правопорушення, вчинені з використанням цифрових технологій, із урахуванням сучасної практики Верховного Суду; методики поєднання економічних, комп'ютерно-технічних і блокчейн-досліджень у межах експертного забезпечення; а також проблеми доведення фактичного контролю особи над цифровими фінансовими інструментами та криптоактивами в умовах транснаціональності кримінально протиправних схем і воєнного стану.

Метою наукової статті є комплексний аналіз проблем доказування у кримінальних провадженнях щодо правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, з урахуванням сучасної слідчої та судової практики, а також обґрунтування науково й практично виважених підходів до вдосконалення процесу збирання, фіксації та оцінки цифрових доказів в умовах цифровізації та воєнного стану.

Виклад основного матеріалу. Доказування у кримінальних провадженнях щодо правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, є складним процесом, спрямованим на встановлення обставин кримінального правопорушення шляхом збирання, перевірки, оцінки та використання доказів, значна частина яких має електронну (цифрову) форму [1; 2]. Специфіка таких проваджень полягає у тому, що доказова інформація формується та зберігається переважно у цифровому середовищі - в інформаційних системах банків, платіжних сервісів, мережах електронних комунікацій, програмному забезпеченні, а також у розподілених реєстрах цифрових активів.

У справах цієї категорії доказування охоплює встановлення як традиційних елементів предмета доказування, передбачених кримінальним процесуальним законодавством, так і специфічних обставин, зумовлених цифровим способом вчинення кримінального правопорушення. Зокрема, поряд із доведенням події кримінального правопорушення, розміру заподіяної шкоди, форми вини та мотивів, доказування включає встановлення способу використання цифрових технологій, характеру доступу до електронних фінансових інструментів, механізму руху грошових коштів або цифрових активів, а також фактичного контролю особи над відповідними технічними й фінансовими ресурсами [5].

Важливою складовою доказування у таких справах є ідентифікація суб'єкта кримінального правопорушення у цифровому середовищі, що передбачає встановлення зв'язку між конкретною фізичною особою та цифровими слідами злочину — обліковими записами, електронними пристроями, IP-адресами, платіжними рахунками, криптогаманцями тощо. На відміну від традиційних форм кримінально протиправної діяльності, у фінансових правопорушеннях, вчинених з використанням цифрових технологій, такий зв'язок є опосередкованим і потребує використання спеціальних знань, експертних досліджень та комплексного аналізу доказів.

Доказування у зазначеній категорії справ також включає перевірку автентичності, цілісності та допустимості цифрових доказів, що зумовлено їх нематеріальним характером і технічною можливістю зміни або знищення електронної інформації. Це вимагає дотримання підвищених процесуальних стандартів фіксації електронних даних, належного документування способів їх отримання та забезпечення можливості подальшої перевірки в судовому провадженні, у тому числі шляхом проведення відповідних експертиз [5].

Отже, доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, є багаторівневим процесом, що поєднує процесуальні, криміналістичні та технічні елементи. Його ефективність безпосередньо залежить від здатності органів досудового розслідування інтегрувати традиційні інструменти доказування з сучасними методами цифрової криміналістики, фінансового аналізу та експертного забезпечення, а також від узгодженості такої діяльності з усталеними стандартами доказування, сформульованими у практиці Верховного Суду.

Доказування у кримінальних провадженнях щодо правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, характеризується підвищеною складністю, що зумовлено нематеріальною природою значної частини доказової інформації, багаторівневістю фінансових операцій та транснаціональним характером злочинних схем. На відміну від традиційних посягань на власність, у зазначеній категорії справ ключові обставини кримінального правопорушення фіксуються у цифровому середовищі, що істотно ускладнює встановлення події кримінального правопорушення, суб'єкта кримінальної відповідальності, форми вини та причинно-наслідкового зв'язку між діями особи й заподіяною майновою шкодою.

Однією з основних проблем доказування є ідентифікація особи, яка безпосередньо вчинила кримінальне правопорушення. Використання VPN-сервісів, анонімізаторів, віртуальних номерів, підставних осіб («дропів»), а також електронних платіжних інструментів і криптоактивів призводить до розриву між цифровими слідами кримінального правопорушення та конкретною фізичною особою. Судова практика, зокрема позиції Верховного Суду, свідчить, що сам по собі факт надходження коштів на рахунок чи використання облікового запису не є достатнім для доведення вини без встановлення фактичного контролю особи над відповідними фінансовими або цифровими інструментами [6; 7; 8].

