



**DOI: 10.21564/2786-7811.2.297362**

**ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС ДОСУДОВОГО  
РОЗСЛІДУВАННЯ ШАХРАЙСТВ,  
ВЧИНЕНИХ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ**

**Гринько Лариса Петрівна,**  
доцент кафедри кримінального права та кримінально-правових дисциплін  
Полтавський юридичний інститут  
Національного юридичного університету імені Ярослава Мудрого

**ORCID:** 0000-0003-1861-8354  
**e-mail:** gull\_ukr@ukr.net

**Анотація.** У статті наголошено, що однією із необхідних умов ефективного розслідування шахрайств, вчинених через мережу Інтернет, є необхідність використання спеціальних знань. Підкреслено, що ефективність розкриття та розслідування шахрайств, вчинених через мережу Інтернет, перед усім, залежить від застосування комплексного підходу, що виявляється у поєднанні різних форм використання спеціальних знань на різних етапах кримінального провадження. Наголошено, що основними формами використання спеціальних знань при розслідуванні досліджуваного шахрайства є отримання консультацій спеціалістів із питань, які потребують спеціальних знань; участь спеціалістів у проведенні слідчих (розшукових) дій; проведення судових експертиз. Процес розкриття та розслідування шахрайств, вчинених через мережу Інтернет, супроводжується провідною роллю спеціаліста у цій сфері, яка полягає в огляді комп'ютерної техніки, цифрових електронних носіїв інформації, мобільних телефонів, опрацюванні робочих записів користувачів комп'ютерної техніки тощо. Дослідження носіїв комп'ютерної інформації дасть змогу достовірно стверджувати про наявність матеріальних слідів вчинення шахрайств (комп'ютерних, електронних, цифрових), професійне її вилучення унеможливе будь-яке пошкодження або знищення наявної інформації. Оскільки механізм вчинення шахрайських дій пов'язаний з використанням низки



електронних носіїв, які відображають інформацію про злочин, та здійсненням ряду операцій, які відбуваються через електронні та телекомунікаційні мережі, по зазначеній категорії справ найчастіше призначають: а) комп'ютерно-технічну експертизу; б) телекомунікаційну; в) товарознавчу; г) судово-економічну та інші.

**Ключові слова:** шахрайство, комп'ютерні технології, шахрайство через мережу Інтернет, кіберзлочини, кіберпростір, судова експертиза.

**USE OF SPECIAL KNOWLEDGE DURING THE PRE-COURT  
INVESTIGATION OF FRAUDS,  
COMMITTED THROUGH THE INTERNET NETWORK**

**Larysa P. Grynko,**

Associated Professor at the Department of Criminal Law  
and Criminal Law Disciplines

Poltava Law Institute of The Yaroslav Mudryi National Law University

**ORCID:** 0000-0003-1861-8354

**e-mail:** gull\_ukr@ukr.net

**Summary.** In article emphasizes that one of the necessary conditions for the effective investigation of fraud committed through the Internet, need to use special knowledge. Emphasizing that the effectiveness of the disclosure and investigation of fraud committed through the Internet depends, first of all, on the application of a comprehensive approach, which is manifested in the combination of various forms of the use of special knowledge at various stages of criminal proceedings. It was emphasized that the main forms of using special knowledge in the investigation of the analyzed fraud are obtaining consultations from specialists on issues that require special knowledge; the participation of specialists in conducting investigative (search) actions; conducting forensic examinations. The process of uncovering and investigating fraud committed through the Internet is accompanied by the leading role of a specialist in this field, consists in the examination of computer equipment, digital electronic media, mobile phones, processing of work records of computer equipment



users, etc. Examine of computer information carriers will make it possible to reliably assert the presence of material traces of fraud (computer, electronic, digital), its professional removal, any damage or destruction of existing information is impossible. Since the mechanism of committing fraudulent actions is related with electronic media that display information about the crime, and the implementation of a number of operations that take place through electronic and telecommunication networks, most often prescribed the following categories of cases : a) computer and technical examination; b) telecommunications; c) commodity expert; d) judicial and commercial and others.

