НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова
праця на правах рукопису

ЛИПКАН ІГОР ІВАНОВИЧ

УДК 343.98: 343.131 (477)

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

12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність»

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

І.І. Липкан

Науковий керівник: **Топчій Василь Васильович,**
доктор юридичних наук, професор,
заслужений юрист України

Київ - 2025

АНОТАЦІЯ

Липкан І. І. Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. – Науково-дослідний інститут публічного права, 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.

На підставі аналізу доктринальних джерел запропоновано визначення цифрових (електронних) доказів, під якими потрібно розуміти інформацію у цифровій формі, 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.

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.

Встановлено, що кримінально протиправні дії, вчинені у віртуальному просторі, безпосередньо зачіпають суспільні відносини у 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 у кваліфікаційних ознаках, через що виникають проблеми у доказуванні факту цих кримінальних правопорушень.

Охарактеризовано використання спеціальних знань у справах про шахрайство, вчинене з використанням цифрових технологій. Доведено, що призначення судових експертиз є важливим інструментом при розслідуванні 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, таких як підроблені документи, печатки, підписи чи інші предмети, що мають юридичну значимість.

Висвітлено проблеми доказування у справах про шахрайство, вчинене з використанням цифрових технологій.

На основі аналізу наукових праць запропоновано напрями удосконалення 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 дозволить уникнути порушень прав осіб і забезпечить прозорість у процесі збору доказів; 3) розробити детальні правила для автентифікації і захисту електронних доказів від маніпуляцій, що є критично важливим у разі їх використання в судовому процесі.

Зроблено висновок, що на сьогодні існує об’єктивна необхідність у розробці комплексної криміналістичної методики, яка: включатиме класифікацію шахрайств за типами технологій, що використовуються злочинцями, передбачатиме алгоритми дій слідчих на різних етапах розслідування, інтегрує рекомендації щодо збирання, збереження й аналізу

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

Досліджено зарубіжний досвід доказування у справах про шахрайство, вчинене з використанням цифрових технологій. Аналіз міжнародного досвіду, зокрема в контексті Європейського Союзу, свідчить про важливість раннього виявлення та 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 і забезпеченню захисту інформаційних ресурсів.

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, включаючи їх прийнятність у суді; інструменти екстрадиції для швидкого переслідування осіб, які вчинили кримінальні правопорушення у кіберпросторі; процедури спільних розслідувань з участю правоохоронних органів різних держав.

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 і обміну даними); навчання фахівців (підготовка кіберекспертів, здатних працювати з цифровими доказами та технологіями розслідування); інформування громадян (проведення інформаційних кампаній для підвищення обізнаності про методи соціальної інженерії та захист особистих даних).

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. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Candidate in Law Sciences in the speciality 12.00.09 – criminal process and forensic science; judicial examination; operational and investigative activities. - Scientific and Research Institute of Public Law, State Tax University, Irpin, 2025.

The dissertation 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.

Based on the analysis of doctrinal sources, the author proposes a definition of digital (electronic) evidence, which should be understood as information in digital form, stored or transmitted by electronic means, which is relevant for establishing the circumstances in a particular criminal proceeding and has a specific technical nature which ensures its authenticity and the possibility of research.

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.

It is established that criminal acts committed in the virtual space directly affect social relations in this environment, but legislation does not always correctly reflect the specifics of these relations. Cyber fraud can be committed

through phishing, malware, social engineering, etc. However, these methods are not actually reflected in the qualifying features, which creates problems in proving the fact of these criminal offences.

The author characterises the use of specialised knowledge in cases of fraud committed with the use of digital technologies. 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 which 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 highlights the problems of proof in cases of fraud committed with the use of digital technologies.

Based on the analysis of scientific works, the author proposes the directions of improvement of criminal procedure legislation with regard to legislative regulation of digital evidence, namely: 1) to define the concept of digital evidence, in particular, what exactly can be considered electronic evidence (telephone records, video recordings, data from electronic devices, etc.); 2) to establish legal norms regarding the sources of obtaining electronic evidence, which will avoid violations of human rights and ensure transparency in the process of evidence collection; 3) to develop detailed rules for authentication and protection of electronic evidence from manipulation, which is critical when it is used in court proceedings.

It is concluded that today there is an objective need to develop a comprehensive forensic methodology which will: include classification of frauds by the types of technologies used by criminals, provide for algorithms of investigators' actions at different stages of investigation, integrate recommendations for collection, preservation and analysis of digital evidence, take into account the need to interact with experts in the field of digital technologies and cover the issues of countering such criminal offences through

preventive measures.

The author examines foreign experience of proving cases of fraud committed with the use of digital technologies. The analysis of international experience, in particular in the context of the European Union, shows the importance of early detection and prompt response to cyber incidents, which is the basis for an effective cyber defence strategy. In the EU, these issues are given a high priority, in particular through the efforts of specialised bodies that facilitate rapid response to cyber threats and ensure the protection of information resources.

The article 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 with the use of 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; procedures for joint investigations involving law enforcement agencies of different states.

Based on the analysis of the current state of Ukraine's international cooperation in terms of investigating fraud committed through digital technologies, the author identifies the areas for improving such cooperation, namely: strengthening international partnership (in particular, expanding the participation of countries in the Budapest Convention and involving the UN in creating new initiatives; unification of standards (establishing global standards for cybercrime investigation and data exchange); training of specialists (training of cyber experts capable of working with digital evidence and technology).

Keywords: criminal offences, evidence, digital technologies, fraud, cyber fraud, criminal proceedings, pre-trial investigation, computer and technical expertise.

