DOI: 10.34015/2523-4552.2025.3.17
УДК 343.98

Гринько Л. П.,
кандидат юридичних наук, доцент кафедри кримінального права та кримінально-правових дисциплін Полтавського юридичного інституту Національного юридичного університету імені Ярослава Мудрого
ORCID: 0000-0003-1861-8354

ТАКТИЧНІ ОСОБЛИВОСТІ ОГЛЯДУ КОМП'ЮТЕРНИХ ЗАСОБІВ ПІД ЧАС РОЗСЛІДУВАННЯ ШАХРАЙСТВ, УЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ МЕРЕЖІ «ІНТЕРНЕТ»

Стаття присвячена дослідженню тактичних особливостей огляду комп'ютерних засобів як ключового елементу розслідування шахрайств, учинених із використанням мережі «Інтернет». Проаналізовано сутність та зміст огляду комп'ютерних засобів як слідчої (розшукової) дії, визначено його місце в системі збирання та дослідження електронних доказів. Особливу увагу приділено підготовчому етапу, який включає попередню розвідку, визначення кола технічних засобів, залучення спеціалістів і забезпечення належного технічного оснащення. Розкрито специфіку проведення огляду комп'ютерних даних, особливості роботи з метаданими, інформаційними слідами, відновленням видалених файлів, а також тактичні аспекти взаємодії з хмарними сховищами та віддаленими ресурсами. Окремо розглянуто правові засади отримання охоронюваної законом інформації, порядок фіксації результатів та вимоги до забезпечення цілісності доказів.

У результаті зроблено висновок, що ефективність огляду комп'ютерних засобів під час розслідування інтернет-шахрайств залежить від комплексного підходу, який поєднує технічні, процесуальні, організаційні та тактичні компоненти. Саме така інтеграція дозволяє не лише виявляти й документувати цифрові докази, а й забезпечувати їх допустимість і доказову силу у кримінальному провадженні.

Ключові слова: *кіберзлочин, інтернет-шахрайство, огляд комп'ютерних засобів, тактика слідчих дій, цифрові докази, метадані, досудове розслідування.*

Постановка проблеми. Розвиток цифрових технологій останніх десятиліть радикально змінив соціально-економічне середовище, у якому функціонують як бізнес, так і пересічні споживачі. Перехід значної частини комунікацій, послуг та фінансових операцій у віртуальний простір, автоматизація бізнес-процесів, спрощення маркетингових стратегій через онлайн-інструменти сприяли зростанню зручності та швидкості обміну інформацією. Суттєвий вплив на цей процес мали й

глобальні виклики — пандемія COVID-19, яка змусила мільйони людей перейти на дистанційні форми роботи та повномасштабна війна, що стимулювала ще ширше використання цифрових каналів для здійснення щоденних операцій. Усе це зумовило зміну споживчих звичок: онлайн-покупки, дистанційні банківські послуги, цифрові сервіси стали не винятком, а нормою життя для більшості користувачів. Однак ті самі технологічні переваги, які спрощують повсякденні процеси, водночас створили сприятливе середовище для розвитку кіберзлочинності. Зростання обсягів фінансових транзакцій в інтернеті, масове використання електронної комерції, активне поширення онлайн-сервісів і мобільного банкінгу призвели до того, що цифровий простір перетворився на одну з найпривабливіших сфер для шахраїв. Злочинці використовують соціальну інженерію, фішинг, шкідливе програмне забезпечення та інші технологічні інструменти для незаконного заволодіння коштами чи персональними даними громадян. Як наслідок, кількість кібершахрайств зросла у геометричній прогресії, а їхні схеми стали більш складними, багаторівневими та ретельно замаскованими під законну діяльність. У цих умовах особливої актуальності набуває питання ефективної протидії кіберзлочинам, зокрема тих, що пов'язані з шахрайством, учиненим через мережу «Інтернет». Успішне розслідування таких правопорушень вимагає не лише сучасного технічного забезпечення та високого рівня фахової підготовки слідчих, а й застосування специфічних тактичних підходів до проведення процесуальних дій. Серед них особливе місце посідає огляд комп'ютерних засобів — ключовий інструмент збирання, фіксації та аналізу цифрових доказів, без якого неможливо ефективно виявити, документувати й довести обставини вчинення інтернет-шахрайств у сучасних реаліях.

