УДК 343.98
DOI https://doi.org/10.32844/2618-1258.2025.6.29

СУСЛІКОВА І.С.

ТИПОВІ СЛІДЧІ СИТУАЦІЇ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ, ЩО ВЧИНЯЮТЬСЯ У ФІНАНСОВІЙ СФЕРІ

TYPICAL INVESTIGATIVE SITUATIONS WHEN INVESTIGATING CYBERCRIMES COMMITTED IN THE FINANCIAL SPHERE

Статтю присвячено дослідженню типових слідчих ситуацій, що виникають під час розслідування кіберзлочинів, учинених у фінансовій сфері. Актуальність теми зумовлена стрімкою цифровізацією фінансових відносин, поширенням безготівкових розрахунків, використанням електронних платіжних сервісів і віртуальних активів, а також зростанням кількості фінансових кіберзлочинів, які характеризуються високим рівнем латентності, транснаціональністю та складністю доказування. В умовах воєнного стану зазначені процеси набувають особливої гостроти, оскільки збільшується обсяг онлайн-платежів, соціальних і благодійних виплат, що створює додаткові можливості для злочинних посягань. У статті проаналізовано поняття та значення слідчої ситуації як криміналістичної категорії й обґрунтовано доцільність її використання для оптимізації тактики досудового розслідування фінансових кіберзлочинів. Виокремлено та детально охарактеризовано основні типові слідчі ситуації, зокрема ситуацію первинного виявлення факту кримінального правопорушення, ідентифікації способу його вчинення, використання підставних осіб і фінансових посередників, трансформації та маскування фінансових потоків, транснаціонального характеру посягання, а також протидії розслідуванню з боку підозрюваних. Розкрито їх інформаційний зміст, характерні ознаки, основні доказові ризики та тактичне значення для вибору слідчих (розшукових) дій. Зроблено висновок, що систематизація типових слідчих ситуацій дозволяє підвищити ефективність кримінального переслідування шляхом своєчасного збереження цифрових і фінансових доказів, правильного визначення напряму розслідування та мінімізації ризиків втрати доказової інформації. Обґрунтовано, що ефективне розслідування фінансових кіберзлочинів потребує комплексного поєднання інструментів цифрової криміналістики, фінансового аналізу, експертних досліджень і міжнародного співробітництва. Отримані результати можуть бути використані у практичній діяльності органів досудового розслідування, а також у подальших наукових дослідженнях проблем криміналістичного забезпечення протидії кіберзлочинам у фінансовій сфері.

Ключові слова: *кіберзлочини у фінансовій сфері, фінансове кібершахрайство, цифрові докази, доказування у кримінальному провадженні, розслідування кіберзлочинів, міжнародні стандарти доказування, зарубіжний досвід, фінансова розвідка, цифрова криміналістика.*

The article is devoted to the study of typical investigative situations that arise during the investigation of cybercrimes committed in the financial sector. The relevance of the topic is due to the rapid digitalization of financial relations, the spread of non-cash payments, the use of electronic payment services and virtual assets, as well as the growth in the number of financial cybercrimes, which are characterized by a high level of latency, transnationality and complexity of proof. In conditions of martial law,

© СУСЛІКОВА І.С. – доктор філософії з економіки, доцент кафедри фінансового та податкового права (Державний податковий університет) https://orcid.org/0000-0003-3399-020X

these processes become especially acute, as the volumes of online payments, social and charitable payments increase, which creates additional opportunities for criminal encroachments. The article analyzes the concept and meaning of the investigative situation as a forensic category and justifies the feasibility of its use to optimize the tactics of pre-trial investigation of financial cybercrimes. The main typical investigative situations are identified and described in detail, in particular, situations of initial detection of the fact of a criminal offense, identification of the method of its commission, use of front persons and financial intermediaries, transformation and masking of financial flows, transnational nature of the encroachment, as well as resistance to the investigation by the suspects. Their information content, characteristic features, main evidentiary risks and tactical significance for the choice of investigative (detective) actions are revealed. It is concluded that the systematization of typical investigative situations allows to increase the efficiency of criminal prosecution by timely preservation of digital and financial evidence, correct determination of the direction of the investigation and minimizing the risks of loss of evidentiary information. It is substantiated that effective investigation of financial cybercrimes requires a comprehensive combination of digital forensics tools, financial analysis, expert research and international cooperation. The results obtained can be used in the practical activities of pre-trial investigation bodies, as well as in further scientific research into the problems of forensic support for combating cybercrimes in the financial sector.