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.

ЗМІСТ

ВСТУП

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

---

[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/

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, 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 та обсяг 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.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ ДОСЛІДЖЕННЯ ДОКАЗУВАННЯ ШАХРАЙСТВА, ВЧИНЕНОГО З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

1.1. Стан наукових досліджень щодо доказування шахрайства, вчиненого з використанням цифрових технологій

Поняття «комп'ютерне шахрайство» виникло внаслідок активного впровадження комп'ютерних технологій і систем у повсякденне життя, що зумовило зміну способів і предметів посягання у сфері економічних кримінальних правопорушень. У 70-х роках минулого століття, зі зростанням популярності комп'ютерних технологій, законодавчі органи у різних країнах зіткнулися з проблемою кваліфікації нових видів протиправних діянь, які не «вписувалися» у традиційні підходи до правової регламентації [199].

Кримінальні парвопорушення у сфері цифрових технологій є специфічною категорією кримінальних правопорушень, яка характеризується інноваційними методами вчинення та предметом посягання. Враховуючи динамічний розвиток технологій, виникає потреба у своєчасному оновленні законодавства для належної протидії таким правопорушенням і гарантування безпеки інформаційного простору [89; 3].

Варто зазначити, що у науці використовуються різні поняття, які характеризують цифрові технології: «електронно-обчислювальна техніка», «комп'ютер» і «кібертехнології» [11]. Різні підходи до визначення цих термінів пов'язані з їх багатогранністю та складністю їх розуміння, а також із постійним розширенням меж їх використання.

Проте, на нашу думку, різноманіття наукових підходів до визначення понять, пов'язаних із цифровими технологіями, є важливим етапом у розвитку відповідної наукової та правової бази. Це стимулює дослідження нових аспектів явищ і сприяє адаптації законодавства до викликів сучасності.

Однак для забезпечення ефективної протидії кіберзлочинності необхідно забезпечити уніфікацію термінології, зокрема на міжнародному рівні. Саме тому розглянемо різні наукові підходи до визначення вищевказаних понять і кримінальних правопорушень, пов'язаних з використанням цифрових технологій.

М. І. Мельник визначає ознаки використання цифрових технологій при вчиненні шахрайства, що дозволяє відмежувати цей вид кримінального правопорушення від інших форм шахрайства. Його визначення містить два основні аспекти:

1. Спрямованість на заволодіння майном або придбання права на майно. Шахрайство, вчинене з використанням цифрових технологій, має включати операції, в основі яких лежить обман або зловживання довірою, що реалізуються виключно через застосування цифрових технологій. Наприклад, це може бути здійснення: електронних платежів, маніпуляцій з безготівковими коштами, використання електронних систем для фальсифікації фінансових транзакцій. Такі дії є неможливими без застосування цифрових технологій, що робить техніку ключовим елементом у механізмі кримінального правопорушення.

2. Обмеження складу шахрайства із використанням цифрових технологій. Якщо такі технології використовується для вчинення дій, які можуть бути виконані іншими засобами (наприклад, набір тексту або створення документа), то це не створює специфічного складу шахрайства з використанням цифрових технологій. У таких випадках техніка відіграє лише допоміжну роль і не визначає суті правопорушення [3, с. 197].

Відповідно до визначень, наведених у Великому тлумачному словнику сучасної української мови, поняття «електронно-обчислювальна техніка» можна розглядати через два ключові аспекти: 1) електронно-обчислювальна - це характеристика техніки або процесів, що виконуються із застосуванням електроніки; 2) обчислювальна техніка визначається як галузь техніки, що охоплює як теоретичні основи, так і практичні аспекти обчислювальних

машин. Це означає, що поняття включає не лише самі технічні пристрої (комп'ютери, сервери, спеціалізовані машини), але й методи, принципи та алгоритми їх роботи, а також галузі знань, що забезпечують їх ефективне використання [13, с. 145].

Окрім цього, у Великому тлумачному словнику сучасної української мови визначено низку термінів, пов'язаних із електронно-обчислювальною технікою, які мають важливе значення як для правозастосування, так і для наукових досліджень. Електронно-обчислювальна машина (ЕОМ) - це цифрова обчислювальна машина, основні вузли якої реалізовані засобами електроніки. Це визначення наголошує на технічній основі ЕОМ та її цифровій природі; персональна обчислювальна машина: Це тип ЕОМ, що призначений для обслуговування одного користувача, характеризується невеликими габаритами, зазвичай ототожнюється з персональним комп'ютером (ПК). Комп'ютер визначається як електронно-обчислювальна машина (ЕОМ), що робить ці поняття тотожними [13, с. 156].

Таким чином, поняття «електронно-обчислювальна техніка» виступає універсальною категорією, що враховує динамічний розвиток технологій і створює умови для ефективного правового регулювання цифрових кримінальних правопорушень.

Ми вважаємо, що термін «електронно-обчислювальна техніка», який використовується у Кримінальному кодексі України, є застарілим і давно вже не відповідає ні реаліям сьогодення, ні вимогам законодавства. Натомість використовуються терміни «інформаційні технології», «цифрові технології» у законодавстві і в практиці його застосування. Так, із набранням чинності Закону України «Про цифровий контент та цифрові послуги» у 2024 році впроваджені у використання терміни «цифрові послуги», «цифрові технології», «цифровий контент» . Саме тому пропонуємо замінити у КК України термін «електронно-обчислювальна техніка» на «цифрові технології». Таку позицію підтримали й опитані практичні працівники (Додаток А).

