МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ЛИПКАН ІГОР ІВАНОВИЧ

УДК 343.98:343.131(477)

ОСОБЛИВОСТІ ДОКАЗУВАННЯ У СПРАВАХ ПРО ШАХРАЙСТВО, ВЧИНЕНЕ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук

Ірпінь – 2025

Дисертацією є рукопис

Робота виконана у Науково-дослідному інституті публічного права

Науковий керівник
доктор юридичних наук, професор,
заслужений юрист України
Топчій Василь Васильович,
Державний податковий університет,
директор навчально-наукового інституту права

Офіційні опоненти:
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
Чернявський Сергій Сергійович,
Національна академія внутрішніх справ,
проректор Національної академії внутрішніх справ

доктор юридичних наук, професор
Циганюк Юлія Володимирівна,
Хмельницький університет управління та права імені Леоніда Юзькова,
професор кафедри кримінального права та процесу

Захист відбудеться «28» серпня 2025 року о 13^{00} на засіданні спеціалізованої вченої ради Д 27.855.03 в Державному податковому університеті за адресою: 08205, Київська область, Бучанський р-н, м. Ірпінь, вул. Університетська, 31

З дисертацією можна ознайомитись у бібліотеці Державного податкового університету за адресою: 08205, Київська область, Бучанський р-н, м. Ірпінь, вул. Університетська, 31

Автореферат розісланий «25» липня 2025 року

Вчений секретар
спеціалізованої вченої ради **Ігор ГРИЦЮК**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Розслідування кримінального правопорушення є складним процесом, що охоплює сукупність дій, спрямованих на встановлення події кримінального правопорушення, виявлення особи, яка його вчинила, і доведення її вини. Цей процес є невід'ємною частиною кримінального провадження, а його ефективність визначається якістю розшукової діяльності.

Варто зазначити, що така діяльність охоплює збір доказів, які підтверджують вчинення кримінального правопорушення, а також дотримання законності всіх процесуальних дій. Особливо це стосується розслідування кримінальних правопорушень, що вчиняються з використанням цифрових технологій, які часто потребують негайних і ретельних дій для збереження доказів, оскільки вони можуть бути швидко знищені або модифіковані в кіберпросторі.

Швидкий розвиток технологій, особливо у сфері цифрових технологій, значно розширює як можливості для правопорушників, так і для органів правопорядку, які намагаються адаптуватися до умов сьогодення. З одного боку, технології дають переваги для розвитку економіки та інших галузей суспільної діяльності, зокрема через покращення комунікацій і процесів обміну інформацією. З іншого боку, ці ж технології використовуються для вчинення кримінальних правопорушень, зокрема тих, що стосуються власності, наприклад, комп'ютерні кримінальні правопорушення, кібершахрайство та інші форми протиправних діянь у мережі «Інтернет».

Розвиток цифрових технологій, зміна суспільно-політичного життя в Україні через повномасштабне вторгнення росії на територію України, збільшення кількості хакерських атак вимагають перегляду існуючих підходів до правового оцінювання кримінальних правопорушень, що вчиняються з використанням цифрових технологій. У зв'язку з цим важливо сформувати оновлене й удосконалити існуюче законодавство для забезпечення ефективної протидії кримінально протиправним посяганням, які здійснюються з використанням цифрових технологій.

Кримінальні правопорушення, що вчиняються у сфері цифрових технологій, мають ряд специфічних особливостей, які ускладнюють їхнє виявлення та протидію. Зокрема, інформація про такі кримінальні правопорушення нечасто надходить від джерел, пов'язаних із безпосереднім затриманням підозрюваних осіб у момент вчинення кримінального правопорушення або одразу після нього. Кіберзлочинці використовують технології, які дають змогу приховувати свою особу, місце перебування й сліди кримінально протиправної діяльності (використання VPN, TOR, підроблених облікових записів, шифрування даних тощо). Більшість кримінальних правопорушень у кіберпросторі вчиняються дистанційно, часто з використанням інфраструктури в іншій країні, що ускладнює оперативне реагування та затримання. Потерпілі можуть не одразу виявити факт шахрайства, особливо якщо йдеться про складні схеми обману або викрадення інформації. Це створює часовий розрив між кримінальним правопорушенням і його виявленням. Окрім цього, кіберзлочинці використовують передові технології й методи, які роблять їх діяльність малопомітною для традиційних інструментів моніторингу та виявлення.

Актуальність обраної теми підтверджується й статистичними показниками. За останні п’ять років кількість кримінальних правопорушень, які вчиняються з використанням цифрових технологій, в Україні значно зросла, подвоївшись порівняно з початком періоду. 2018 року було зафіксовано 1 070 кримінальних правопорушень за статтею 362 Кримінального кодексу України (далі – КК України), яка стосується несанкціонованого доступу до інформації, 2019 року – 1 876, 2020 року – 2 231, 2021 року кількість таких кримінальних правопорушень зросла приблизно на 25 % порівняно з 2020 роком. За 2023 рік кіберполіцією було виявлено понад 3 600 кіберзлочинів, з них повідомлено про підозру понад 1 700 особам, що на 59 % перевищує аналогічний показник 2022 року[1]. Ці кримінально протиправні діяння охоплюють хакерські атаки, фішингові кампанії та шахрайство, особливо під час війни.

Перший в історії світовий рейтинг кіберзлочинності, складений у рамках дослідження Оксфордського університету та Університету Нового Південного Вельсу, засвідчує, що Україна займає друге місце після росії за кількістю вчинених кримінальних правопорушень з використанням цифрових технологій[2]. Зростання пов’язане зі збільшенням цифровізації, активністю міжнародних злочинних груп і недостатньою підготовкою частини правоохоронців. Також важливим чинником є кібервійна, яка посилилася через зовнішні атаки на українську критичну інфраструктуру та державні установи.

Кібершахрайство в Україні продовжує бути серйозною проблемою, яка впливає як на громадян, так і на бізнес. 2022 року сума збитків від незаконних дій із платіжними картками зросла на 46 % і досягла 481 млн грн, причому понад 50 % цих випадків були спричинені соціальною інженерією, коли злочинці отримують доступ до конфіденційної інформації через маніпуляції або обман[3]. Найчастіше злочини пов’язані з покупками в інтернеті, шахрайськими фішинговими посиланнями та зламом облікових записів у соціальних мережах.

Також варто зазначити, що близько 2 тисяч шахрайських кол-центрів діють в Україні, значна частина яких спрямована на виманювання коштів у громадян інших країн, через що ускладнюється притягнення до відповідальності. Ці аргументи свідчать про необхідність оновлення методики розслідування кримінальних правопорушень у сфері цифрових технологій.

Окремі питання кримінального процесуального доказування були предметом дослідження в працях О. В. Бабаєвої, В. В. Вапнярчука, І. В. Гловюк, В. П. Гмирка, Ю. М. Грошевого, Є. Г. Коваленка, М. І. Костіна, С. А. Крушинського,

---

[1] Звіт про результати роботи департаменту кіберполіції / Національна поліція України : офіційний вебсайт. URL : https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-u--roczi-969/

[2] World-first "cybercrime index" ranks countries by cybercrime threat level. URL : https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level

[3] Фінансове шахрайство. Як протидіяти кібершахрайству у фінансовому секторі. URL : https://delo.ua/opinions/finansove-saxraistvo-yak-protidiyati-kibersaxraistvu-u-finansovomu-sektori-418081/

О. В. Литвина, А. О. Ляша, М. М. Михеєнка, В. Т. Нора, М. А. Погорецького, В. О. Попелюшка, О. В. Рибалки, С. М. Стахівського, М. М. Стоянова, М. Є. Шумила та інших науковців.