Key words: *cybercrimes in the financial sector, financial cyberfraud, digital evidence, evidence in criminal proceedings, cybercrime investigation, international standards of evidence, foreign experience, financial intelligence, digital forensics.*

Актуальність теми. Актуальність дослідження типових слідчих ситуацій при розслідуванні кіберзлочинів, учинених у фінансовій сфері, зумовлена стрімкою цифровізацією фінансових відносин, зростанням обсягів безготівкових розрахунків, використанням електронних платіжних сервісів і віртуальних активів, а також транснаціональним характером сучасної кіберзлочинності. Зазначені процеси істотно ускладнюють діяльність органів досудового розслідування, оскільки кримінально протиправні посягання на фінансові ресурси дедалі частіше здійснюються із застосуванням складних цифрових технологій, а докази набувають нематеріальної, динамічної та розподіленої форми [1].

Особливої значущості ця проблематика набуває в умовах воєнного стану, коли зростає кількість онлайн-платежів, благодійних зборів, соціальних і державних виплат, що створює сприятливе середовище для фінансових кіберзлочинів, зокрема кібершахрайства, фішингових атак і незаконного заволодіння коштами. Водночас типові для таких правопорушень слідчі ситуації характеризуються дефіцитом початкової інформації, швидкою втратою цифрових слідів, використанням підставних осіб та транснаціональних платіжних інструментів, що ускладнює встановлення кінцевого вигодонабувача та доведення фактичного контролю над фінансовими активами.

Незважаючи на наявність окремих наукових досліджень у сфері кіберзлочинності та фінансових правопорушень, проблематика типових слідчих ситуацій у цій категорії кримінальних проваджень залишається недостатньо систематизованою. Відсутність науково обґрунтованої класифікації слідчих ситуацій та чітких тактичних рекомендацій щодо дій слідчого на різних етапах розслідування призводить до втрати доказової інформації, затягування кримінального провадження та зниження ефективності кримінального переслідування.

У зв'язку з цим наукове дослідження типових слідчих ситуацій при розслідуванні кіберзлочинів у фінансовій сфері є актуальним і практично значущим. Воно спрямоване на вдосконалення криміналістичного забезпечення досудового розслідування, підвищення якості доказування та формування ефективної тактики реагування органів правопорядку на сучасні виклики фінансової кіберзлочинності.

Аналіз останніх досліджень і публікацій. Проблематику типових слідчих ситуацій у справах про кіберзлочини, вчинені у фінансовій сфері, у своїх наукових працях досліджували М. А. Погорецький, Т. Г. Фоміна, І. Г. Каланча, А. В. Гутник, А. Я. Хитра, А. Є. Жилін, К. О. Чаплинський, М. І. Хавронюк, С. С. Чернявський.

Незважаючи на наявність наукових праць, присвячених кіберзлочинності та фінансовим кримінальним правопорушенням, проблематика типових слідчих ситуацій у цій категорії кримінальних проваджень залишається фрагментарно дослідженою. У криміналістичній науці

відсутня уніфікована класифікація таких ситуацій з урахуванням специфіки цифрових доказів, транснаціонального характеру фінансових операцій, використання підставних осіб і віртуальних активів. Недостатньо розробленими залишаються тактичні алгоритми дій слідчого на початковому етапі розслідування в умовах дефіциту інформації та швидкої втрати цифрових слідів, а також питання доказування фактичного контролю особи над фінансовими й цифровими інструментами у складних багатоепізодних схемах.

Крім того, подальшого наукового осмислення потребують проблеми співвідношення та достатності цифрових і фінансових доказів у межах окремих слідчих ситуацій, критерії їх оцінки судом, а також особливості застосування міжнародних механізмів отримання електронних доказів у транснаціональних провадженнях. Практично недослідженим залишається вплив активної протидії з боку підозрюваних, зокрема використання засобів анонімізації й шифрування, на трансформацію слідчих ситуацій і вибір тактики розслідування, а також питання комплексного використання експертних досліджень у справах про кіберзлочини у фінансовій сфері.

Метою дослідження наукове обґрунтування та систематизація типових слідчих ситуацій, що виникають під час розслідування кіберзлочинів у фінансовій сфері, а також розроблення теоретичних і прикладних підходів до вибору оптимальної тактики дій слідчого з урахуванням специфіки цифрових і фінансових доказів, транснаціонального характеру правопорушень та сучасних викликів доказування.