Цифрові технології - це електронні інструменти, пристрої та ресурси , які обробляють генерують або зберігають дані. Найбільш розповсюджені приклади - соціальні мережі, ігри, мультимедіа та мобільні телефони.

Варто зазначити, що шахрайство з використанням цифрових технологій постійно еволюціонує, зумовлюючи виникнення нових видів кримінальних правопорушень або удосконалення вже існуючих схем. Науковці розглядають такі види шахрайства:

1. Шахрайство у сфері дистанційного банківського обслуговування: фейкові банки – це створення підроблених вебсайтів або додатків банків для отримання персональних даних клієнтів; електронні віртуальні гаманці - це маніпуляції з онлайн-гаманцями для крадіжки коштів; фішинг – це отримання конфіденційної інформації через підроблені електронні листи, SMS або сайти; креммінг – це модифікація банкоматів для викрадення даних карток.

2. Шахрайство в електронних платіжних системах: фейкові електронні листи: надсилання повідомлень від імені відомих організацій для отримання доступу до рахунків; інтернет-аукціони і лотереї: підроблені аукціони та розіграші, що приманюють жертв обіцянками виграшів; віртуальне казино й тоталізатори, нелегальні або фейкові азартні платформи.

3. Кредитне шахрайство: оформлення кредитів на ім'я жертви через викрадені персональні дані.

4. Кіберсквоттинг: захоплення доменних імен для подальшого перепродажу їх законним власникам або використання у шахрайських схемах.

5. *Банкоматне шахрайство*: скіммінг – це використання пристроїв для зчитування даних банківських карток з метою подальшого їх дублювання, використання «білого пластику», застосування підроблених карток із записаними на них викраденими даними.

6. *Шахрайство за допомогою шкідливого програмного забезпечення*: spyware - програми для збору інформації про жертву без її відома; keyloggers

– інструменти для запису натискань клавіш і крадіжки паролів; поах-програми – використання програмного забезпечення для віддаленого доступу до пристроїв жертви.

7. SMS-шахрайство (Smishing): надсилання підроблених SMS із запитом конфіденційної інформації або вимогою переказу грошей.

8. Інтернет-жебрацтво (cyber-begging): використання емоційних історій на платформах для збору коштів з метою власного збагачення.

9. Рерайтинг, серфінг: обман з використанням обіцянок легкого заробітку через фейкові вакансії або сайти [187, с. 145].

Така еволюція шахрайства з використанням цифрових технологій демонструє складність адаптації правоохоронних органів і законодавства до нових викликів. Збільшення кількості таких кримінальних правопорушень обумовлена високою доступністю технологій, а також низькою обізнаністю жертв про загрози в цифровому середовищі.

Як зазначає Л. М. Кривоченко, шахрайство, вчинене за допомогою таких засобів, вирізняється своїми особливостями, зокрема застосування цифрових технологій є специфічним інструментом, який дозволяє обходити традиційні механізми захисту прав людини. Використання техніки полегшує доступ до великих фінансових або інформаційних ресурсів. Наприклад, злам банківських рахунків або фішингові атаки дають змогу заволодіти значними коштами [6, с. 160], а М. І. Хавронюк вважає, що цифрові технології у ч. 3 ст. 190 КК України є засобом вчинення шахрайства [176, с. 196].

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:

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 кримінальними правопорушеннями з використанням цифрових технологій;

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 цифрових технологій.

3) М. В. Гуцалюк, Д. О. Зиков, М. І. Камлик, М. В. Карчевський, В. А. Колесник — аналізували специфіку використання комп'ютерної техніки при вчиненні шахрайств і методи їх 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 кіберзлочинності.

Пріоритетними напрямами досліджень у цій сфері стали:

1. Розробка методів збирання, фіксації та аналізу цифрових доказів.
2. Особливості розслідування кіберзлочинів, зокрема міжнародне співробітництво у цій сфері.
3. Використання спеціалізованого програмного забезпечення для розслідування кримінальних правопорушень вчинених за допомогою цифрових технологій.
4. Розробка алгоритмів протидії новітнім формам кіберзлочинності.
5. Вивчення впливу цифрових технологій на методи та способи вчинення кримінальних правопорушень.

Одним із перших кроків у напрямі криміналістичного вивчення кримінальних правопорушень, пов'язаних із використанням цифрових технологій, є дослідження О. І. Мотляха в його дисертації «Питання

методики розслідування злочинів у сфері інформаційних комп'ютерних технологій» (2005). У своїй роботі вчений запропонував криміналістичну характеристику таких правопорушень як інформаційну модель [115, с. 10].

О. І. Мотлях пропонує розглядати такі структурні елементи криміналістичної характеристики:

Способи вчинення кримінального правопорушення:

Безпосередній доступ до комп'ютерної інформації або операційної системи - включає різні методи прямого доступу до даних, такі як хакерські атаки, несанкціонований доступ через фізичні чи програмні вразливості.

Видалений (опосередкований) доступ - доступ через мережі Інтернет або інші канали зв'язку, що дозволяє зловмиснику працювати з віддалених локацій.

Виготовлення і розповсюдження шкідливих програм - створення вірусів, троянів, програм для дистанційного контролю тощо, які можуть бути поширені через електронні носії інформації або Інтернет.

Слідова картина кримінальних правопорушень:

Незаконне втручання в роботу ЕОМ, систем і комп'ютерних мереж - фіксація цифрових слідів, що вказують на злом, вторгнення в системи або мережі, зміну їх роботи.

Викрадення, привласнення або вимагання комп'ютерної інформації - дослідження слідів, які вказують на несанкціонований доступ до конфіденційної або цінної інформації.