Питання, пов'язані з методикою розслідування кримінальних правопорушень, учинених із використанням цифрових технологій, є актуальним напрямом наукових досліджень. Значний внесок у розробку цієї тематики зробили такі вчені, як: Д. С. Азаров, Б. В. Андрєєв, О. А. Баранов, Ю. М. Батурін, А. С. Білоусов, В. М. Бутузов, О. В. Вакуленко Т. В. Варфоломеєв, М. С. Вертузаєв, О. Г. Волєводз, В. Д. Гавловський, В. О. Голубєв, В. Г. Гончаренко, В. А. Губанов, С. В. Головкін, М. В. Гуцалюк, Д. О. Зиков, М. І. Камлик, М. В. Карчевський, Н. Ю. Кириленко, О. В. Курман, В. А. Коршенко, В. А. Колесник, А. А. Комаров, Т. В. Коршикова О. І. Котляревський, В. В. Крилов, О. П. Кучинська, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд, В. Б. Міщенко, А. Б. Мізерак О. Л. Мусієнко, О. І. Мотлях, Я. В. Неділько, В. І. Оборський, Т. А. Пазинич, Б. В. Романюк, С. В. Самойлов, О. В. Смаглюк, О. М. Стрільців, О. І. Усов, Т. В. Охрімчук, О. С. Тарасенко, В. В. Топчій, Л. Д. Удалова, С. С. Чернявський, С. В. Чучко, В. П. Хорст, В. С. Цимбалюк, В. П. Шеломенцев, О. М. Юрченко та інші.

Вищевказані науковці, безперечно, зробили вагомий внесок у теорію та практику розвитку правової доктрини щодо доказування шахрайств, учинених з використанням цифрових технологій, їхні напрацювання стали основою для розроблення нових обґрунтованих пропозицій щодо вдосконалення розслідування та наукових концепцій з цього питання. Водночас аналіз їхніх праць свідчить про те, що проведені дослідження стосувалися загалом лише окремих теоретичних і практичних питань доказування шахрайств, учинених з використанням цифрових технологій. Проте на сьогодні залишаються недостатньо дослідженими й такими, що не знайшли достатнього правового врегулювання, питання щодо сутності, ознак та видів шахрайства, вчиненого з використанням цифрових технологій, джерел доказів у справах про шахрайство, вчинене з використанням цифрових технологій, напрямів удосконалення доказування у справах про шахрайство, вчинене з використанням цифрових технологій в умовах сьогодення тощо.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722/2019; Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020; Національної стратегії у сфері прав людини на 2021–2023 роки, затвердженої Указом Президента України від 24 березня 2021 року № 119/2021; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, затвердженого Указом Президента України від 11 травня 2023 року № 273/2023; Стратегії кібербезпеки України, затвердженої Указом Президента України від 14 травня 2021 року № 447/2021; Рішення Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», затвердженому Указом Президента України від 13 лютого 2017 року № 32/2017.

Тему дисертації затверджено рішенням Вченої ради Науково-дослідного

інституту публічного права від 17 листопада 2015 року (протокол № 5).

Мета і завдання дослідження. *Метою дослідження* є комплексний аналіз особливостей доказування у справах про шахрайство, вчинене з використанням цифрових технологій, розроблення на його основі науково обґрунтованих пропозицій і рекомендацій щодо вдосконалення правової регламентації та практики застосування законодавства з цього питання.

Відповідно до поставленої мети сформульовані такі *завдання:*

– висвітлити стан наукових досліджень щодо доказування шахрайства, вчиненого з використанням цифрових технологій;

– розглянути віртуальний простір як середовище шахрайства, вчиненого з використанням цифрових технологій;

– дослідити сутність, ознаки та види шахрайства, вчиненого з використанням цифрових технологій;

– визначити обставини, що підлягають доказуванню у справах про шахрайство, вчинене з використанням цифрових технологій;

– проаналізувати джерела доказів у справах про шахрайство, вчинене з використанням цифрових технологій;

– охарактеризувати використання спеціальних знань у справах про шахрайство, вчинене з використанням цифрових технологій;

– висвітлити проблеми доказування у справах про шахрайство, вчинене з використанням цифрових технологій;

– детально дослідити зарубіжний досвід доказування у справах про шахрайство, вчинене з використанням цифрових технологій;

– охарактеризувати міжнародне співробітництво у справах про шахрайство, вчинене з використанням цифрових технологій.

Об'єктом дослідження є суспільні відносини, що виникають у процесі доказування шахрайства, вчиненого з використанням цифрових технологій.

Предметом дослідження є особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій.

Методи дослідження були обрані з урахуванням визначеної мети та поставлених завдань, а також об'єкта й предмета дослідження. Методологічною основою дослідження стали загальнонаукові та спеціальні методи пізнання. *Діалектичний метод* був використаний для розгляду всіх аспектів теми в динаміці, виявлення їх взаємозв'язку та взаємообумовленості. Цей метод застосовувався в розділах 1, 2 та 3 дослідження. Методи *системного аналізу та системно-структурний* метод застосовувалися під час аналізу обставини, що підлягають доказуванню у справах про шахрайство, вчинене з використанням цифрових технологій, та джерел доказів у цих справах (підрозділи 2.1, 2.2). *Статистичний метод* використовувався для обробки емпіричної бази даних, яка слугувала джерелом інформації про об'єкт дослідження (розділи 1, 2, 3). Метод *порівняльного правознавства* дав змогу провести аналіз норм кримінального процесуального законодавства та інших нормативних актів, які регулюють питання доказування у справах про шахрайство, вчинене з використанням цифрових технологій, у кримінальному процесуальному праві України й окремих країнах ЄС (підрозділи 3.2, 3.3). *Соціологічний підхід* застосовувався під час проведення соціологічного

опитування (анкетування) слідчих, оперативних працівників і прокурорів з питань доказування у справах про шахрайство, вчинене з використанням цифрових технологій (розділи 1, 2, 3). *Формально-юридичний підхід* дав змогу визначити сутність, ознаки й види шахрайства, вчиненого з використанням цифрових технологій (підрозділ 1.3).

Емпіричну базу дослідження становлять узагальнені дані, отримані під час аналізу статистичних даних та аналітичних матеріалів місцевих судів, правових позицій Верховного Суду, узагальнені дані проведеного соціологічного опитування 89 слідчих, 76 оперативних працівників, 65 прокурорів, матеріали вивчення 352 кримінальних проваджень у таких областях, як Хмельницька, Черкаська, Вінницька, Рівненська, Тернопільська, Закарпатська, Тернопільська, Львівська, Київська, м. Київ за період з 2016 до 2023 рр.