Виклад основного матеріалу. У криміналістиці слідчу ситуацію прийнято розглядати як сукупність фактичних обставин, інформаційних можливостей, процесуальних умов та поведінкових чинників, що складаються на певному етапі досудового розслідування і визначають напрям, зміст та тактику слідчих (розшукових) дій. Для кіберзлочинів у фінансовій сфері такі ситуації мають специфічний характер, зумовлений нематеріальністю об'єкта посягання, динамічністю цифрових доказів і складною структурою фінансових операцій [1].

Розглянемо кілька найбільш поширених слідчих ситуацій.

Ситуація первинного виявлення факту фінансового кіберзлочину формується на початковому етапі досудового розслідування та характеризується вкрай обмеженим обсягом перевіреної інформації, що має фрагментарний і нестабільний характер. У більшості випадків підставою для внесення відомостей до Єдиного реєстру досудових розслідувань є заява потерпілого про незаконне списання коштів з банківського рахунку, платіжної картки чи електронного гаманця або повідомлення про введення його в оману шляхом використання цифрових засобів комунікації.

Інформаційний зміст цієї слідчої ситуації, як правило, обмежується суб'єктивними поясненнями потерпілого, окремими відомостями про час і суму списання коштів, а також загальними обставинами користування фінансовими або цифровими сервісами. Водночас об'єктивні дані про спосіб учинення кримінального правопорушення, технічний механізм доступу до фінансової інформації, використані цифрові інструменти, а також особу правопорушника та його місцезнаходження на цьому етапі відсутні або не піддаються негайній ідентифікації [2].

Характерною ознакою цієї слідчої ситуації є підвищений ризик втрати доказової інформації. Банківські логи, журнали доступу, дані платіжних систем, телекомунікаційна інформація та інші цифрові сліди мають обмежений строк зберігання та можуть бути змінені або знищені внаслідок технічних процедур або дій злочинців. За таких умов зволікання з фіксацією й збереженням інформації суттєво ускладнює подальше доказування та може призвести до втрати ключових доказів.

Варто відмітити, що значення ситуації первинного виявлення фінансового кіберзлочину полягає у необхідності негайної реалізації комплексу невідкладних слідчих (розшукових) та процесуальних дій, спрямованих на збереження цифрових і фінансових даних. Пріоритетними завданнями слідчого на цьому етапі є забезпечення термінового збереження інформації у банківських установах і платіжних сервісах, фіксація цифрових слідів, а також формування первинної версійної бази щодо можливого способу вчинення кримінального правопорушення [3].

Водночас ця слідча ситуація потребує від слідчого особливої обережності у формулюванні процесуальних рішень, оскільки наявна інформація не дозволяє однозначно кваліфікувати дії правопорушника або визначити ступінь участі третіх осіб. Саме на цьому етапі закладається доказова основа подальшого розслідування, а помилки у визначенні тактичних пріоритетів можуть мати незворотні негативні наслідки для всього кримінального провадження.

Ситуація ідентифікації способу вчинення фінансового кіберзлочину формується після первинної фіксації факту протиправного заволодіння коштами та характеризується поступовим накопиченням цифрової інформації, яка дозволяє окреслити загальний механізм злочинного посягання. На цьому етапі досудового розслідування слідчий зосереджує увагу на з'ясуванні того, яким саме способом було здійснено доступ до фінансових ресурсів потерпілого: шляхом

фішингового впливу, застосування методів соціальної інженерії, злому облікового запису, компрометації платіжного інструменту або використання інших цифрових схем.

Інформаційна база цієї слідчої ситуації формується за рахунок аналізу окремих цифрових слідів, що залишилися внаслідок злочинної діяльності. До таких слідів належать електронні повідомлення, посилання на підроблені вебресурси, доменні імена, журнали доступу, IP-адреси, дані платіжних транзакцій, а також інформація, отримана від банківських установ, платіжних сервісів і телекомунікаційних операторів. Водночас ці відомості, як правило, не містять безпосередньої ідентифікації особи правопорушника, що зумовлює інформаційну неповноту та потребу в подальшому аналітичному опрацюванні доказового матеріалу [3].