Аналіз останніх досліджень і публікацій. Проблематика організації та тактики проведення слідчих дій, зокрема огляду комп'ютерних засобів, активно досліджується сучасними науковцями. К. О. Чаплинський (2011) розглядає тактику огляду як комплекс ефективних дій, спрямованих на виявлення та фіксацію доказової інформації, а В. С. Гнатенко (2021) акцентує увагу на ролі слідчого у процесі доказування. Л. П. Паламарчук (2005) підкреслює важливість спеціальних технічних знань під час розслідування злочинів у сфері інформаційних технологій, а О. А. Самойленко (2020) пропонує практичні підходи до виявлення та дослідження цифрових доказів. А. В. Коваленко (2023) зосереджується на сучасних викликах і новітніх методах роботи з метаданими, хмарними сервісами та відновленням видалених файлів. Аналіз цих досліджень свідчить про потребу комплексного підходу до тактики огляду комп'ютерних засобів під час розслідування інтернет-шахрайств, що зумовлює актуальність і практичну значущість цієї статті.

Постановка завдання. Мета статті полягає у комплексному аналізі тактичних особливостей огляду комп'ютерних засобів під час розслідування шахрайств, учинених з використанням мережі «Інтернет».

Виклад основного матеріалу. Під тактикою огляду К. О. Чаплинський розуміє комплекс найбільш ра-

ціональних і ефективних дій або найдоцільнішу лінію поведінки уповноважених осіб, що забезпечує виявлення максимальної кількості слідів кримінального правопорушення та речових доказів, інформації про досліджувану подію [1, с. 25]. Погоджуємося з ученим, що рекомендації тактико-криміналістичного характеру мають бути спрямовані саме на забезпечення максимально ефективної поведінки уповноважених осіб під час проведення слідчих (розшукових) та інших процесуальних дій.

Процесуальний зміст слідчих (розшукових) дій визначено у главі 20 КПК України, а підставами для їх проведення є наявність достатніх відомостей, які свідчать про можливість досягнення процесуальної мети. У кримінальних провадженнях щодо інтернет-шахрайств постає низка завдань, більшість з яких вирішується шляхом проведення слідчих (розшукових) дій. Аналіз судово-слідчої практики свідчить, що найчастіше проводиться допит потерпілої особи (97%), огляд (86%), тимчасовий доступ до речей і документів (84%), обшук (53%) та експертиза (26%).

Серед негласних дій найпоширенішими є зняття інформації з комунікаційних мереж, електронних інформаційних систем, а також встановлення місцезнаходження радіообладнання, що визначає необхідність зосередження уваги на тактиці дій, спрямованих на отримання інформації з матеріальних джерел, серед яких огляд займає ключове місце [2, с. 63].

Огляд комп'ютерних даних визначається як гласна слідча (розшукова) дія, що проводиться стороною обвинувачення із використанням електронно-обчислювальної техніки шляхом безпосереднього сприйняття аудіовізуального виразу комп'ютерних даних із метою отримання відомостей про факти, що мають значення для кримінального провадження. Такий огляд є одним із ключових інструментів збирання та дослідження електронних доказів і відіграє важливу роль у криміналістичному процесі доказування. Враховуючи специфіку об'єкта, доцільно розмежовувати огляд комп'ютерних даних і огляд комп'ютерної техніки, які можуть здійснюватися як окремо, так і одночасно, при цьому огляд даних виступає самостійною складовою зі своїми завданнями й об'єктом.

Підготовка до проведення огляду починається з попередньої розвідки: уповноважена особа має ознайомитися з матеріалами провадження, визначити коло пристроїв і носіїв даних, типи файлів, які можуть бути виявлені та очікувану інформацію. Важливо також сформувати склад учасників процесуальної дії, залучивши судових експертів або фахівців із комп'ютерних технологій, які володіють необхідними знаннями та навичками роботи з технічними засобами і програмним забезпеченням. У справах про інтернет-шахрайства доцільно залучати спеціалістів з комп'ютерної техніки та програмного забезпечення, оскільки це дозволяє застосовувати спеціальні технічні засоби, здійснювати фіксацію перебігу обшуку й огляду, ідентифікувати об'єкти, надавати технічні консультації та переносити дані на зовнішні носії для подальшого аналізу [3, с. 8]. До технічних засобів, які необхідні для проведення

огляду належать портативний комп'ютер з автономним живленням, змінні батареї, приводи CD/DVD, інсталяційні носії операційних систем і програмного забезпечення, накопичувачі інформації більшої ємності, блокувачі жорстких дисків, набір інструментів та інші допоміжні пристрої.