Наукова новизна одержаних результатів полягає в тому, що за характером і змістом дисертаційна робота є одним із перших комплексних монографічних досліджень особливостей доказування шахрайства, вчиненого з використанням цифрових технологій. Найістотнішими результатами дослідження, що зумовлюють його новизну та визначають особистий внесок у розроблення зазначеної проблематики, є такі положення, висновки та пропозиції:

вперше:

– представлено оновлений теоретичний підхід щодо джерел цифрових доказів, до яких віднесено цифрові документи та інші електронні докази, записи автономних систем, електронні докази, отримані через слідчі (розшукові) дії або негласні слідчі (розшукові) дії, електронні докази, отримані через заходи забезпечення або запобіжні заходи, електронні докази, отримані за допомогою технічних засобів (фото-, кінозйомка, відеозапис), електронні докази, отримані в результаті тимчасового вилучення майна;

– запропоновано зміни до кримінального процесуального законодавства щодо критеріїв допустимості копії цифрового доказу, яка виготовлена без участі спеціаліста в разі відсутності оригіналу цифрового доказу;

– з метою забезпечення уніфікованого підходу до збирання доказів під час розслідування кримінальних правопорушень, вчинених з використанням цифрових технологій, та з метою уникнення неоднакового тлумачення кваліфікуючих ознак за ст. 190 КК України запропоновано внести уточнення до статті 190 КК України щодо специфіки використання технічних засобів у шахрайських схемах;

удосконалено:

– доктринальні положення щодо переліку питань, які можуть бути поставлені експерту під час проведення комп’ютерно-технічної експертизи, зокрема, добавлено такі: чи є на носії інформації дані, які вказують на виконання шкідливого програмного забезпечення? Чи зберігаються на комп’ютерному носії відомості, які були змінені чи видалені, і якщо так, то коли?;

– наукову позицію щодо напрямів удосконалення процедури проведення телекомунікаційних експертиз, до яких віднесено: створення централізованої бази даних для телекомунікаційних експертиз, що містить у собі розробку та впровадження національної або міжнародної бази даних, яка містила б перевірену й актуальну інформацію для судових експертів, створення національних стандартів

для комп'ютерно-технічних і телекомунікаційних експертиз (встановлення чітких стандартів і методичних рекомендацій для проведення телекомунікаційних експертиз), підвищення кваліфікації експертів і забезпечення їх доступом до новітніх наукових досліджень; забезпечення надійного документування та сертифікації програмного забезпечення й технічних засобів;

– доктринальні положення щодо обставин, які мають бути встановлені під час розслідування шахрайств, учинених з використанням цифрових технологій, на основі чого сформовано чотири групи таких обставин, які встановлені за результатами вивчення судово-слідчої практики;

– пропозицію щодо вдосконалення законодавчих норм для забезпечення більш ефективного тимчасового доступу до ключових доказів, що є особливо важливим у розслідуваннях, пов'язаних із сучасними формами шахрайства в кіберпросторі, на основі чого сформульовано пропозиції щодо внесення змін до ст. 166 КПК України;

дістали подальшого розвитку:

– положення щодо пріоритетних напрямів досліджень у сфері доказування шахрайств, вчинених з використанням цифрових технологій, до яких віднесено: розробку алгоритмів протидії новітнім формам кіберзлочинності; вивчення впливу цифрових технологій на методи та способи вчинення кримінальних правопорушень тощо;

– рекомендації щодо зменшення можливостей для шахрайства в електронній комерції, зокрема посилення вимог до ідентифікації користувачів платіжних систем, а саме зобов'язати їх надавати більше інформації про свої особисті дані, забезпечення інтеграції з правоохоронними органами, адже платіжні системи мають співпрацювати з державними органами для швидкого реагування на випадки шахрайства тощо;

– наукова думка ключових елементів системи кіберзахисту в зарубіжних країнах і можливості їхнього використання в Україні.

Практичне значення одержаних результатів полягає в тому, що сформульовані та викладені в роботі положення, висновки можуть бути впроваджені й використані в:

– *законотворчій діяльності* – під час внесення змін до відповідних нормативно-правових актів щодо регулювання розслідування шахрайства, вчиненого з використанням цифрових технологій;

– *практичній діяльності* – як рекомендації під час практичної діяльності правоохоронних органів, а також у процесі проведення занять щодо підвищення кваліфікації;

– *науково-дослідній сфері* – для подальших науково-дослідних розробок;

– *освітньому процесі* – для проведення різних форм занять із здобувачами вищої освіти денної та заочної форм навчання за такими навчальними дисциплінами: «Судові та правоохоронні органи», «Кримінальне процесуальне право України», «Криміналістика» (акт впровадження Державного податкового університету від 8 квітня 2024 року).

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній положення, узагальнення, висновки,

рекомендації та пропозиції обґрунтовано на підставі самостійно проведених досліджень.

У науковій статті «Проблемні питання розслідування шахрайств, вчинених з використанням цифрових технологій», підготовленої спільно В. Топчієм, здобувачем особисто виокремлено напрями покращення процесу доказування кримінальних правопорушень, вчинених з використанням цифрових технологій.

Ідеї та розробки, що належать співавторам, разом з якими були опубліковані наукові статті, в дисертації не використовувалися. Для аргументації окремих положень дисертації використовувалися наукові праці інших учених, на які зроблено посилання.

Апробація результатів дисертації. Основні положення дисертації обговорювалися на засіданнях відділів Науково-дослідного інституту публічного права. Результати дослідження були оприлюднені на 3 міжнародних науково-практичних конференціях, а саме: «Вітчизняна юридична наука в умовах сучасності» (м. Київ, 19–20 липня 2017 р.), «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 12–13 серпня 2020 р.), Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 22–23 вересня 2021 р.).

Публікації. Основні наукові результати дисертації викладені у 8 наукових публікаціях, серед яких 4 статті, опубліковані в юридичних фахових виданнях України, затверджених наказом Міністерства освіти і науки України, 1 – в іноземному фаховому виданні та 3 тези доповідей, опубліковані в збірниках матеріалів міжнародних науково-практичних конференцій.

Структура дисертації. Робота складається із вступу, трьох розділів, що містять дев’ять підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 259 сторінок, з них основний текст – 228 сторінок, список використаних джерел – 24 сторінки (200 найменувань) та 3 додатки на 7 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** розглянуто обґрунтування вибору теми дослідження, визначено рівень наукової розробки проблеми, встановлено зв’язок роботи із науковими програмами, сформульовано мету, завдання, об’єкт і предмет дослідження, описано його методологічну, теоретичну й емпіричну базу, зазначено зв’язок роботи з державними програмами, планами, темами, грантами. Уточнено основні теоретичні положення, які відображають наукову новизну, теоретичне й практичне значення отриманих результатів, а також наведено інформацію про апробацію та публікації.

Розділ 1 «Теоретичні та правові аспекти дослідження доказування шахрайства, вчиненого з використанням цифрових технологій» складається з трьох підрозділів.

У *підрозділі 1.1 «Стан наукових досліджень щодо доказування шахрайства, вчиненого з використанням цифрових технологій»* розглянуто дисертаційні роботи, монографічні дослідження та інші наукові праці, що стосуються особливостей доказування, вчиненого з використанням цифрових технологій.

Зазначено, що питання, пов’язані з методикою розслідування кримінальних правопорушень, учинених із використанням цифрових технологій, є актуальним напрямом наукових досліджень. Значний внесок у розробку цієї тематики зробили такі вчені:

1) Д. С. Азаров, Б. В. Андрєєв, О. А. Баранов, Ю. М. Батурін, В. М. Бутузов – їхні дослідження стосуються особливостей збирання цифрових доказів і технологій боротьби з кіберзлочинами;

2) Т. В. Варфоломеєв, М. С. Вертузаєв, О. Г. Волєводз, В. Д. Гавловський, В. О. Голубєв, В. Г. Гончаренко, В. А. Губанов – досліджували тактику й організацію розслідувань у сфері інформаційних технологій;

3) М. В. Гуцалюк, Д. О. Зиков, М. І. Камлик, М. В. Карчевський, В. А. Колесник – аналізували специфіку використання комп’ютерної техніки в шахрайствах і методи їхнього викриття;

4) А. А. Комаров, О. І. Котляревський, В. В. Крилов, В. Д. Ларичев, А. К. Лебедєв, О. В. Лисодєд, В. Б. Міщенко – досліджували методи аналізу цифрових слідів, залишених кіберзлочинцями;

5) О. І. Мотлях, В. І. Оборський, Б. В. Романюк, О. В. Смаглюк, О. М. Стрільців, О. І. Усов – займалися розробкою методик виявлення та документування кримінальних правопорушень, пов’язаних із незаконним доступом до інформації;

6) С. С. Чернявський, В. П. Хорст, В. С. Цимбалюк, В. П. Шеломенцев, О. М. Юрченко – внесли вклад у розробку профілактичних заходів та вдосконалення нормативно-правової бази у сфері протидії кримінальним правопорушенням, вчиненим з використанням цифрових технологій.