Суттєві труднощі виникають і при доведенні суб'єктивної сторони кримінального правопорушення, насамперед прямого умислу. У багатьох кримінальних провадженнях сторона обвинувачення обмежується констатацією об'єктивних обставин (руху коштів, доступу до сервісів), не надаючи належних доказів усвідомлення особою протиправного характеру своїх дій. За відсутності доказів координації дій, розподілу ролей, цифрового листування або інших даних, що свідчать про цілеспрямованість поведінки, суди визнають доказову базу недостатньою.

Окремий блок проблем пов'язаний із допустимістю та належністю цифрових доказів. Скріншоти електронного листування, дані з вебресурсів, мобільних додатків або месенджерів нерідко визнаються судами недопустимими через порушення порядку їх отримання, фіксації чи збереження. Верховний Суд послідовно наголошує, що цифрові докази повинні відповідати вимогам автентичності, цілісності та перевірюваності, а у разі виникнення сумнівів щодо цих характеристик — підтверджуватися результатами відповідних експертних досліджень.

Особливої складності набуває доказування у справах, де незаконно отримані кошти конвертуються у криптовалюту або переміщуються через децентралізовані фінансові сервіси. У таких випадках проблемним є не лише відстеження ланцюжка транзакцій, а й доведення фактичного володіння чи контролю особи над криптогаманцем. За відсутності комплексного поєднання блокчейн-аналітики, комп'ютерно-технічної експертизи та фінансового аналізу встановлення цих обставин є вкрай ускладненим.

Не менш проблемним є доведення причинно-наслідкового зв'язку між діями у цифровому середовищі та настанням майнової шкоди. Фінансові кібершахрайські схеми часто мають багатоступеневий характер, що призводить до фрагментарності доказової інформації та ускладнює

відтворення цілісного механізму злочину. У таких умовах за відсутності системного підходу до доказування суди нерідко визнають причинно-наслідковий зв'язок недоведеним, навіть за наявності очевидних фінансових втрат.

Таким чином, проблеми доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, мають комплексний і системний характер та зумовлені поєднанням технологічних, процесуальних і організаційних чинників. Їх подолання потребує вдосконалення процесуальних механізмів збирання й оцінки цифрових доказів, активнішого використання спеціальних знань, а також узгодження слідчої та судової практики з усталеними стандартами доказування, сформульованими у рішеннях Верховного Суду.

Аналіз судової практики у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, дозволяє виокремити типові ситуації доказування, у яких наочно проявляється специфіка предмета та засобів доказування.

Приклад 1. Фішингове шахрайство з використанням підробленого банківського сервісу. У кримінальному провадженні за фактом заволодіння коштами потерпілого шляхом введення його в оману через фейковий вебсайт банку орган досудового розслідування довів факт незаконного списання грошових коштів і наявність цифрових слідів доступу до банківського акаунту. Водночас суд визнав доказування неповним, оскільки сторона обвинувачення не надала належних доказів, що саме обвинувачений здійснював адміністрування фішингового ресурсу та контролював рух коштів. Цей приклад демонструє, що доведення події кримінального правопорушення та шкоди саме по собі не є достатнім без встановлення персоніфікованого зв'язку між особою і цифровими інструментами кримінального правопорушення.

Приклад 2. Використання «дропів» у схемі фінансового кібершахрайства. У справі про заволодіння коштами громадян шляхом телефонного шахрайства та подальшого перерахування коштів на рахунки підставних осіб суд критично оцінив докази обвинувачення щодо «дропа», на рахунок якого надходили кошти. Суд зазначив, що сам факт надходження грошових коштів на банківський рахунок не підтверджує умисної участі особи у кримінальному правопорушенні без доведення її обізнаності щодо кримінально протиправного походження коштів та контролю над їх подальшим використанням. Цей приклад ілюструє проблему доведення суб'єктивної сторони та співучасті у цифрових фінансових кримінальних правопорушень.