Характерною рисою цієї слідчої ситуації є ймовірність багатоваріантності способу вчинення злочину, коли окремі цифрові ознаки можуть відповідати кільком кримінальним механізмам одночасно. Наприклад, фішинг може поєднуватися з елементами соціальної інженерії, а компрометація облікового запису — із подальшим використанням шкідливого програмного забезпечення. За таких умов існує ризик помилкового визначення способу вчинення злочину, що може призвести до неправильного вибору тактики розслідування та неефективного використання слідчих і експертних ресурсів.

Тактичне значення ситуації ідентифікації способу вчинення фінансового кіберзлочину полягає у формуванні первинної криміналістичної моделі злочину, яка визначає напрями подальшого збирання доказів. Саме встановлення способу посягання обумовлює вибір конкретних слідчих (розшукових) дій, необхідність призначення відповідних експертиз (комп'ютерно-технічних, телекомунікаційних, фінансово-економічних), а також визначення кола суб'єктів, у яких слід витребувати доказову інформацію.

Водночас ця слідча ситуація потребує від слідчого дотримання принципу версійності та критичного аналізу наявних даних. Передчасне або необґрунтоване закріплення єдиної версії щодо способу вчинення злочину може обмежити подальші можливості доказування та ускладнити встановлення повної картини кримінального правопорушення. Тому на цьому етапі особливого значення набуває комплексний підхід до аналізу цифрових слідів і поступове уточнення механізму злочину з урахуванням нових доказів.

Ситуація використання підставних осіб та фінансових посередників є однією з найбільш характерних і водночас складних для розслідування фінансових кіберзлочинів. Вона виникає у випадках, коли викрадені або незаконно отримані кошти не надходять безпосередньо у розпорядження організатора кримінального правопорушення, а спрямовуються на рахунки третіх осіб або проходять через низку платіжних сервісів, електронних гаманців чи фінансових платформ. Такі особи часто виконують роль так званих «дропів» і формально виступають власниками або користувачами рахунків, що використовуються у кримінально протиправній схемі.

Специфіка цієї слідчої ситуації полягає у наявності чітко зафіксованих фінансових операцій та документально підтверджених платіжних транзакцій за одночасної відсутності очевидного зв'язку між рухом коштів і конкретною особою-організатором злочину. Формальна належність рахунків підставним особам створює ілюзію легітимності фінансових операцій та ускладнює встановлення справжнього суб'єкта контролю над коштами. У ряді випадків такі особи можуть усвідомлювати свою роль у злочинній схемі, однак нерідко вони залучаються шляхом обману або під виглядом законної фінансової діяльності [4].

Ключовою проблемою доказування у межах цієї слідчої ситуації є необхідність відмежування формального володіння фінансовим інструментом від фактичного контролю над ним. Для кримінально-правової оцінки вирішального значення набуває не сам факт відкриття рахунку на певну особу, а встановлення того, хто реально ініціював фінансові операції, приймав рішення щодо руху коштів, мав доступ до засобів автентифікації та отримував кінцеву вигоду.

Значення цієї слідчої ситуації полягає у необхідності зміщення акценту з формального встановлення власників рахунків на дослідження реального механізму управління фінансовими потоками. Пріоритетного значення набувають слідчі (розшукові) дії, спрямовані на аналіз цифрових слідів доступу до рахунків, дослідження зв'язків між підставними особами та іншими учасниками схеми, а також встановлення способів передачі контролю над фінансовими інструментами.

Водночас ця ситуація характеризується підвищеним ризиком помилкової криміналізації дій осіб, які фактично не усвідомлювали свого залучення до злочинної діяльності. Тому від слідчого вимагається ретельна оцінка суб'єктивної сторони діяння кожного учасника фінансової схеми, а також диференційований підхід до процесуального статусу таких осіб. Саме у межах цієї слідчої ситуації формуються передумови для правильного встановлення кола співучасників та забезпечення справедливості кримінального переслідування [4].

Ситуація трансформації та маскування фінансових потоків виникає у випадках, коли після первинного заволодіння коштами злочинці здійснюють їх багатоетапне переміщення з метою

ускладнення або унеможливлення встановлення походження активів, кінцевого вигодонабувача та зв'язку між злочином і фінансовим результатом. Найчастіше це проявляється у конвертації коштів у криптовалюти, використанні електронних гаманців, міжнародних платіжних систем, сервісів швидких переказів, а також інструментів анонімізації та фінансового «розшарування».