На основі вивчення наукових праць щодо доказування шахрайства, вчиненого з використанням цифрових технологій, зроблено висновок, що сучасними пріоритетними напрямами досліджень у цій сфері є: 1) обґрунтування й розробка методів збирання, фіксації та аналізу цифрових доказів; 2) удосконалення досудового розслідування кримінальних правопорушень, учинених з використанням цифрових технологій, та посилення міжнародного співробітництва у цій сфері, особливо в умовах воєнного стану; 3) потреба у використанні спеціалізованого програмного забезпечення для розслідування кримінальних правопорушень у кіберпросторі; 4) розробка алгоритмів протидії новітнім формам кіберзлочинності; 5) вивчення впливу цифрових технологій на методи та способи вчинення кримінальних правопорушень.

У *підрозділі 1.2 «Віртуальний простір як середовище шахрайства, вчиненого з використанням цифрових технологій»* висвітлено доктринальні позиції та законодавче підґрунтя щодо регулювання віртуального простору як середовища шахрайства, вчиненого з використанням цифрових технологій.

Визначено, що професійне шахрайство є глобальною проблемою сьогодення, і його протидія стає важливим аспектом правоохоронної діяльності в усіх країнах світу. Водночас зазначено, що, хоча конкретні результати протидії шахрайству можуть змінюватися залежно від країни, загальні тенденції та схеми шахрайських дій мають багато спільного в різних регіонах. Зловживання, пов’язані з фінансовими

махінаціями, а також їхня легалізація (відмивання незаконно отриманих доходів), є частими супутниками таких кримінальних правопорушень.

На основі визначень віртуального простору й особливостей його використання як середовища для вчинення шахрайства виокремлено основні труднощі в доказуванні таких кримінально протиправних діянь: 1) анонімність учасників, адже в інтернеті-середовищі важко ідентифікувати шахраїв через анонімність користувачів і можливість використання фальшивих даних; 2) невизначеність щодо умов угоди, оскільки вони часто укладаються на підставі стандартних умов, що можуть бути неправильно зрозумілі чи не належно представлені покупцям; 3) технічні складнощі: для збору доказів потрібно мати доступ до електронного листування, транзакційних записів та іншої цифрової інформації, що може бути технічно складно або не завжди доступно; 4) різноманітність платіжних систем і способів оплати.

Підсумовано, що з метою підвищення ефективності доказування таких кримінальних правопорушень важливо розуміти специфіку укладання електронних угод і порядку здійснення онлайн-розрахунків, зокрема: 1) встановлення чітких алгоритмів для збору електронних доказів (наприклад, логів транзакцій, скріншотів сайтів, записів про угоди); 2) використання новітніх технологій для відстеження шахрайських схем (наприклад, блокчейн для перевірки транзакцій); 3) навчання правоохоронців для розпізнавання ознак шахрайства в інтернеті й ефективного збору доказів.

У *підрозділі 1.3 «Сутність, ознаки та види шахрайства, вчиненого з використанням цифрових технологій»* на основі судово-слідчої практики й аналізу законодавчих актів виокремлено найбільш поширені види шахрайства, вчиненого з використанням цифрових технологій в Україні.

Проаналізувавши судові рішення, пов’язані з інтернет-шахрайством, виявлено суттєві особливості в кримінально-правовій кваліфікації таких дій: 1) кваліфікуюча ознака використання комп’ютерної техніки. Із 439 судових рішень цієї категорії 292 випадки (67 %) були кваліфіковані як шахрайство, вчинене через незаконні операції із використанням цифрових технологій (ч. 3 ст. 190 КК України). У цих випадках злочинці використовували інтернет-майданчики для пропозиції товарів або послуг, яких вони фактично не мали, з метою заволодіння передплатою; 2) кваліфікація як звичайне шахрайство. У третині досліджених вироків дії злочинців були кваліфіковані як звичайне шахрайство (ч. 1-2 ст. 190 КК України). Це спостерігалося навіть за аналогічних обставин, коли злочинці застосовували інтернет-технології для отримання коштів від потерпілих.

Аналіз судових рішень також дав змогу зробити висновок, що в 14 % випадків (21 вирок із 146), коли кваліфікуюча ознака «шляхом незаконних операцій з використанням електронно-обчислювальної техніки» не була інкримінована. Суди наголошували, що сам факт використання інтернет-майданчиків або технічних засобів не завжди є вирішальним для кваліфікації кримінального правопорушення за ознакою застосування цифрових технологій. У деяких випадках кримінально протиправні дії були здійснені без значної інтеграції технічних засобів у механізм шахрайства, наприклад через прямий контакт із потерпілими після онлайн-комунікації. Крім того, органи досудового розслідування іноді не надавали

достатніх доказів того, що технічні засоби були ключовим інструментом для реалізації шахрайської схеми. У таких випадках суди кваліфікували дії винних за загальною нормою шахрайства (ст. 190 КК України) без спеціальної кваліфікуючої ознаки. Суди іноді вважали, що пропозиція неіснуючих товарів через інтернет-платформи є проявом звичайного шахрайства, якщо техніка слугувала лише засобом комунікації, а не інструментом для реалізації незаконних операцій. Така позиція судів вказує на відсутність чіткої межі між «звичайним шахрайством» та шахрайством із використанням електронно-обчислювальної техніки. Це може спричиняти нерівність у підходах до кримінальної відповідальності залежно від судового округу або складу суду.

Зроблено висновок, що неоднозначність підходу до кваліфікації суттєво впливає на процес доказування цифрових доказів і зумовлена такими чинниками: 1) розбіжності в практиці та недостатня уніфікація тлумачення кваліфікуючих ознак. У деяких справах використання інтернет-майданчиків не вважалося вирішальним для застосування ч. 3 ст. 190 КК України; 2) обмеження доказової бази. Не завжди вдавалося довести факт безпосереднього використання комп'ютерної техніки для шахрайства, що призводило до кваліфікації за загальними нормами; 3) невідповідність законодавства сучасним технологіям. Певні аспекти кримінально протиправної діяльності з використанням цифрових технологій потребують більш чіткого врегулювання в КК України. На основі зазначеного для уникнення неоднакового тлумачення судами кваліфікуючих ознак запропоновано внести уточнення до статті 190 КК України щодо специфіки використання технічних засобів у шахрайських схемах.

Розділ 2 «Процесуальні аспекти доказування шахрайства, вчиненого з використанням цифрових технологій» складається з трьох підрозділів.

У *підрозділі 2.1 «Обставини, що підлягають доказуванню у справах про шахрайство, вчинене з використанням цифрових технологій»* визначено перелік обставин, які підлягають доказуванню під час розслідування шахрайства, вчиненого з використанням цифрових технологій, та на основі судово-слідчої практики вдосконалено цей перелік.