На робочій стадії огляду уповноважені особи повинні ознайомитися зі змістом комп'ютерних даних і зафіксувати їх у придатній для сприйняття формі. Дослідження скопійованих або вилучених даних здійснюється шляхом підключення носіїв до службового комп'ютера, відкриття файлів і безпосереднього перегляду інформації. Для уникнення зараження системи шкідливим програмним забезпеченням рекомендується використовувати ізольовані віртуальні середовища. Дані з відкритих джерел в інтернеті чи месенджерів оглядаються через веббраузери або спеціалізовані клієнтські програми. Розвиток цифрових технологій призвів до появи нової категорії доказової інформації — інформаційних слідів, які можуть виникати внаслідок знищення, змін чи пошкодження даних, а також проявлятися як сліди роботи антивірусних програм чи системних логів. Їх виявлення потребує спеціальних методів аналізу. Крім того, злочинці часто застосовують механізми захисту, такі як аутентифікація, криптографічне шифрування чи архівація на віддалених серверах, що ускладнює роботу з інформацією та вимагає залучення спеціалістів [3, с. 8].

Важливим аспектом огляду є робота з метаданими — додатковою інформацією про файли, зокрема їхній розмір, час створення, редагування, формат, користувача тощо, які можуть мати доказове значення. Їх обов'язково потрібно зафіксувати в протоколі. Під час обшуків у справах про інтернет-шахрайства найчастіше вилучаються мобільні телефони, електронні носії, комп'ютерна техніка, програмне забезпечення, аудіо- та відеозаписи, договори й фінансові документи. Це підкреслює центральну роль цифрових джерел інформації у збиранні доказів.

Фіксація перебігу та результатів огляду є ключовим етапом і здійснюється шляхом складання протоколу, у якому відображаються місце, час, учасники, технічні засоби, програмне забезпечення та інші важливі обставини. В описовій частині фіксуються дії уповноважених осіб, результати огляду, витяги з текстів, скріншоти та стопкадри із зазначенням таймкодів. До протоколу можуть додаватися повні копії даних, зокрема побітні копії носіїв. Для підтвердження цілісності інформації рекомендується застосовувати методи гешування. Додатками можуть бути відеозаписи екрана, фототаблиці, роздруківки електронних документів та інші матеріали, які підсилюють доказову базу.

Сучасна практика показує, що значна частина інформації зберігається у хмарних сервісах або на віддалених серверах. Це створює ризик її знищення чи модифікації під час обшуку, зокрема за допомогою мобільних пристроїв. З тактичних міркувань усім присутнім слід заборонити користування телефонами або гаджетами та забезпечити контроль за ними. Також інформація, яка зберігається в операторів і провайдерів, належить до охоронюваної законом таємниці (п. 7 ч. 1 ст. 162 КПК Украї-

ни), і тимчасовий доступ до неї може бути наданий лише за рішенням суду (ч. 6 ст. 163 КПК України) [4].

Залучення спеціалістів відіграє ключову роль не лише під час аналізу даних, а й на етапі технічних процедур. О. А. Самойленко запропонувала алгоритм огляду локального комп'ютера, який включає налаштування BIOS, завантаження операційної системи зі спеціального носія, підготовку контрольного накопичувача, зняття системної інформації, запуск відеозапису екрана, демонстрацію структури носія, копіювання даних, створення образів, перевірку контрольних сум, підготовку другого носія та оформлення протоколу. Для віддалених ресурсів цей алгоритм доповнюється визначенням IP-адреси, маршруту передавання даних і їх збереженням для подальшого дослідження [5, с. 38].