Інформаційна специфіка цієї слідчої ситуації полягає у наявності значного масиву фінансових і цифрових даних, які, однак, не утворюють очевидного та лінійного ланцюга руху коштів. Фінансові операції можуть здійснюватися у різних юрисдикціях, із використанням різних валют, платіжних платформ і технологічних рішень, що призводить до фрагментації доказової інформації. За таких умов встановлення причинно-наслідкового зв'язку між первинним злочинним посяганням і подальшими фінансовими операціями потребує спеціального аналітичного опрацювання [5].

Особливої складності ця слідча ситуація набуває у випадках використання віртуальних активів. Псевдонімний характер блокчейн-транзакцій, відсутність прямої прив'язки гаманця до конкретної особи, а також можливість застосування міксерів, сервісів приховування транзакцій і децентралізованих платформ суттєво ускладнюють персоніфікацію фінансової діяльності. У таких умовах доказування не може обмежуватися аналізом окремих транзакцій і потребує комплексного поєднання цифрових, фінансових і поведінкових доказів.

Тактичне значення ситуації трансформації та маскування фінансових потоків полягає у необхідності застосування міждисциплінарного підходу до розслідування. Слідчий змушений поєднувати методи цифрової криміналістики, фінансового аналізу та економічної експертизи з даними, отриманими в результаті оперативно-розшукових заходів і міжнародного співробітництва. Пріоритетним завданням є не лише фіксація окремих фінансових операцій, а й відтворення загальної логіки руху коштів як елементу єдиного злочинного механізму.

Водночас ця слідча ситуація потребує від слідчого чіткого розуміння меж допустимого втручання у фінансову сферу та дотримання принципів законності, необхідності й пропорційності. Неналежне процесуальне оформлення отримання фінансових і цифрових даних або порушення стандартів їх збереження може призвести до втрати доказової сили навіть за наявності об'єктивно значущої інформації. Таким чином, ситуація трансформації та маскування фінансових потоків є однією з найбільш складних з точки зору доказування та вимагає високого рівня професійної підготовки слідчого і залучених фахівців.

Ситуація транснаціонального характеру фінансового кіберзлочину виникає у випадках, коли елементи кримінально протиправного механізму пов'язані з кількома юрисдикціями. Як правило, серверна інфраструктура, платіжні платформи, криптовалютні сервіси або кінцеві вигодонабувачі розташовані за межами держави, на території якої здійснюється досудове розслідування. Така ситуація є типовою для сучасних фінансових кіберзлочинів і суттєво ускладнює доступ до доказової інформації.

Інформаційною особливістю цієї слідчої ситуації є фрагментарність доказів, розпорошених між різними державами, а також залежність слідчого від іноземних провайдерів послуг, фінансових установ і компетентних органів інших країн. Отримання цифрових і фінансових даних у таких умовах потребує застосування механізмів міжнародної правової допомоги, які традиційно характеризуються складністю процедур і значними часовими витратами. Зволікання з ініціюванням таких механізмів може призвести до втрати або зміни доказової інформації.

Тактичне значення ситуації транснаціонального характеру злочину полягає у необхідності максимально раннього визначення міжнародного елементу кримінального провадження та своєчасного застосування процедур термінового збереження електронних доказів. Для слідчого критично важливим є правильне формулювання запитів про міжнародну правову допомогу, визначення кола необхідних даних і дотримання вимог іноземного законодавства щодо захисту персональних даних та прав людини. Саме в цій ситуації особливого значення набуває координація з органами прокуратури та використання міжнародних правових інструментів у сфері кіберзлочинності.

Водночас транснаціональна слідча ситуація потребує від слідчого врахування ризиків визнання доказів недопустимими у разі порушення процедур їх отримання. Неналежне процесуальне оформлення міжнародних запитів або ігнорування вимог іноземної юрисдикції може поставити під сумнів результати всього розслідування, що зумовлює необхідність підвищеної уваги до формальних аспектів доказування [6].

Ситуація протидії розслідуванню виникає на будь-якому етапі досудового розслідування фінансових кіберзлочинів і характеризується активною або пасивною поведінкою підозрюваних, спрямованою на ускладнення або блокування збирання доказів. Така протидія може проявлятися у приховуванні або знищенні цифрових слідів, використанні засобів шифрування та анонімізації, відмові від надання доступу до цифрових пристроїв, а також у зловживанні процесуальними правами з метою затягування розслідування.