Охарактеризовано предмет посягання (гроші, інформація, доступ до банківських рахунків тощо) як обов'язкову обставину, яка підлягає доказуванню під час розслідування шахрайств, учинених з використанням цифрових технологій.

За результатами аналізу судово-слідчої практики встановлено, що часто перерахування коштів потерпілими розглядається окремими судами як добровільна дія, що не може бути кваліфікована як шахрайство, учинене за допомогою використання цифрових технологій. Це створює прогалину в правозастосуванні, адже в цьому випадку саме електронні платіжні системи використовуються як інструмент для отримання кримінально протиправних доходів. На основі цього запропоновано внести зміни до ст. 190 КК України, зокрема чітко визначити, що використання вебсайтів, електронних платіжних систем або інших технологій для обману потерпілих є формою незаконної операції.

Встановлено, що кримінально протиправні дії, вчинені у віртуальному просторі, безпосередньо зачіпають суспільні відносини в цьому середовищі, але законодавство не завжди правильно відображає специфіку цих відносин.

Кібершахрайство може реалізуватися через фішинг, шкідливе програмне забезпечення, соціальну інженерію тощо. Однак ці способи фактично не знаходять відображення в кваліфікаційних ознаках, через що виникають проблеми в доказуванні факту цих кримінальних правопорушень.

Саме тому запропоновано замінити в Кримінальному кодексі України поняття «електронно-обчислювальна техніка» на «цифрові технології», додавши до нього сучасні технології, як-от інтернет, мобільні пристрої, програмне забезпечення, блокчейн тощо. Крім того, доведено, що в кримінальному законодавстві потрібно передбачити спеціальну статтю для кібершахрайства, яка б враховувала всі специфічні способи вчинення цього кримінального правопорушення в умовах цифрового середовища.

У *підрозділі 2.2 «Джерела доказів у справах про шахрайство, вчинене з використанням цифрових технологій»* проаналізовано різні види джерел доказів у справах про шахрайство, вчинене з використанням цифрових технологій.

Особливу увагу звернено на цифрові докази, які дають змогу виокремити їх як специфічну категорію доказів у кримінальному процесі. До їхніх особливостей віднесено: 1) цифрова (електронна) форма: це інформація, представлена у форматі, що може бути збережений, переданий і оброблений за допомогою інформаційно-комунікаційних технологій; 2) наявність електронного носія: інформація має зберігатися або бути доступною на специфічному електронному носієві (фізичному чи віртуальному), що забезпечує її автентичність; 3) релевантність: інформація повинна мати значення для конкретного кримінального провадження, тобто бути безпосередньо пов’язаною з обставинами, які підлягають встановленню; 4) специфічна природа: інформація повинна характеризуватися технічними особливостями, як-от можливість відновлення, копіювання без зміни первісного змісту, наявність метаданих і залежність від певних програмних та апаратних засобів для доступу.

На підставі аналізу доктринальних джерел запропоновано визначення цифрових доказів, під якими потрібно розуміти інформацію в цифровій формі, що збережена або передана за допомогою електронних засобів, яка є релевантною для встановлення обставин у конкретному кримінальному провадженні та має специфічну технічну природу, що забезпечує її автентичність і можливість дослідження.

У *підрозділі 2.3 «Використання спеціальних знань у справах про шахрайство, вчинене з використанням цифрових технологій»* особливості проведення окремих видів експертиз у вищезазначеній категорії кримінальних проваджень.

Згідно з Інструкцією про призначення та проведення судових експертиз, затвердженою наказом Міністерства юстиції України від 08.10.1998 № 53/5, криміналістичні експертизи охоплюють кілька основних напрямів, що можуть бути застосовані під час розслідування шахрайств:

Експертиза документів – для виявлення підробок, зміни або фальсифікації документів, що використовуються шахраєм для створення ілюзії законності своїх дій. Це може охоплювати перевірку підписів, печаток, виправлень, змін або фальшивих реквізитів.

Експертиза цифрових доказів – оскільки шахрайства все частіше здійснюються через інтернет або з використанням цифрових засобів, експертизи комп'ютерних даних, електронної пошти, чатів, онлайн-транзакцій і фінансових записів стають важливими для виявлення шахрайських схем.

Експертиза матеріальних предметів – наприклад, підроблені гроші, цінні папери або інші предмети, що можуть бути використані для обману потерпілих.

Психологічна експертиза – для вивчення поведінки шахрая, його мотивів і способів маніпулювання потерпілими, а також для визначення, чи були особи під впливом психічного тиску або маніпуляцій.

Експертиза підписів – однією з найпоширеніших експертиз у випадках шахрайства є перевірка автентичності підписів на документах, зокрема в разі підробки договорів, кредитних угод або інших важливих юридичних документів.

За результатами аналізу матеріалів кримінальних проваджень та судово-слідчої практики встановлено, що слідчі використовують різні види експертиз для розслідування шахрайств, вчинених за допомогою цифрових технологій. Найбільшу частку серед них займають криміналістичні експертизи, оскільки шахрайства часто пов'язані з підробленням документів, фальсифікацією підписів та іншими маніпуляціями з матеріальними доказами.

Розділ 3 «Напрями вдосконалення доказування у справах про шахрайство, вчинене з використанням цифрових технологій, в умовах сьогодення» складається з трьох підрозділів.

У *підрозділі 3.1 «Проблеми доказування у справах про шахрайство, вчинене з використанням цифрових технологій»* розглянуто основні прогалини в правозастосовній практиці доказування у справах про кібершахрайство.

На основі проведеного анкетування практичних працівників встановлено, що норма про проведення тимчасового доступу до речей і документів у кримінальному процесуальному законодавстві є неефективною. Така позиція сформована на основі декількох чинників. По-перше, процес тимчасового доступу до документів і речей часто затягується. Цей захід є важливим, але повільним і залежить від численних додаткових кроків, як-от потреба в присутності представника організації, у володінні якого зберігаються потрібні документи чи матеріали (наприклад, банківських установ, операторів телекомунікаційних послуг). Це ускладнює процес і збільшує час, потрібний для збору важливої інформації, що може вплинути на успішність розслідування, особливо у справах про шахрайство, вчинене з використанням цифрових технологій.

По-друге, відсутні чіткі процесуальні строки в кримінальному процесуальному законодавстві. Так, у КПК України відсутні чіткі вказівки щодо терміну, впродовж якого слідчий суддя повинен розглянути клопотання про тимчасовий доступ до речей і документів. Це створює правову невизначеність і може призвести до затримок у зборі доказів, що особливо критично у справах, пов'язаних із кібершахрайствами, де швидкість реагування має вирішальне значення.

По-третє, присутні штучні бар'єри в здобутті інформації. Одна з основних проблем, з якою стикаються слідчі, – це штучне ускладнення доступу до інформації, що становить банківську таємницю. Банківські установи часто створюють додаткові

перешкоди для надання цієї інформації, незважаючи на законодавче регулювання, яке має забезпечувати доступ до таких даних у разі кримінальних розслідувань.

По-четверте, наявні законодавчі прогалини щодо банківської таємниці. Так, ст. 62 Закону України «Про банки та банківську діяльність» встановлює спеціальний режим доступу до інформації, що є банківською таємницею, але на практиці цей процес часто ускладнюється бюрократичними вимогами та додатковими обмеженнями, що значно збільшує час, потрібний для отримання доступу до важливих доказів.

Усі ці чинники вказують на потребу в удосконаленні законодавчих норм і процедур для забезпечення більш ефективного доступу до ключових доказів, що є особливо важливим у розслідуваннях, пов'язаних із сучасними формами шахрайства в кіберпросторі. На основі цього сформульовано пропозиції щодо внесення змін до ст. 166 КПК України.