Порушення правил експлуатації автоматизованих систем - з'ясування факту використання систем не за призначенням, порушення протоколів або політик безпеки, що призвело до неправомірних дій.

Особливості особи злочинця, мотиви і мета кримінального правопорушення:

Вік злочинців - статистика показує, що більшість злочинців у сфері комп'ютерних технологій перебувають у віковій групі від 20 до 40 років, але також є випадки серед молоді до 20 років та осіб старших за 40 років.

Мотиви та мета - дослідження мотивів і цілей, з якими здійснюються комп'ютерні кримінальні правопорушення, може виявити прагнення до фінансової вигоди, помсти, політичних цілей чи навіть соціальної активності (наприклад, хактивізм).

Обставини вчинення кримінального правопорушення:

Обставини можуть варіюватися в залежності від контексту, наприклад, мета злочину може бути спрямована на фінансову вигоду, а сама дія може здійснюватися у рамках професійної діяльності (наприклад, зловживання службовим становищем), або ж може бути результатом індивідуальних мотивів злочинця (наприклад, особисті мотиви або бажання проявити технічні здібності) [115, с. 13].

Отже, науковець відзначає важливість методичного підходу до розслідування таких кримінальних правопорушень, оскільки сфера цифрових технологій є специфічною і потребує від слідчих високої кваліфікації та спеціальних знань у галузі цифрових технологій. Таким чином, дослідження науковця стало важливим етапом у розвитку криміналістики в контексті цифрових кримінальних правопорушень, зокрема в частині методики розслідування правопорушень, пов'язаних з інформаційними комп'ютерними технологіями.

Л. П. Паламарчук у своїй дисертаційній роботі «Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» детально аналізує питання, що стосуються методики розслідування таких кримінальних правопорушень, зокрема розглядає способи їх вчинення і слідову картину [127, с. 6]

З розвитком теорії криміналістики та накопиченням практичного матеріалу, почали активно вивчатися методологічні засади розслідування кримінальних правопорушень, вчинених за допомогою електронно-обчислювальних технологій. Це стало можливим завдяки впровадженню нових наукових підходів і технічних інструментів, а також через необхідність

адаптації криміналістичних методів до особливостей сучасних цифрових кримінальних правопорушень [49; 81; 7; 152; 156; 164].

Процес вивчення методологічних засад включає кілька ключових етапів:

1. Розробка теоретичних засадю Теоретичне осмислення специфіки цифрових злочинів, розробка методів і технік, що враховують нові форми кримінальної діяльності. Вивчення особливостей таких злочинів, як шахрайство через інтернет, кібератаки, порушення конфіденційності даних, а також визначення місця ЕОТ у цих злочинах.

2. Методологічні засади дослідження. У рамках методології розслідування кримінальних правопорушень, вчинених з використанням цифрових технологій, акцент робиться на специфічних методах збору та аналізу цифрових доказів, таких як виявлення слідів на комп'ютерних носіях, встановлення джерела атаки, відновлення стертих даних, аналіз логів та інших електронних артефактів.

3. Розвиток криміналістичних технологій. Важливим етапом є розвиток технічних засобів і технологій для збору, збереження та аналізу електронних доказів, зокрема програмних засобів для цифрової криміналістики, що дозволяють ефективно працювати з інформацією, що зберігається в електронному вигляді, та надають можливість проводити ретельне дослідження у випадках, пов'язаних із кіберзлочинністю.

4. Адаптація методик до умов сьогодення. Врахування новітніх технологій, таких як штучний інтелект, машинне навчання, блокчейн, що також можуть бути використані для вчинення кримінальних правопорушень або ж для їх розслідування, вимагало розробки нових методик.

5. Навчання фахівців. З ростом популярності цифрових технологій і їх використання в кримінальних правопорушеннях виникла необхідність у спеціалізованих освітніх програмах для правоохоронців, прокурорів, суддів, а також експертів з криміналістики, щоб вони могли ефективно застосовувати нові методи розслідування в умовах швидкої цифровізації.

Так, основи методик розслідування шахрайств, зокрема тих, що вчиняються з використанням електронно-обчислювальних технологій (ЕОТ), були закладені багатьма вітчизняними науковцями, серед яких виділяються:

А. В. Крижевський – один із фахівців, який приділяв увагу питанням методики розслідування шахрайств у цифровому середовищі. Він розробляв підходи до виявлення, збору та аналізу доказів, зокрема в контексті використання інтернет-ресурсів для здійснення шахрайських дій. Його наукові праці містять рекомендації щодо використання новітніх технологій у розслідуванні цих кримінальних правопорушень [88, с. 9].

О. Л. Мусієнко у своїх дослідженнях акцентував увагу на особливостях шахрайства через мережу Інтернет, на проблемах цифрових доказів і методах їх збирання та аналізу. Також він розглядав роль психології в розслідуванні шахрайств, особливо в ситуаціях, коли злочинці маніпулюють довірою жертв через фальшиві сайти чи фальшиві пропозиції. О. Л. Мусієнко в своїй дисертаційній роботі «Теоретичні засади розслідування шахрайства в сучасних умовах» (2008) та у монографії «Теоретичні засади розслідування шахрайства в сучасних умовах» (2010) надає важливий теоретичний внесок у розвиток методики розслідування шахрайств, зокрема, в умовах, коли ці правопорушення стають дедалі складнішими через використання новітніх технологій. Вченим було розроблено цілісну концепцію розслідування шахрайства, яка поєднує класичні підходи з новітніми положеннями криміналістики, враховуючи сучасні реалії [116; 117].