Інформаційна специфіка цієї слідчої ситуації полягає у зменшенні доступності доказової інформації та зростанні ролі непрямих доказів. Слідчий часто стикається з обмеженим доступом до первинних цифрових даних і змушений відновлювати механізм кримінального правопорушення на підставі аналізу фінансових операцій, поведінкових моделей, зв'язків між учасниками та результатів експертних досліджень. За таких умов особливої ваги набуває послідовність і системність доказування.

Тактичне значення ситуації протидії розслідуванню полягає у необхідності забезпечення бездоганної процесуальної форми кожної слідчої (розшукової) дії. Будь-які порушення вимог кримінального процесуального закону щодо фіксації, збереження або використання цифрових доказів можуть бути використані стороною захисту для дискредитації доказової бази. Тому в цій ситуації ключовим завданням слідчого є дотримання стандартів допустимості, належності та достовірності доказів [6].

Крім того, ситуація протидії розслідуванню вимагає від слідчого прогнозування можливих дій підозрюваних і застосування превентивних заходів, спрямованих на збереження доказової інформації. Саме в таких умовах особливого значення набуває своєчасне залучення експертів, застосування технічних засобів фіксації та чітке документування всіх етапів роботи з цифровими доказами. У підсумку ефективне подолання протидії розслідуванню є вирішальним чинником успішного завершення кримінального провадження у справах про фінансові кіберзлочини.

Висновки. Проведений аналіз типових слідчих ситуацій при розслідуванні кіберзлочинів, учинених у фінансовій сфері, свідчить, що такі кримінальні провадження характеризуються підвищеним рівнем інформаційної невизначеності, динамічністю доказової бази та складною структурою фінансово-цифрових взаємозв'язків. На кожному етапі досудового розслідування слідчий стикається з різними комбінаціями інформаційних, процесуальних і поведінкових чинників, що зумовлює формування специфічних слідчих ситуацій — від первинного виявлення факту злочину до активної протидії розслідуванню та транснаціонального характеру посягання. Систематизація таких ситуацій дозволяє глибше усвідомити механізм фінансового кіберзлочину та визначити ключові ризики втрати або спотворення доказової інформації.

Узагальнення типових слідчих ситуацій створює наукову основу для формування ефективної тактики досудового розслідування, що має базуватися на принципах оперативності, комплексності та процесуальної бездоганності. Встановлення способу вчинення кримінального правопорушення, доведення фактичного контролю над фінансовими інструментами, подолання транснаціональних бар'єрів і протидії з боку підозрюваних потребують поєднання цифрової криміналістики, фінансового аналізу та міжнародного співробітництва. Запропонований підхід сприяє підвищенню якості доказування, забезпеченню допустимості цифрових доказів і, як наслідок, підвищенню ефективності кримінально-правової протидії кіберзлочинам у фінансовій сфері.

Список використаних джерел:

1. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика)* : наук.-практ. журнал. Київ : МНДЦ при РНБО України. 2014. No 1 (32). С. 213–225.

2. Самойлов С. В. Типові слідчі ситуації початкового етапу розслідування шахрайств, що вчиняються з використанням мережі «Інтернет», відповідні їм слідчі версії та алгоритми їх перевірки. *Проблеми правознавства та правоохоронної діяльності.* 2014. No4. С. 25–31. URL: http://nbuv.gov.ua/UJRN/pppd_2014_4_6

3. Павлова Н. В. Особливості початкового етапу розслідування кримінальних правопорушень, вчинених шляхом шахрайства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. No 2. С. 466–471.

4. Свобода Є. Ю., Кофанов А. В., Самодін А. В. та ін. Участь спеціаліста-криміналіста під час проведення окремих слідчих (розшукових) дій : навчальний посібник. Вінниця : ТОВ «Ніланд-ЛТД», 2018. 432 с.

5. Криміналістика : підручник. У 2 т. Т. 1. за ред. В. Ю. Шепітька. Харків : Право, 2019. 456 с.

6. Чаплинський К. О., Рейнгольд А. В., Павлова Н. В. Чаплинський К.О**.** Методика розслідування шахрайства в інтернет-комерції: теорія та практика : монографія. Одеса : Видавництво «Юридика», 2024. 242 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/13318/1/Чаплинський%20К.О._Методика%20розслідування%20шахрайства%20в%20інтернет%20комерції_preview.pdf.

Дата першого надходження статті до видання: 10.10.2025
Дата прийняття статті до друку після рецензування: 10.11.2025
Дата публікації (оприлюднення) статті: 24.11.2025