Приклад 3. Використання месенджерів і скріншотів як доказів. У низці справ про фінансове кібершахрайство сторона обвинувачення посилалася на скріншоти листування у месенджерах як підтвердження координації дій між учасниками злочинної схеми. Однак суди визнавали такі докази неналежними або недостатніми у випадках, коли не було встановлено належність облікового запису конкретній особі або не підтверджено автентичність цифрових даних шляхом експертного дослідження. Ці справи демонструють, що цифрова форма доказу потребує підвищених стандартів перевірки та процесуальної легітимації**.**

Приклад 4. Конвертація коштів у криптовалюту. У кримінальному провадженні щодо легалізації коштів, отриманих у результаті фінансового кібершахрайства, слідство довело факт переведення грошових коштів у криптовалюту та подальшого їх руху через низку гаманців. Проте суд дійшов висновку про недоведеність обвинувачення через відсутність переконливих доказів того, що обвинувачений мав фактичний контроль над конкретним криптогаманцем. Цей приклад наочно засвідчує складність доведення контролю над цифровими активами та необхідність комплексного експертного забезпечення.

Приклад 5. Причинно-наслідковий зв'язок між цифровими діями і шкодою. У справах, де фінансова шкода є результатом серії цифрових операцій (доступ до акаунтів, перекази, конвертація коштів), суди звертають особливу увагу на відтворення цілісного механізму злочину. За відсутності системного фінансово-економічного та цифрового аналізу суди визнають причинно-наслідковий зв'язок між діями обвинуваченого і шкодою недоведеним, навіть за очевидної наявності фінансових втрат у потерпілих [6; 7; 8].

Наведені приклади судової практики підтверджують, що доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, виходить за межі традиційного встановлення факту кримінального правопорушення та шкоди. Воно потребує доведення персоніфікованого зв'язку між особою і цифровими інструментами, контролю над фінансовими потоками, автентичності електронних доказів та наявності умислу, що зумовлює необхідність комплексного, міждисциплінарного підходу до доказування.

Висновки. Проведений аналіз засвідчує, що доказування у справах про кримінальні правопорушення у фінансовій сфері, вчинені з використанням цифрових технологій, характеризується

підвищеною складністю та багаторівневістю, що зумовлено цифровою природою доказової інформації, використанням анонімізованих технічних рішень, багатоступеневими фінансовими операціями й транснаціональним характером кримінально протиправних схем. У таких провадженнях основні труднощі виникають не стільки при встановленні факту заподіяння майнової шкоди, скільки при доведенні причетності конкретної особи до кримінального правопорушення, фактичного контролю над фінансовими й цифровими інструментами, а також суб'єктивної сторони кримінального правопорушення. Судова практика, зокрема позиції Верховного Суду, підтверджує необхідність дотримання підвищених стандартів допустимості, належності та перевірюваності цифрових доказів.

Узагальнені результати дослідження дають підстави стверджувати, що підвищення ефективності доказування у справах цієї категорії можливе лише за умови комплексного підходу, який поєднує процесуальні гарантії, криміналістичні методи та сучасні інструменти цифрової криміналістики й фінансового аналізу. Вдосконалення методик збирання та фіксації електронних доказів, розвиток спеціалізації слідчих і прокурорів, стандартизація експертного забезпечення та узгодження практики досудового розслідування з актуальними підходами суду сприятимуть підвищенню якості кримінального провадження та ефективному захисту фінансових інтересів держави й громадян.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17

2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

3. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15

4. Про віртуальні активи : Закон України від 17.02.2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20

5. Holt T. J., Bossler A. M. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge, 2016. URL: https://www.routledge.com/Cybercrime-in-Progress/Holt-Bossler/p/book/9781138820156

6. Постанова Верховного Суду від 03.11.2020 у справі № 127/20580/18 (щодо допустимості електронних доказів). URL: https://reyestr.court.gov.ua/Review/92611863

7. Постанова Верховного Суду від 16.02.2023 у справі № 761/37627/20 (щодо доведення контролю над електронними засобами). URL: https://reyestr.court.gov.ua/Review/108964211

8. Постанова Верховного Суду від 07.09.2022 у справі № 753/22860/19 (щодо оцінки цифрових доказів у сукупності). URL: https://reyestr.court.gov.ua/Review/106455837.

Дата першого надходження рукопису до видання: 22.08.2025
Дата прийнятого до друку рукопису після рецензування: 10.09.2025
Дата публікації: 25.09.2025