У *підрозділі 3.2 «Зарубіжний досвід доказування у справах про шахрайство, вчинене з використанням цифрових технологій»* досліджено норми законодавства провідних зарубіжних країн щодо доказування у справах про шахрайство, вчинене з використанням цифрових технологій.

Доведено, що вивчення досвіду розвинених зарубіжних країн у протидії інтернет-шахрайствам та його імплементація в національному законодавстві може стати важливим кроком для підвищення ефективності розслідування таких кримінальних правопорушень в Україні.

Аналіз міжнародного досвіду, зокрема в контексті Європейського Союзу, свідчить про важливість раннього виявлення й оперативного реагування на кіберінциденти, що є основою для ефективної стратегії кіберзахисту. В ЄС ці питання отримують високий пріоритет, зокрема завдяки зусиллям спеціалізованих органів, що сприяють оперативному реагуванню на кіберзагрози та забезпеченню захисту інформаційних ресурсів.

Зазначено, що Україна активно бере участь у міжнародному співробітництві в рамках європейських і міжнародних проєктів, зокрема щодо протидії кіберзлочинності. Це співробітництво охоплює численні програми, ініціативи та партнерства з ключовими організаціями, що забезпечують платформу для обміну інформацією та кращими практиками в галузі кібербезпеки. Одним з таких проєктів є CyberCrime@EAP, що є частиною Програми Східного партнерства Європейського Союзу. Цей проєкт спрямований на підтримку країн Східного партнерства, включно із Україною, у боротьбі з кіберзлочинністю, допомагаючи розвивати національні механізми реагування на кіберзагрози та підвищуючи рівень кіберзахисту.

Встановлено, що для покращення ефективності доказування шахрайства, вчиненого з використанням цифрових технологій, потрібно: 1) розвивати культуру протидії шахрайства, забезпечуючи постійну підготовку та навчання співробітників організацій; 2) інвестувати в спеціалізовані технології для виявлення шахрайства, як-от програми для моніторингу транзакцій, аналізу поведінки користувачів і використання машинного навчання для виявлення аномалій; 3) залучати зовнішніх експертів для проведення аудитів і розслідувань, що дасть змогу виявити можливі слабкі місця в захисті й покращити системи безпеки, розвивати законодавчу базу,

що регулює протидію шахрайства, охоплюючи посилення відповідальності за шахрайські дії в інтернеті.

У *підрозділі 3.3 «Міжнародне співробітництво у справах про шахрайство, вчинене з використанням цифрових технологій»* охарактеризовано стан та напрями міжнародного співробітництва у справах про шахрайство, вчинене з використанням цифрових технологій.

На основі аналізу сучасного стану міжнародного співробітництва України в частині розслідування шахрайства, вчиненого за допомогою цифрових технологій, визначено напрями покращення такої співпраці, а саме: посилення міжнародного партнерства (зокрема, розширення участі країн у Будапештській конвенції та залучення ООН до створення нових ініціатив); уніфікація стандартів (встановлення глобальних стандартів для розслідування кіберзлочинів та обміну даними); навчання фахівців (підготовка кіберекспертів, здатних працювати із цифровими доказами й технологіями розслідування); інформування громадян (проведення інформаційних кампаній для підвищення обізнаності про методи соціальної інженерії та захист особистих даних).

ВИСНОВКИ

У **висновках** дисертації наведено теоретичне узагальнення та запропоновано нове розв’язання наукового завдання, що полягає в комплексному дослідженні особливостей доказування шахрайства, вчиненого з використанням цифрових технологій. До основних результатів, сформульованих на підставі дослідження законодавства, наукових джерел і правозастосовної практики, належать такі положення:

1. Встановлено, що сучасний стан протидії шахрайствам, учинених з використанням цифрових технологій, висвітлив ряд важливих проблем у криміналістичній, кримінальній процесуальній науках, які досі залишаються невирішеними. Найсуттєвіші з них стосуються криміналістичної методики, адже саме в цій галузі спостерігається значне відставання рівня науково-методичних розробок від практичних потреб.

Основними питаннями, які потребують подальшого наукового дослідження, є: 1) розробка методик для нових типів правопорушень (значна частина сучасних злочинів, пов’язаних із використанням цифрових технологій, залишається поза увагою розробників методичних рекомендацій); 2) оновлення підходів (традиційні методики розслідування деяких правопорушень (зокрема, шахрайств) не враховують суттєвих змін у способах їхнього вчинення, хоча їхня кримінально-правова форма залишається незмінною); 3) недостатня практична орієнтованість (більшість рекомендацій створено за шаблонними схемами, без урахування реальних потреб слідчої практики).

Зроблено висновок, що на сьогодні існує об’єктивна потреба в розробці комплексної криміналістичної методики, яка: охоплюватиме класифікацію шахрайств за типами технологій, що використовуються злочинцями, передбачатиме алгоритми дій слідчих на різних етапах розслідування, інтегруватиме рекомендації щодо збирання, збереження й аналізу цифрових доказів, враховуватиме потребу у

взаємодії з експертами у сфері цифрових технологій та охоплюватиме питання протидії подібним кримінальним правопорушенням через профілактичні заходи.

2. Проаналізовано думки науковців щодо поняття віртуального середовища, в якому вчиняються кримінальні правопорушення, пов'язані з використанням цифрових технологій. Визначено, що в науковій літературі часто існує консенсус щодо ототожнення понять «кіберпростір», «віртуальний простір» та «інформаційний простір», що дає змогу вільно застосовувати їх у контексті дослідження злочинності, пов'язаної з цифровими технологіями. Зазначено, що «віртуальний простір» є більш конкретним поняттям і однією з основних складових кіберпростору. Враховуючи те, що інтернет є важливим інструментом для злочинців, які здійснюють шахрайства та інші правопорушення в онлайн-просторі, використання терміна «віртуальний простір» для опису саме цих порушень є доцільним.

3. На основі аналізу судових рішень, пов'язаних з кібершахрайством, виявлено суттєві проблеми доказування таких кримінальних правопорушень.

Встановлено відсутність серед суддів чіткої межі між «звичайним шахрайством» і шахрайством із використанням цифрових технологій. Це може спричиняти неоднаковість застосування законодавства, а відтак порушення принципів кримінального та кримінального процесуального права.

Для уникнення неоднакового тлумачення судами кваліфікуючих ознак запропоновано внести зміни до кримінального законодавства, виклавши ч. 4 ст. 190 КК України в такій редакції: «4. Шахрайство, вчинене у великих розмірах або за допомогою незаконних операцій з використанням цифрових технологій, – карається позбавленням волі на строк від трьох до восьми років». А також запропоновано додати примітку до статті, вказавши, що ч. 4 цієї статті може застосовуватись лише в разі використання як інструменту для реалізації незаконних операцій.

4. Виокремлено чотири основні групи обставин, які мають бути встановлені під час розслідування шахрайств, учинених з використанням цифрових технологій:

1) Обставини щодо події кримінального правопорушення: факт учинення шахрайства в кіберпросторі; час учинення шахрайства: тривалість і періодизація злочину, що допомагає визначити ключові моменти в схемі вчинення кримінального правопорушення; просторові межі: визначення місця, де відбулося шахрайство, зокрема визначення джерела кібератак чи електронного втручання, особа потерпілого; способи вчинення шахрайства: вивчення методів, через які здійснювався шахрайський вплив, предмет посягання (гроші, інформація, доступ до банківських рахунків тощо); характер і розмір завданої шкоди: оцінювання матеріальних і нематеріальних збитків для потерпілого, охоплюючи ймовірні майбутні наслідки, джерела електронних (цифрових) слідів.