О. Л. Мусієнко визначає шахрайство як «інтелектуальну» кримінально протиправну діяльність, де шахрай розробляє детально продумані схеми для здійснення шахрайських операцій. Зі значною увагою вчений підходить до психологічних аспектів вчинення шахрайства, що є важливим для розуміння мотивації зловмисників і визначення характеру їхніх дій.

Особливе місце в роботах О. Л. Мусієнка займає аналіз нових видів шахрайства, зокрема інтернет-шахрайства. У працях відображено сучасні тенденції у правопорушеннях, пов’язаних із використанням технологій,

таких як Інтернет і електронні платіжні системи. У своїй роботі вчений також аналізує традиційні та нетрадиційні способи шахрайства, підкреслюючи необхідність адаптації методів розслідування до нових умов, пов’язаних із розвитком технологій.

О. Л. Мусієнко надає рекомендації щодо найбільш ефективних слідчих (розшукових) дій, які повинні бути реалізовані в комплексі з урахуванням специфіки кожного конкретного випадку. Важливим аспектом є поєднання слідчих (розшукових) дій з оперативно-розшуковими та організаційно-технічними заходами, що дозволяють комплексно розв’язувати проблеми, пов’язані з розслідуванням шахрайства.

Т. А. Пазинич працювала над розробкою методичних рекомендацій у сфері шахрайств, зокрема щодо виявлення фальшивих інтернет-магазинів, фінансових махінацій через електронні платіжні системи, а також вивчав роль юридичних аспектів у таких злочинах. На нашу думку, праці Т. А. Пазинич є важливим внеском у розвиток криміналістичної науки, особливо в аспекті розслідування шахрайств, вчирнених із використанням цифрових технологій. Авторка не лише здійснила детальну класифікацію шахрайств, але й визначила їх криміналістичні особливості та розробила рекомендації щодо методик розслідування цих кримінальних правопорушень.

Особливістю дослідження є виділення окремої категорії шахрайств, вчинених за допомогою цифрових технологій. Т. А. Пазинич підкреслила, що шахрайства у таких випадках мають специфічні особливості, які обумовлені використанням електронних засобів і специфічних середовищ для здійснення правопорушень. Це включає використання мобільного зв’язку, пластикових карток, Інтернету та інших технологічних засобів, що значно ускладнює процес виявлення та фіксації доказів.

Науковиця також зазначила, що шахрайства цієї категорії можуть бути вчинені в різних сферах суспільного життя, від побутових до підприємницьких відносин. Особливою рисою таких злочинів є те, що місце їх вчинення не збігається з місцем знаходження потерпілого або місцем

настання наслідків (наприклад, через відстань між злочинцем і жертвою завдяки використанню технологій). Це ускладнює процес розслідування, оскільки необхідно враховувати не тільки місце вчинення злочину, але й характер електронних слідів.

Т. А. Пазинич також розглянула найтиповіші способи шахрайства в умовах використання цифрових технологій, серед яких:

1) Обманне заволодіння грошима громадян-абонентів мобільних мереж: через переконання у необхідності перерахування коштів для участі в акціях, коли шахраї отримують коди поповнення рахунку.

2) Обманне заволодіння коштами за допомогою підроблених пластикових карток: використання крадених карток для незаконного зняття грошей.

3) Шахрайства через шлюбні сайти: обманне заволодіння грошовими коштами іноземних громадян через фальшиві пропозиції на шлюбних платформах.

4) Інтернет-шахрайства через злом банківських систем: злочинці отримують доступ до банківських рахунків за допомогою зламу захисту банківської електронної системи, переводячи гроші на підставні рахунки в різних країнах [126, с. 12].

С. С. Чернявський розробляв комплексні методики розслідування шахрайств з використанням цифрових технологій, зокрема аналізував стратегії попередження цих кримінальних правопорушень, ефективність правозастосування та взаємодії між правоохоронними органами на різних рівнях при розслідуванні таких правопорушень.

Ці дослідження мають велике значення для розвитку криміналістичної науки в умовах цифровізації та інформаційної епохи, оскільки надають методичні рекомендації щодо виявлення та розслідування нових форм шахрайства, що здійснюються через Інтернет та інші електронні ресурси. Їхні праці визначають важливість комплексного підходу до дослідження таких

злочинів, використання новітніх технічних засобів і методів для ефективного розслідування.

С. В. Самойлов у своїй дисертації «Розслідування шахрайств, учинених із використанням мережі «Інтернет»» здійснив глибоке дослідження криміналістичної характеристики шахрайств, що вчиняються за допомогою Інтернету. Він детально розкрив основні елементи цієї характеристики, акцентуючи увагу на специфіці таких правопорушень [158, с. 7].

Одним із важливих аспектів роботи є класифікація способів учинення шахрайств у мережі Інтернет. С.В. Самойлов детально описав різні методи, які використовують зловмисники для обману, такі як фальшиві інтернет-магазини, фішинг (захоплення конфіденційної інформації через підроблені веб-сторінки), шахрайства на аукціонах та інші види, пов’язані з використанням онлайн-платформ. Він підкреслив, що ці способи мають спільні риси, але також відрізняються за механізмами здійснення і технічними засобами, які при цьому застосовуються.

Крім того, С. В. Самойлов розробив теоретичні основи розслідування шахрайств у мережі Інтернет і надав практичні рекомендації для досудового розслідування цієї категорії кримінальних правопорушень. Він акцентував увагу на необхідності застосування новітніх технологій для збору та аналізу доказів у кіберпросторі, а також на важливості координації дій правоохоронних органів різних країн через глобальний характер інтернет-простору.