**Key words:** fraud, computer technology, fraud committed through the Internet, cybercrimes, cyberspace, forensics.

**Постановка проблеми.** Бурхливий розвиток інформаційних технологій, комп'ютеризація та інформатизація пронизала усі сфери життєдіяльності суспільства. Такий динамічний і стрімкий розвиток використання мережі Інтернет зумовило глобальну інформатизацію і, як наслідок, виникнення нових можливостей для вчинення кримінальних правопорушень. Інтернет створив передумови для скоєння протиправних діянь, серед яких провідне місце займає шахрайство. З-поміж найпоширеніших схем злочинці використовують злам акаунтів у соцмережах, створення шахрайських сайтів, реєстрацію неправдивих аккаунтів тощо.

На сьогодні кількість кримінальних проваджень за фактом шахрайства зростає. Так, за вісім місяців 2023 року в Україні було відкрито 59 605 кримінальних проваджень. Це найбільший показник за останні два роки. Наприклад, у 2021 році було відкрито 23 847 кримінальних справ за фактом шахрайства, а у 2022 — 32 086. Водночас кількість справ про шахрайство, які доходять до суду, зменшилась. У 2023 році лише кожна дев'ята справа досягає судового розгляду [1]. Серед загальної кількості шахрайств ті, що вчинені через мережу Інтернет складають приблизно 12 %. Зазначені показники не



відображають масштаби шахрайств у цілому, оскільки останніх досить важко оцінити через високу латентність такого виду злочину. Шахрайські схеми постійно удосконалюються, набувають нових способів вчинення, адаптуючись до реалій сьогодення. Такий стан потребує розробки нових ефективних засобів і методів розкриття досліджуваного виду кримінального правопорушення з залученням спеціальних знань під час розслідування шахрайств, вчинених через мережу Інтернет.

**Стан опрацювання обраної проблематики, аналіз останніх публікацій та досліджень.** Вагомий внесок у дослідження теоретичних та практичних питань, пов'язаних з вчиненням шахрайств через мережу Інтернет здійснили такі відомі вчені-криміналісти як А. І. Анапольська, Р. С. Атаманов, Н. Ю. Кириленко, С. М. Князєв, А. В. Крижевський, О. В. Курман, О. Л. Мусієнко, Т. В. Охрімчук, Т. А. Пазинич, Д.А. Птушкін, В. П. Сабадаш, С.В. Самойлов, М. М. Федотов, К.О. Чередник, С. С. Чернявський, С.В. Чучко, С. В. Шапочка, А. Ю. Юрчук та інші.

**Метою статті** є дослідження напрямів використання спеціальних знань при розслідуванні шахрайств, вчинених через мережу Інтернет та визначення їх місця у протидії досліджуваного злочину.

**Виклад основного матеріалу.** Однією із необхідних умов ефективного розслідування шахрайств, вчинених через мережу Інтернет, є необхідність використання спеціальних знань. Професійне використання спеціальних знань під час досудового розслідування є однією з причин його ефективного завершення.

Спеціальні знання – це професійні знання, навички та вміння в галузі криміналістичних досліджень, інженерних технологій, медицини, мистецтва, необхідні для вирішення питань, що виникають під час розслідування та розгляду матеріалів кримінального провадження в суді [2, с. 57].

Ефективність розкриття та розслідування шахрайств, вчинених через мережу Інтернет, перед усім залежить від застосування комплексного підходу,



що виявляється у поєднанні різних форм використання спеціальних знань на різних етапах кримінального провадження. Формами використання спеціальних знань під час розслідування досліджуваного кримінального правопорушення найчастіше є: отримання консультацій спеціалістів із питань, які потребують спеціальних знань; участь спеціалістів у проведенні слідчих (розшукових) дій; проведення судових експертиз.

Для правильного збору та збереження доказів під час розслідування шахрайств, вчинених через мережу Інтернет, необхідно мати відповідні навички у сфері комп'ютерних технологій. Саме тому, поширеним видом залучення спеціаліста є його консультативна діяльність. Під час розслідування досліджуваного злочину допомогу слідчому технічного та програмного характеру можуть надавати різні спеціалісти : програміст, системний інженер, ІТ спеціаліст тощо.