2) Інші обставини кримінального правопорушення: відомості про причинно-наслідковий зв'язок: обставини, що сприяли вчиненню шахрайства, розгляд зв'язків з іншими кримінальними правопорушеннями, обставини посткримінальної діяльності, відомості про свідків.

3) Обставини щодо підозрюваного: безпосередні ознаки особи підозрюваного, винуватість, мотив і мета підозрюваного, співучасть у вчиненні шахрайства.

4) Обставини, які можуть мати додаткове значення: чинники, які впливають на тяжкість кримінального правопорушення, підстави для закриття провадження чи

звільнення від кримінальної відповідальності; розмір процесуальних витрат: оцінка витрат, пов’язаних з проведенням розслідування та підтримкою судового процесу, що є важливим для визначення покарання або для оцінювання ефективності роботи правоохоронних органів.

5. У результаті дослідження встановлено, що в кримінальному процесуальному законодавстві досі відсутнє визначення поняття «електронний доказ». КПК України не містить чітких положень щодо джерел отримання електронних доказів, а також відсутнє визначення поняття «електронних доказів» у контексті доказування кримінальних правопорушень.

На основі вивчення судової практики встановлено чинники допустимості цифрових доказів:

1) запис телефонних розмов. Якщо телефонна розмова була записана за допомогою програми автоматичного запису, то такий запис може бути допущений як доказ. Це ґрунтується на тому, що така програма є частиною функціоналу пристрою, і немає потреби в додаткових діях для фіксації розмов. Проте запис, зроблений потерпілим на диктофон, може бути визнаний недопустимим, якщо він був здійснений цілеспрямовано без знання або згоди іншої сторони. Це пов’язано з порушенням принципу добросовісності збору доказів;

2) відеозаписи з камер відеоспостереження. Відеозаписи, отримані за допомогою системи відеоспостереження міста, зокрема у Києві, є допустимими доказами. Це пояснюється тим, що система відеоспостереження є відкритою та здійснюється на визначених об’єктах, що не суперечить нормам законодавства щодо потреби в отриманні спеціального дозволу на негласні слідчі (розшукові) дії. Відеоспостереження не є засобом негласного збирання доказів, оскільки воно орієнтоване на загальний контроль і не порушує прав осіб.

На основі аналізу наукових праць запропоновано напрями вдосконалення кримінального процесуального законодавства щодо законодавчого регулювання цифрових доказів, а саме: 1) визначити поняття цифрових доказів, зокрема, що саме може вважатися електронним доказом (записи телефонних розмов, відеозаписи, дані з електронних пристроїв тощо); 2) встановити правові норм щодо джерел отримання електронних доказів, що дасть змогу уникнути порушень прав осіб і забезпечить прозорість у процесі збору доказів; 3) розробити детальні правила для автентифікації та захисту електронних доказів від маніпуляцій, що є критично важливим у разі їхнього використання в судовому процесі.

Крім того, запропоновано внести зміни до законодавства та роз’яснити джерела цифрових доказів, до яких віднесено цифрові документи й інші електронні докази, записи автономних систем, електронні докази, отримані через слідчі (розшукові) дії або негласні слідчі (розшукові) дії, електронні докази, отримані через заходи забезпечення або запобіжні заходи, електронні докази, отримані за допомогою технічних засобів (фото-, кінозйомка, відеозапис), електронні докази, отримані в результаті тимчасового вилучення майна.

Запропоновані пункти щодо джерел електронних доказів є виваженими й відповідають вимогам сучасної правової практики. Вони містять широкий спектр джерел, охоплюючи цифрові документи, записи з автономних систем, електронні докази, отримані через слідчі чи негласні дії, а також докази, отримані через заходи

забезпечення чи тимчасове вилучення майна. Це дасть змогу забезпечити більш ефективний та оперативний процес збору доказів, зокрема в умовах розвитку інформаційних технологій і зростання кіберзлочинності.

Крім того, на практиці також виникають проблеми, які стосуються саме ситуацій, коли оригінали цифрових доказів не можуть бути збережені через технічні обмеження (наприклад, короткий термін зберігання відеозаписів на камерах спостереження). У таких випадках питання допустимості копій доказів стає критичним для кримінального провадження.

Тому запропоновано доповнити частину 4 статті 99 КПК України таким змістом:

«Копія цифрового доказу, виготовлена слідчим, дізнавачем без участі спеціаліста в разі відсутності оригіналу цифрового доказу, може бути визнана судом допустимою, якщо відсутні ознаки втручання з метою зміни відомостей після моменту виготовлення копії».

6. Під час розслідування шахрайств, вчинених за допомогою цифрових технологій, проводяться такі види експертиз:

Почеркознавчі– 34 %. Це найпоширеніший вид експертиз, адже шахраї часто використовують підроблені підписи на документах або інших письмових свідченнях для реалізації кримінально протиправних схем.

Технічні документів – 31 %. Вони важливі для виявлення змін у документах, як-от підробки, виправлення або інші втручання, які можуть свідчити про шахрайство.

Комп’ютерно- експертизи – 14 %. З огляду на сучасні тенденції шахрайства, яке часто здійснюється через інтернет чи з використанням цифрових технологій, ці експертизи допомагають виявляти фальшиві електронні документи або маніпуляції з цифровими даними.

Телекомунікаційна– 13 %. Телекомунікаційна експертиза у справах про шахрайство проводиться, коли є підозра, що телекомунікаційні засоби, як-от телефони, комп’ютери, електронна пошта або соціальні мережі, використовувалися для скоєння злочину. Основна мета такої експертизи – зібрати докази, які можуть підтвердити або спростувати участь підозрюваної особи в шахрайстві.

Дактилоскопічні експертизи – 4 %. Цей вид експертизи допомагає ідентифікувати особу, яка залишила відбитки пальців на документах чи інших предметах, що можуть бути пов’язані з кримінальним правопорушенням тощо.

7. Розглянуто проблеми доказування шахрайств, учинених з використанням цифрових технологій, та запропоновано рекомендації для мінімізації помилок, що виникають у процесі розслідування таких кримінальних правопорушень: забезпечення спеціалізованої підготовки для спеціально уповноважених суб’єктів; забезпечення використання спеціального обладнання (наприклад, сумок або кейсів із захистом від сигналів (Faraday Bags) для ізоляції телефонів від зовнішніх впливів); фіксація процесу вилучення, а саме оформлення детального протоколу, охоплюючи фото- та відеофіксацію всіх дій з пристроєм, проведення консультацій з експертами, а в складних випадках – залучення спеціалістів із цифрової криміналістики.

8. На основі розгляду зарубіжного досвіду встановлено, що ключовими елементами системи кіберзахисту в зарубіжних країнах є: інтеграція технологій і

координація між органами, а саме взаємодія між різними агентствами, як-от ENISA, CERT-EU, EC3, дає змогу швидко реагувати на інциденти й ефективно розслідувати шахрайства, вчинені з використанням цифрових технологій; оперативне реагування, а саме виявлення й блокування атак за допомогою технологічних інструментів (датчики на серверах, моніторинг активності); інтернаціональний підхід. Європейські органи активно взаємодіють між собою і з іншими міжнародними структурами, щоб забезпечити комплексну протидію кібершахрайствам на глобальному рівні.