Різноманітні аспекти розслідування шахрайств були детально розглянуті у низці досліджень.

О. В. Курман у роботі «Методика розслідування шахрайства з фінансовими ресурсами» (2002) зосередився на специфіці розслідування шахрайств, пов'язаних із незаконним заволодінням фінансовими коштами. У дослідженні обґрунтовано важливість точного визначення характеру шахрайських дій та особливостей фінансових операцій, що допомагає у процесі збору доказів та виявлення слідів злочину. Курман приділив увагу

важливості правильної класифікації фінансових шахрайств та описав основні слідчі дії, які застосовуються для розслідування таких правопорушень [94].

С. В. Головкін у роботі «Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування» аналізував шахрайства, які спрямовані на заволодіння майном особи. Дослідження зосереджено на вивченні різних способів обману, що використовуються для здійснення таких кримінальних правопорушень, і підкреслює необхідність правильної організації розслідування на самому початковому етапі для ефективного виявлення доказів і встановлення обставин вчинення кримінального правопорушення [29].

Т. В. Охрімчук у дослідженні «Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування» докладно розглянула методи, які слід використовувати для ефективного виявлення та запобігання фінансовим шахрайствам. Науковиця акцентує увагу на необхідності застосування спеціальних знань і технологій для розслідування, а також на важливості комплексного підходу до дослідження таких протиправних дій [123, с. 9].

Н. Ю. Кириленко у дослідженні «Методика розслідування шахрайства у сфері побутових відносин» звернула увагу на специфіку шахрайств, що вчиняються в побутовій сфері. Вона описала методи обману, що застосовуються в таких ситуаціях, та підкреслила важливість врахування психологічних аспектів при розслідуванні, адже в даних випадках жертви часто можуть не усвідомлювати факт обману до певного часу [63, с. 25].

Н. М. Ахтирська зосереджувалась на адаптації методик розслідування до змін у характері шахрайських дій, спричинених розвитком цифрових технологій та появою нових способів вчинення таких кримінальних правопорушень. Її роботи містять рекомендації щодо впровадження сучасних технічних засобів та аналітичних інструментів у процес збору доказів [5, с. 110].

К. В. Воробйова акцентувала увагу на психологічних аспектах шахрайських дій, підкреслюючи важливість аналізу поведінки підозрюваних і жертв. Її дослідження спрямовані на вдосконалення підходів до взаємодії слідчих із потерпілими, особливо у випадках, де шахрайство має складні соціальні чи економічні наслідки [27, с. 96–99].

А. А. Патик у своїх працях робив акцент на розробці спеціалізованих методик розслідування нових форм шахрайства, таких як інтернет-шахрайство, шахрайство з електронними платежами та криптовалютами. Він пропонував інтегрувати до слідчої діяльності новітні технології кібербезпеки, а також розширювати співпрацю між слідчими і фахівцями з інформаційних технологій [128, с. 8].

Наукові дослідження, присвячені питанням здійснення окремих процесуальних дій під час розслідування кримінальних правопорушень, вчинених із використанням цифрових технологій, також є важливим внеском у розвиток сучасної криміналістики. У цьому контексті варто виділити праці таких дослідників.

В. А. Коршенко у своїй роботі «Теоретичні та методичні основи судової телекомунікаційної експертизи» здійснив комплексне дослідження концептуальних засад цієї експертизи та розробив рекомендації щодо її наукових, методичних і організаційних положень.

Науковець дав поняття судово-телекомунікаційної експертизи, під яким запропонував розуміти експертне дослідження, що базується на спеціальних знаннях у галузі електроніки, телекомунікаційних систем, засобів, мереж, а також інформації, що передається, приймається, обробляється цими засобами. Його метою є встановлення фактичних даних, які мають значення для кримінального провадження

Розроблені автором методи охоплюють дослідження апаратних і програмних засобів, що використовуються в телекомунікаційних мережах, включно з їх технічними характеристиками, алгоритмами функціонування та обробкою інформації. Особливу увагу приділено аналізу слідів кримінально

протиправної діяльності в телекомунікаційних системах. За його словами, використання результатів експертизи для документування кримінальних правопорушень, пов’язаних із телекомунікаціями, зокрема шахрайства, хакерських атак, кіберзлочинів [83, с. 7].

О. М. Моїсеєв вважає, що дослідження комп’ютерної техніки в умовах криміналістичної лабораторії є важливим аспектом сучасної криміналістичної практики, особливо у сфері розслідування шахрайств із використанням цифрових технологій та кіберзлочинів. На його думку, це мінімізує ризик помилок під час вилучення, аналізу чи фіксації доказів. В умовах криміналістичної лабораторії працюють кваліфіковані фахівці, які володіють необхідними знаннями та досвідом у сфері комп’ютерних технологій [114, с. 81–85].

Запропонований О. М. Моїсеєвим підхід акцентує увагу на критичній ролі фахівців і спеціалізованих лабораторій у розслідуванні шахрайств, учинених із використанням цифрових технологій. Це забезпечує збереження цифрових доказів і підвищує якість досудового розслідування, сприяючи ефективному розкриттю кіберзлочинів.

Думка О. М. Миколенко, яку ми підтримуємо, справедливо акцентує на важливості призначення експертизи в провадженнях, що стосуються шахрайств із використанням цифрових технологій. Навіть за відсутності прямої законодавчої вимоги щодо обов'язковості експертизи, її проведення дозволяє отримати критично важливу інформацію, без якої ефективне розслідування стає неможливим. Експертиза допомагає виявляти технічні нюанси, встановлювати особу зловмисника, механізм вчинення злочину та способи приховування слідів.