Процес розкриття та розслідування шахрайств, вчинених через мережу Інтернет, супроводжується провідною роллю спеціаліста у цій сфері, яка полягає в огляді комп'ютерної техніки, цифрових електронних носіїв інформації, мобільних телефонів, опрацюванні робочих записів користувачів комп'ютерної техніки тощо. Дослідження носіїв комп'ютерної інформації дасть змогу достовірно стверджувати про наявність матеріальних слідів вчинення шахрайств (комп'ютерних, електронних, цифрових), професійне їх вилучення унеможливе будь-яке пошкодження або знищення наявної інформації.

Спеціаліст надає допомогу під час огляду web-сторінок та web-сайтів, акаунтів користувачів у соціальних мережах з подальшим зберіганням та роздруківкою скріншоту із криміналістично значимою інформацією. Огляд web-сторінки, на якій розміщено сайт певної фірми, з проведенням подальшого експертного дослідження у сфері телекомунікації, надає змогу вивчити зміст інформації стосовно діяльності певних суб'єктів, які мають відношення до події кримінального правопорушення, а також зафіксувати ІР-адресу комп'ютерного



обладнання, з якого здійснювалось управління web-сайтом та визначити Інтернет-провайдера, який надавав доступ до web-сайту [3, с. 65].

Участь спеціаліста в проведенні слідчих (розшукових) дій найбільш поширена при проведенні: огляду комп'ютерної техніки, обшуку, тимчасового доступу до речей та документів, зняті інформації з телекомунікаційних мереж та електронних систем, допиті та ін.

Спеціаліст під час проведення слідчих (розшукових) дій також допомагає виявити спеціальні засоби, встановлені власником в комп'ютері для знищення інформації при несанкціонованому доступі до нього; встановити, чи необхідний пароль для доступу до інформації; які правила його використання та чи не призведе порушення цих правил до знищення файлів [4, с. 201].

У процесі складання протоколу огляду участь спеціаліста полягає у фіксуванні у документах слідчої дії порядку огляду комп'ютерної техніки, здійснених маніпуляцій слідчого чи спеціаліста з нею в процесі проведення слідчої дії з обов'язковим використанням комп'ютерної термінології, зокрема зазначення назв, серії та номерів пристроїв, що вилучаються, наявні на них сліди впливу, дефекти, інші індивідуальні ознаки, конфігурації комп'ютерної техніки з чітким описом усіх комплектуючих (за наявності такої можливості) та пристроїв, назви моделей і серійні номери кожного з пристроїв та іншої інформації із заводських наклейок. Застосування відеозапису покликане забезпечити найбільш точну і повну фіксацію фактів, що мають доказове значення [5].

Водночас призначення судових експертиз є найбільш ефективною процесуальною формою використання спеціальних знань у розслідуванні шахрайств, вчинених через мережу Інтернет. Аналіз судової практики з досліджуваного злочину свідчить про той факт, що судові експертизи призначалися у 90% випадків.

Однією з розповсюджених судових експертиз, яка призначається по шахрайствам, вчинених через мережу Інтернет, є комп'ютерно-технічна



експертиза (призначається у 64 %). Основна мета даної експертизи – це встановлення робочого стану комп'ютерної техніки; встановлення обставин, пов'язаних з використанням комп'ютерної техніки, виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях. Так, у справі № 283/1748/17 висновком комп'ютерно-технічної експертизи від 14.06.2017 року встановлено, що на жорсткому диску «Seagate», модель ST500LT012, серійний номер SBY2WRZ9, об'єм 500Гб ноутбука Lenovo ideapad 100-15IBY, вилученого під час проведення обшуку в помешканні обвинуваченого встановлені браузері Google Chrome, Opera, тобто в даному випадку експертиза комп'ютерної техніки проводилась з метою виявлення інформації у програмах, які використовувались обвинуваченим під час скоєння шахрайства з використанням комп'ютерних технологій; експертиза виявила, що саме з даних браузерів обвинувачений вів переписку з потерпілими особами з приводу замовлення товарів [6]. У іншому прикладі для доведення вини обвинуваченого по справі також було проведено комп'ютерно-технічну експертизу [7].