9. Визначено, що кіберзагрози стали одним із основних ризиків для світової економіки, що підкреслює серйозність ситуації з кібербезпекою. На жаль, низький рівень довіри до правоохоронних органів і небагато звернень до поліції в Україні та ЄС створюють сприятливі умови для шахраїв, що зі свого боку збільшує кількість атак. Зважаючи на зростаючі кіберзагрози, важливо продовжувати освітні ініціативи та підвищувати рівень цифрової грамотності в Україні. Успішний досвід країн, як-от Польща, може слугувати орієнтиром для розвитку програм, які сприяють безпеці користувачів та ефективному захисту від шахраїв.

Для ефективної протидії шахрайствам, учиненим з використання цифрових технологій, важливо уніфікувати: механізми збору електронних доказів, включно із їх прийнятністю в суді; інструменти екстрадиції для швидкого переслідування осіб, які вчинили кримінальні правопорушення в кіберпросторі; процедури спільних розслідувань за участю правоохоронних органів різних держав.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Липкан І. І. Наукові основи доказування шахрайств, вчинених з використанням цифрових технологій. *Юридичний науковий електронний журнал.* 2016. № 2. С. 221–223. URL : http://lsej.org.ua/2_2016/73.pdf.

2. Липкан І. І. Електронні докази у системі доказування шахрайств, вчинених з використанням цифрових технологій. *Knowledge, Education, Law, Management.* 2021. № 4 (40). С. 266–269. URL : https://kelmczasopisma.com/viewpdf/12395.

3. Топчій В. В., Липкан І. І. Проблемні питання розслідування шахрайств, вчинених з використанням цифрових технологій. *Юридична наука*. 2020. № 3, том 2. С. 150–157. URL : https://journal-nam.com.ua/index.php/journal/article/view/734.

4. Липкан І. І. Сучасні види шахрайств, вчинених з використанням цифрових технологій. *Держава та регіони. Серія: Право*. 2017. № 1 (55). С. 141–144. URL : http://www.law.stateandregions.zp.ua/archive/1_2017/28.pdf.

5. Липкан І. І. Поняття віртуального простору як середовища для вчинення кібершахрайств. *Право та державне управління*. 2022. № 3. С. 399–403. URL : http://pdu-journal.kpu.zp.ua/archive/3_2022/61.pdf.

6. Липкан І. І. Щодо необхідності оновлення методики розслідування шахрайств, вчинених з використанням цифрових технологій. *Вітчизняна юридична наука в умовах сучасності* : матеріали Міжнародної науково-практичної конференції, м. Київ, 19–20 липня 2017 року. Київ : Науково-дослідний інститут публічного права, 2017. С. 26–28.

7. Липкан І. І. Проблеми доказування шахрайств, вчинених з використанням

цифрових технологій. *Виклики сучасності та наукові підходи до їх вирішення* : матеріали Міжнародної науково-практичної конференції, м. Київ, 12–13 серпня 2020 р. Київ : Науково-дослідний інститут публічного права, 2020. С. 152–154.

8. Липкан І. І. Особливості мережі Інтернет як середовища для вчинення кібершахрайств. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення* : матеріали Міжнародної науково-практичної конференції, м. Київ, 22–23 вересня 2021 р. Київ : Науково-дослідний інститут публічного права, 2021. С. 136–137.

АНОТАЦІЯ

Липкан І. І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій. – *Рукопис*.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Державний податковий університет, Ірпінь, 2025.

Дисертацію присвячено комплексному дослідженню особливостей доказування шахрайств, учинених з використанням цифрових технологій. Висвітлено стан наукових досліджень щодо доказування шахрайства, вчиненого з використанням цифрових технологій. Розглянуто віртуальний простір як середовище шахрайства, вчиненого з використанням цифрових технологій. Досліджено сутність, ознаки та види шахрайства, вчиненого з використанням цифрових технологій.

Визначено коло обставин, що підлягають доказуванню у справах про шахрайство, вчинене з використанням цифрових технологій. Проаналізовано джерела доказів у справах про шахрайство, вчинене з використанням цифрових технологій. Охарактеризовано використання спеціальних знань у справах про шахрайство, вчинене з використанням цифрових технологій. Висвітлено проблеми доказування у справах про шахрайство, вчинене з використанням цифрових технологій. Доведено, що призначення судових експертиз є важливим інструментом під час розслідування шахрайств, особливо коли йдеться про виявлення підроблених документів, використаних злочинцями для досягнення своїх цілей. Криміналістичні експертизи є основним класом експертиз, які проводяться для з'ясування обставин, що можуть стосуватися як самого шахрайства, так і конкретних елементів кримінального правопорушення, як-от підроблені документи, печатки, підписи чи інші предмети, що мають юридичну значимість.

Досліджено зарубіжний досвід доказування у справах про шахрайство, вчинене з використанням цифрових технологій. Охарактеризовано міжнародне співробітництво у справах про шахрайство, вчинене з використанням цифрових технологій. Встановлено, що для ефективної протидії шахрайствам, учиненим з використання цифрових технологій, важливо уніфікувати: механізми збору електронних доказів, охоплюючи їх прийнятність у суді; інструменти екстрадиції

для швидкого переслідування осіб, які вчинили кримінальні правопорушення в кіберпросторі тощо.

Ключові слова: кримінальні правопорушення, доказування, цифрові технології, шахрайство, кібершахрайство, кримінальне провадження, досудове розслідування, комп'ютерно-технічна експертиза.

SUMMARY

Lypkan I. I. Peculiarities of proof in cases of fraud committed with the use of digital technologies. – *The manuscript*.

Thesis for obtaining the scientific degree of candidate of legal sciences on the specialty 12.00.09 – criminal procedure and forensics; forensic examination; operational and investigative activities. – State Tax University, Irpin, 2025.

The thesis is devoted to a comprehensive study of the peculiarities of proving fraud committed with the use of digital technologies. The state of scientific research on proving fraud committed with the use of digital technologies is highlighted. The virtual space as an environment of fraud committed with the use of digital technologies is considered. The essence, signs and types of fraud committed with the use of digital technologies are investigated.

The author defines the range of circumstances to be proved in cases of fraud committed with the use of digital technologies. The sources of evidence in cases of fraud committed with the use of digital technologies are analysed. The use of specialised knowledge in cases of fraud committed with the use of digital technologies is characterised. The problems of proof in cases of fraud committed with the use of digital technologies are highlighted. It is proved that the appointment of forensic examinations is an important tool in the investigation of fraud, especially when it comes to identifying forged documents used by criminals to achieve their goals. Forensic examinations are the main class of examinations conducted to clarify the circumstances that may relate to both the fraud itself and specific elements of a criminal offence, such as forged documents, seals, signatures or other items of legal significance.

The author examines foreign experience of proving in cases of fraud committed with the use of digital technologies. The author describes international cooperation in cases of fraud committed with the use of digital technologies. It is established that in order to effectively counteract frauds committed using digital technologies, it is important to unify the following: mechanisms for collecting electronic evidence, including its admissibility in court; extradition tools for the rapid prosecution of persons who have committed criminal offences in cyberspace.

Key words: criminal offences, evidence, digital technologies, fraud, cyber fraud, criminal proceedings, pre-trial investigation, computer forensics.

Підписано до друку 23.07.2025. Формат 60×84/16.
Папір офсетний. Друк офсетний.
Друк. арк. 0,8. Тираж 100 прим.
Замов. № ____.

Видрукувано в Державному податковому університеті.
08205, Київської обл., Бучанський р-н, м. Ірпінь, вул. Університетська, 31