Науковці відмічають, що цифрові докази часто мають складну структуру і потребують спеціалізованого аналізу. Без експертного висновку така інформація може бути сприйнята судом як недостатньо обґрунтована. Експертний висновок є одним із основних видів доказів у кримінальних провадженнях і часто виступає вирішальним аргументом [110, с. 155–157].

А. С. Білоусов у 2008 році, здійснюючи криміналістичний аналіз об’єктів комп’ютерних кримінальних правопорушень, суттєво розширив і поглибив вчення про криміналістичну характеристику цієї категорії кримінальних правопорушень. Він звернув увагу на такі важливі аспекти:

1. Особливості слідів комп’ютерних кримінальних правопорушень:

Сліди таких правопорушень відрізняються специфічністю, оскільки їх вчинення, як правило, спрямоване на вплив на комп’ютерну інформацію. Ці сліди мають нематеріальну природу та часто не є очевидними, що потребує застосування спеціальних методів виявлення й фіксації [97].

2. Різноманітність носіїв інформації:

При вчиненні кримінальних правопорушень за допомогою цифрових технологій використовується широкий спектр носіїв даних, включаючи пам’ять комп’ютера, електронні засоби зв’язку, роздруківки з принтерів тощо. Це вимагає від спеціалістів наявності технічних засобів і відповідних навичок роботи з різними типами інформаційних носіїв.

3. Значення спеціальних знань:

Вчений наголошує, що розслідування комп’ютерних кримінальних правопорушень неможливе без залучення фахівців із спеціальними знаннями у сфері інформаційних технологій. Такі знання необхідні для правильного вилучення, аналізу й збереження цифрових доказів.

4. Завдання для спеціалістів у слідчих (розшукових) діях:

Автор доповнив перелік завдань, які ставляться перед спеціалістом під час слідчих (розшукових) дій у справах цієї категорії. Це включає ідентифікацію способів вчинення кримінальних правопорушень, аналіз виявленої інформації, відновлення видалених даних, фіксацію слідів цифрових втручань тощо [9, с. 5].

Сучасні науковці, такі як А. С. Білоусов, О. Л. Мусієнко, С. В. Самойлов, В. В. Тіщенко, С. С. Чернявський та інші, акцентують увагу на нагальній потребі у розробці комплексної методики розслідування шахрайств, учинених із використанням цифрових технологій. Вони

зазначають, що практика розслідування виявляє нові виклики, спричинені створенням складних і багаторівневих схем кримінально протиправної діяльності в кримінальному середовищі.

Науковці обґрунтовують таку позицію на твердженнями:

1. Складність кримінально протиправних схем. Злочинці активно використовують сучасні цифрові технології для реалізації багаторівневих шахрайських схем. Це вимагає від слідчих глибокого розуміння принципів роботи інформаційних систем та їх вразливостей.

2. Необхідність узагальненої методики. Розслідування цих правопорушень потребує чітких криміналістичних рекомендацій, які враховували б загальні риси кримінальних правопорушень, учинених із використання цифрових технологій [102; 99]. Такі рекомендації мають ґрунтуватися на криміналістичних характеристиках цих правопорушень, узагальнених із різних випадків слідчої практики.

3. Використання вимог сьогодення. Ефективне розслідування потребує поєднання традиційних методик криміналістики з інноваційними підходами, зокрема з використанням інструментів цифрової криміналістики, аналізу великих даних і штучного інтелекту.

4. Глобальний характер кримінальних правопорушень. Більшість шахрайств, учинених із використанням цифрових технологій, мають транснаціональний характер, що ускладнює їх розслідування. Вирішення цих проблем вимагає міжнародного співробітництва, що також має бути враховано у загальних рекомендаціях [159, с. 64].

На основі цього, науковці пропонують створити методику, яка:

- включатиме класифікацію шахрайств за типами технологій, що використовуються злочинцями;
- передбачатиме алгоритми дій слідчих на різних етапах розслідування;
- інтегрує рекомендації щодо збирання, збереження й аналізу цифрових доказів;

- враховуватиме необхідність взаємодії з експертами у сфері інформаційних технологій;
- охоплюватиме питання запобігання подібним кримінальним правопорушенням за допомогою профілактичні заходи.

Низка методичних рекомендацій була присвячена способам встановлення місцезнаходження електронно-обчислювальної техніки, за допомогою якої вчинялися кримінальні правопорушення. Зокрема, значний внесок у розвиток цієї тематики зроблено через публікацію таких рекомендацій, як «Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту» (2014) [164, с. 27], «Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів» (2016) [12], «Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернет-провайдерами» (2017) [165], «Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет» (2021) [166], «Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій» (2023) [119], «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» (2021) [85].

Отже, сучасний стан протидії з шахрайствам, учиненими з використанням цифрових технологій, висвітлив низку важливих проблем у сфері кримінального процесу та криміналістики, які залишаються невирішеними. Найсуттєвіші з них стосуються криміналістичної методики, адже саме в цій галузі спостерігається значне відставання рівня науково-методичних розробок від практичних потреб.

Основними проблемами у цьому напрямку залишаються:

1. Відсутність методик для нових типів правопорушень. Значна частина сучасних кримінальних правопорушень, пов'язаних із

використанням цифрових технологій, залишаються поза увагою розробників методичних рекомендацій.

2. Застарілість підходів. Традиційні методики розслідування деяких правопорушень (зокрема, шахрайств) не враховують суттєвих змін у способах їх учинення, хоча їх кримінально-правова форма залишається незмінною.