Комп'ютерно-технічна експертиза залежно від завдань, що вирішуються, поділяється на два різновиди: 1) технічна експертиза комп'ютерів, їх вузлів та пристроїв (встановлення призначення і характеристик комп'ютерної техніки, її технічного стану; можливостей використання для досягнення певної мети тощо); 2) експертизи даних та програмного забезпечення (виявлення інформації, що міститься на комп'ютерних носіях, та визначення її цільового призначення; відновлення знищеної інформації; встановлення характеру змін, внесених у програми тощо) [8, с. 177].

При здійсненні комп'ютерно-технічної експертизи комп'ютера або іншого пристрою підозрюваного або обвинуваченого у вчиненні Інтернет-шахрайства, в залежності від конкретного виду експертизи, проводиться дослідження наступних об'єктів:

1) Апаратні об'єкти:

а. комп'ютери;



- b. комплектуючі для комп'ютерів і інших пристроїв;
- c. периферичні пристрої (принтери, сканери, модеми тощо);
- d. мережеві апаратні засоби (сервери, мережеві кабелі тощо);
- e. інтегровані системи (мобільні телефони, органайзери та ін.).

2) Програмні об'єкти:

- a. системне програмне забезпечення;
- b. прикладне програмне забезпечення.

3) Інформаційні об'єкти (дані):

- a. документи, виготовлені за допомогою комп'ютерних засобів;
- b. дані в мультимедійні форматах (аудіо- та відеофайли, зображення тощо);
- c. комп'ютерна інформація, що міститься в базах даних [9, с. 194].

Основними завданнями судової комп'ютерно-технічної експертизи є: визначення робочого стану комп'ютерно-технічних засобів, а також властивостей, якості, статусу та особливостей використання технічних комп'ютерних систем; встановлення особливостей розробки і використання програмних продуктів (при встановленні фактів використання програмного забезпечення з порушенням авторських прав його розробника); установлення обставин, пов'язаних з використанням комп'ютерно-технічних засобів, інформації та програмного забезпечення; виявлення інформації та програмного забезпечення, що містяться на комп'ютерних носіях; встановлення вартості програмного забезпечення; отримання доступу до інформації на носіях; підтвердження або спростування заявлених розробником характеристик, алгоритмів та властивостей програмного забезпечення; дослідження інформації, створеної користувачем або програмою для реалізації інформаційних процесів; виявлення причин блокування сайтів (віруси, мережеві атаки), а також несанкціонованого втручання в роботу сайту, сервера, комп'ютера, електронної пошти тощо; ідентифікаційне дослідження мережевих комунікацій та інтернет-технологій [10].





Напрямок та обсяг експертного дослідження визначаються питаннями, поставленими слідчим перед експертом.

Оскільки механізм вчинення шахрайських дій пов'язаний з використанням низки електронних носіїв, які відображають інформацію про злочин, та здійсненням ряду операцій, які відбуваються через електронні та телекомунікаційні мережі, по зазначеній категорії справ також призначають судову телекомунікаційну експертизу як різновиду інженерно-технічних експертиз (22%). Одними з найчастіше досліджуваних об'єктів телекомунікаційної експертизи при розслідуванні Інтернет-шахрайств є мобільні телефони, смартфони, планшети. Завданням судової телекомунікаційної експертизи є ототожнення конкретного засобу, програми, користувача мережі, визначення характеристик та параметрів телекомунікаційних систем та засобів, встановлення фактів та способів передачі (отримання) інформації в телекомунікаційних системах, встановлення типу, марки, моделі та інших класифікаційних категорій телекомунікаційних систем та засобів; дослідження алгоритмів обробки інформації та її захисту у сфері телекомунікацій тощо.

Ще одним різновидом судових експертиз, які призначаються по даній категорії справ є судова товарознавча експертиза (складає 19 %). До завдань цієї експертизи відносять визначення вартості, способу виготовлення та належності товару до певної групи чи класифікації тощо.