Окремого значення під час розслідування шахрайств, учинених із використанням мережі «Інтернет», набуває робота з віддаленими ресурсами та так званими «хмарними» сервісами. Сучасна інформація дедалі частіше зберігається не на локальних пристроях, а на серверах, розташованих за межами приміщення або навіть країни. Це створює додаткові тактичні виклики, адже слідчий повинен не лише забезпечити доступ до таких джерел, а й зафіксувати інформацію в належній формі для її подальшого використання в доказуванні. Одним із ефективних способів є ідентифікація IP-адреси віддаленого ресурсу, визначення маршруту передавання пакетів даних під час обміну інформацією з ним та збереження цих технічних характеристик як доказової інформації. Такі дії дозволяють підтвердити зв'язок між конкретним користувачем і сервером, встановити місцезнаходження ресурсу або сервера, з якого здійснювались незаконні операції, а також зафіксувати факт доступу до певних даних чи сервісів у конкретний проміжок часу.

Значну увагу слід приділяти й юридичним аспектам доступу до інформації, яка може містити охоронювану законом таємницю. Відповідно до п. 7 ч. 1 ст. 162 КПК України, до такої інформації належать дані, які зберігаються в операторів чи провайдерів телекомунікацій, у тому числі відомості про абонентів, маршрути передачі, тривалість і зміст послуг. Отримання доступу до цієї інформації можливе лише за ухвалою слідчого судді, якщо сторона кримінального провадження доведе можливість використання її як доказу та неможливість доведення обставин іншими способами (ч. 6 ст. 163 КПК України). Такий механізм забезпечує баланс між інтересами досудового розслідування та правами особи на недоторканність приватного життя й конфіденційність комунікацій. У цьому контексті особливого значення набуває належне обґрунтування клопотання про надання тимчасового доступу, яке має чітко вказувати на зв'язок запитуваної інформації з предметом доказування та її значення для встановлення обставин злочину.

Додаткові тактичні особливості виникають під час роботи з електронними документами. Відповідно до ст. 15 Закону України «Про електронну комерцію», якщо законом або договором встановлено строк зберігання окремих видів документів, сторони зобов'язані забезпечити їх архівне зберігання в засобах, які га-

рантують цілісність і незмінність інформації. Це означає, що електронні документи можуть зберігатися як на спеціалізованих серверах суб'єктів господарювання, так і в інформаційно-комунікаційних системах сторонніх провайдерів. Для слідства це відкриває додаткові можливості, але водночас потребує тактично вивірених дій для отримання доступу до цих архівів. Одним із ефективних підходів є взаємодія з адміністраторами таких систем і залучення фахівців, які здатні забезпечити витяг даних без порушення їхньої цілісності та без ризику зміни їх змісту.

Під час роботи з цифровими доказами важливо пам'ятати, що будь-які зміни у структурі даних можуть поставити під сумнів їх автентичність та допустимість у суді. Саме тому під час огляду комп'ютерних засобів особливу увагу приділяють не лише змісту самих даних, а й способу їх отримання та фіксування. Для забезпечення автентичності широко застосовується методика гешування — створення унікального цифрового відбитка інформації до і після її копіювання. Збіг геш-значень підтверджує, що дані не були змінені під час слідчих дій. У складних випадках, коли є підозра на шифрування або приховування доказової інформації, доцільним є призначення комп'ютерно-технічної експертизи, яка дозволяє відновити видалені файли, розшифрувати дані та дослідити залишкові сліди роботи користувачів у системі [6].

Окреме значення має правильне визначення обсягу інформації, яка підлягає фіксації та долученню до матеріалів провадження. Необхідно розмежовувати релевантні дані, що мають значення для встановлення обставин злочину, від другорядних або технічних, які не впливають на зміст доказування. Водночас усі результати огляду, включаючи побітні копії, журнали подій операційних систем, мережеві журнали та дані з хмарних сервісів, мають зберігатися на окремих носіях із дотриманням правил пакування, маркування та зберігання речових доказів. Це необхідно як для підтвердження їх автентичності, так і для можливості повторного дослідження під час судового розгляду.