Судово-економічна експертиза документів фінансово-кредитних операцій, які проходять саме через Інтернет-банкінг призначалась у 12 % випадків. Основною метою проведення судово-економічних експертиз є встановлення документального підтвердження фінансово-кредитних операцій та належності до них документів, які формувались за допомогою комп'ютерної техніки. Експертиза (дослідження) документів фінансово-кредитних операцій, проведених через Інтернет-банкінг, спрямована на дослідження операцій з перерахування та зарахування коштів на поточний рахунок, розрахунків за



участь в онлайн-аукціонах, використання сервісів з переказування або обміну валюти, розрахунків в інтернет-магазинах, внесення коштів на депозит або кредитування. Завдання, які експерти розв'язують під час подібних експертних досліджень, спрямовані на визначення документальної обґрунтованості: банківських операцій з відкриття рахунків та руху грошових коштів на рахунках; операцій з видачі, використання й погашення кредитів і депозитів, а саме — їх оформлення та відображення в обліку [11, с. 468-469]. Так, у справі № 203/1357/19, відповідно до висновку проведеної судово-економічної експертизи, яка досліджувала банківські виписки ТОВ «Метротайл-Україна» по розрахунковому рахунку потерпілої особи, відкритого в АТ «Укрсиббанк» встановлено перерахування грошових коштів на розрахункові рахунки обвинуваченого [12]. Таким чином, судово-економічна експертиза займає провідне місце у протидії шахрайствам, вчинених через мережу Інтернет.

**Висновки та пропозиції.** Дослідження технічних можливостей електронно-обчислювальної техніки та особливостей функціонування мережі Інтернет вимагає використання спеціальних знань при розслідуванні Інтернет-шахрайств, що дозволяє виявити певні факти, які можуть свідчити про шахрайські дії та запобігти подальшій їх реалізації.

## ЛІТЕРАТУРА

1. Ільченко Л. Кількість справ про шахрайство в Україні у 2023 році сягнула історичного антирекорду. *Економічна правда*. 02 жовтня 2023 р. URL: <https://www.epravda.com.ua/news/2023/10/2/704975/>. (дата звернення 11.11.2023).
2. Клименко Н. І. Зміни в правовому регулюванні судово-експертної діяльності. *Криміналістичний вісник*. 2005. № 1. С. 56-60.
3. Криушенко Л.І. Особливості виявлення обставин, що підлягають з'ясуванню під час розслідування шахрайства в банківській сфері. *Науковий вісник Ужгородського національного університету*. 2016. Вип. 39 (2). С. 94-99.



4. Охріменко С.С. Залучення слідчим спеціалістів під час розслідування комп'ютерних злочинів. *Електронний репозитарій НАВС*. С. 198-202. URL: <https://elar.naiu.kiev.ua/server/api/core/bitstreams/9a63eb10-0979-4e71-90b2-0c761bd406e7/content>. (дата звернення 11.11.2023).

5. Самойленко О. А. Протидія кіберзлочинам: криміналістичний аспект: навч.-метод. посіб. Одеса, 2020. 133 с.

6. Вирок Малинського районного суду Житомирської області від 17 квітня 2018 по справі № 283/1748/17. URL: <https://reyestr.court.gov.ua/Review/73413028>. (дата звернення 11.11.2023).

7. Вирок Первомайського міськрайонного суду Миколаївської області, від 10 листопада 2016 року, у справі №484/3014/16-к. URL: <https://reyestr.court.gov.ua/Review/62936930>. (дата звернення 11.11.2023).

8. Волобуєв А. Ф. Розслідування і попередження розкрадань майна у сфері підприємництва : Навч. посіб. / За ред. О. М. Бандурки. Х.: Рубікон, 2000. 272 с.

9. Баєв О. О. Боротьба з кіберзлочинністю: правовий та виховний аспекти. *Спеціальна техніка у правоохоронній діяльності : матеріали V міжнар. наук.-практ. конф. (Київ, 25 листоп. 2011 р.)*. К. : Нац. акад. внутр. справ України, 2012. С. 194-197.

10. Інструкція про призначення та проведення судових експертиз та експертних досліджень : Наказ Міністерства юстиції України від 8 жовтня 1998 р. № 53/5. URL: <https://zakon.rada.gov.ua/laws/show/z0705-98>. (дата звернення 11.11.2023).

11. Говорова К.І. Місце судово-економічної експертизи у протидії шахрайствам з надання послуг у банківській сфері через інтернет. Теорія і практика судової експертизи і криміналістики. 2020. № 22. С. 461-472.

12. Вирок Кировського районного суду м. Дніпропетровська, від 13 серпня 2020 року, у справі №203/1357/19. URL: <https://reyestr.court.gov.ua/Review/90960245>. (дата звернення 11.11.2023).