Тактика огляду комп'ютерних засобів повинна враховувати й людський фактор. Учасники процесуальної дії мають бути поінформовані про свої права та обов'язки, а також про наслідки спроб видалення або модифікації даних. З тактичної точки зору доцільно забезпечити контроль за поведінкою осіб, які перебувають на місці огляду, зокрема обмежити їх доступ до мережі та електронних пристроїв, які можуть бути використані для дистанційного втручання в інформаційні ресурси.

Ефективне проведення огляду також неможливе без ретельного планування взаємодії між слідчим, оперативними підрозділами, експертами та фахівцями з кібербезпеки. Кожен із них виконує свою роль: слідчий забезпечує процесуальну сторону дій і фіксує результати, оперативні працівники забезпечують безпеку та виявлення додаткових джерел доказів, експерти проводять технічний аналіз, а спеціалісти з кібербезпеки відповідають за виявлення та нейтралізацію цифрових загроз. Така командна робота дозволяє підвищити якість та ефективність досудового розслідування.

Висновки. Огляд комп'ютерних засобів у кримінальних провадженнях про шахрайства, учинені із використанням мережі «Інтернет», виступає багатокомпонентним процесом, що поєднує технічні, правові, організаційні та тактичні елементи. Його метою є не лише отримання фактичної інформації, а й забезпечення її процесуальної допустимості та доказової сили. Ефективна реалізація цієї слідчої дії вимагає системного підходу: ретельної підготовки, належного технічного забезпечення, залучення компетентних спеціалістів, дотримання процесуальних гарантій, належного фіксування та збереження отриманих результатів. Комплекс цих дій дає змогу не лише розкрити механізм вчинення злочину, а й простежити цифрові сліди його учасників, підтвердити факт незаконних транзакцій, відновити знищені або приховані дані та сформувати надійну доказову базу для подальшого судового розгляду. Такий підхід є ключовим чинником ефективності боротьби з інтернет-шахрайствами в умовах стрімкого розвитку цифрового середовища та зростання кіберзлочинності.

Список використаних джерел

1. Чаплинський К. О. Організаційно-тактичні основи проведення слідчого огляду. *Криміналістичний вісник*. 2011. № 1 (15). С. 22–29.
2. Гнатенко В. С. Доказування обставин кримінального правопорушення слідчим. *Вісник Харківського національного університету імені В. Н. Каразіна.* Серія: Право. 2021. Випуск 32. С. 61–67.
3. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. ... канд. юрид. наук спец.: 12.00.09. Київ, 2005. 18 с.
4. Кримінально-процесуальний кодекс України : Кодекс України від 28.12.1960 № 1001-05 : станом на 19 листопада 2012 р. URL: https://zakon.rada.gov.ua/laws/show/1001-05#Text (дата звернення: 29.08.2025).
5. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 212 с.
6. Коваленко А. В. Організація і тактика проведення огляду комп'ютерних даних. *Kherson State University Herald Series Legal Sciences*. 2023. № 4. С. 53–58. DOI: https://doi.org/10.32999/ksu2307-8049/2023-4-9

Grynko Larysa, *PhD in law, Associated Professor of the Department of Criminal Law and Criminal Law Disciplines Poltava Law Institute of The Yaroslav Mudryi National Law University*
ORCID: 0000-0003-1861-8354

Tactical Features of Computer Device Examination During The Investigation of Fraud Committed Using The Internet

This article examines the tactical features of computer device inspection as a key element in investigating fraud committed via the Internet. Special attention

is given to the preparatory stage, which includes preliminary analysis, determining the range of technical tools, involving specialists, and ensuring adequate technical support. The study reveals the specifics of computer data examination, features of working with metadata, digital traces, and the recovery of deleted files, as well as tactical aspects of interaction with cloud storage and remote resources. It also addresses the legal framework for obtaining legally protected information, the procedure for documenting results, and the requirements for ensuring the integrity of evidence.

The study concludes that the effectiveness of computer device inspections in investigating internet fraud depends on a comprehensive approach that combines technical, procedural, organizational, and tactical components. Such integration makes it possible not only to identify and document digital evidence but also to ensure its admissibility and evidentiary value in criminal proceedings.

Keywords: *cybercrime, internet fraud, computer device inspection, investigative tactics, digital evidence, metadata, pre-trial investigation.*