3. Недостатня практична орієнтованість. Багато рекомендацій створено за шаблонними схемами, без урахування реальних потреб слідчої практики, що знижує їхню ефективність.

Проаналізувавши думки науковців можемо погодитися з тим, що на сьогодні існує об'єктивна необхідність у розробці комплексної криміналістичної методики, яка:

- узагальнює та впорядковує наявні рекомендації щодо розслідування шахрайств, учинених із використанням цифрових технологій;
- базується на характеристиках різних видів кримінальних правопорушень, що дозволяє об'єднати окремі рекомендації в цілісну систему;
- включає адаптовані методи, які враховують рівень сприйняття користувачем, забезпечуючи їхню зручність для практичного використання.

Основою нової методики мають стати:

- Криміналістична класифікація правопорушень, яка дозволяє впорядковувати кримінальні правопорушення за спільними рисами.
- Криміналістична характеристика правопорушень, яка забезпечує опис типових ознак кримінальних правопорушень.
- Теорія криміналістичного прогнозування, що допомагає передбачати нові виклики, пов'язані з розвитком технологій.

Попри значну увагу до проблем розслідування кримінальних правопорушень, пов'язаних із використанням цифрових технологій, ці питання на рівні дисертаційних досліджень залишаються недостатньо висвітленими. Це додатково підкреслює актуальність їхнього всебічного

вивчення та розробки нових науково-методичних підходів. Узагальнення і впорядкування теоретичних положень у рамках єдиної концепції сприятиме підвищенню ефективності боротьби з шахрайствами та іншими кримінальними правопорушеннями у сфері цифрових технологій.

1.2. Віртуальний простір як середовище шахрайства, вчиненого з використанням цифрових технологій

До недавнього часу кримінальні правопорушення, вчинені з використанням цифрових технологій, часто розглядалися винятково в контексті порушень у сфері комп’ютерної інформації, зокрема, це стосувалося кібератак, крадіжок особистих даних або несанкціонованого доступу до комп’ютерних систем. Проте в умовах глобалізації Інтернет став не лише інструментом для вчинення специфічних комп’ютерних кримінальних правопорушень, але й засобом для вчинення традиційних кримінальних првопорушень, таких як шахрайство, торгівля незаконними товарами або фінансові махінації [118, с. 304–307].

Таким чином, злочинці використовують Інтернет для здійснення різноманітних правопорушень, що додає нових складнощів у боротьбу з кримінально протиправною діяльністю, оскільки традиційні методи правозастосування часто виявляються малоефективними для вирішення проблем, пов'язаних з цифровим середовищем. Це підкреслює важливість адаптації правових та криміналістичних підходів до нових реалій, зокрема у боротьбі з такими кримінальними правопорушеннями, які стають усе більш поширеними та складними у розслідуванні [104, с. 123].

Справді, багато дослідників погоджуються, що кримінальні правопорушення, пов'язані з використанням цифрових технологій, неможливі без існування певного віртуального простору, де ці кримінальні правопорушення вчиняються. Однак стрімкий розвиток інформаційно-комунікаційних технологій призвів до суттєвого розширення й трансформації

самого поняття «віртуальний простір». Це поняття стало широко вживаним, і його інтерпретація набуває різноманітних смислових відтінків залежно від контексті [37, с. 163–170].

Аналіз наукової літератури показує, що термін «віртуальний простір» часто замінюється іншими поняттями, такими як «інтернет-простір», «кіберпростір», «інформаційний простір», «віртуальний світ» тощо. Це викликає питання щодо їх синонімічності або, навпаки, різного значення, оскільки кожне з цих понять може мати своє власне трактування в різних сферах.

Так, більшість фахівців погоджуються з тим, що інтернет-простір є невід’ємною складовою інформаційного простору. Він не лише забезпечує засоби обміну соціальною інформацією, а й стає носієм специфічної культури, яка виникає у результаті взаємодії користувачів у віртуальному середовищі [66, с. 346–349].

Інтернет-простір можна трактувати як платформу, де здійснюється глобальний обмін інформацією між індивідами, організаціями, державами. Це середовище не обмежується лише технічними аспектами (наприклад, мережею серверів чи протоколами зв'язку), а включає соціальні, культурні та економічні зв’язки, що утворюються в процесі використання інтернет-ресурсів. Інтернет стає не лише способом передавання даних, але й умовою виникнення нових форм комунікації, культурних явищ, спільнот, а також нових типів кримінальних правопорушень.

На думку О.О. Кіпи, віртуальний простір можна розглядати як складну модель, що існує завдяки комп’ютерним технологіям. Цей простір є інформаційною мережею, де зберігаються та передаються дані про осіб, об'єкти, явища, події та процеси. Віртуальний простір характеризується тим, що ці дані можуть бути представлені в різних формах — від математичних моделей і символьних виразів до інших форматів інформації, що зберігаються або передаються через локальні й глобальні комп'ютерні мережі [66, с. 346–349].

Основні характеристики цього віртуального простору, згідно з думкою науковця, включають:

1) моделювання інформації, оскільки віртуальний простір складається з даних, які можуть бути представлені в різних математичних, символьних або інших формах;

2) динамічний процес, адже дані в цьому просторі перебувають у постійному русі через мережі або зберігаються на різних фізичних або віртуальних пристроях;

3) інформаційні носії: це можуть бути фізичні пристрої, як комп'ютери чи сервери, або віртуальні носії, спеціально призначені для зберігання, обробки та передачі інформації [101].

О. Ткаченко та Т. Ткаченко наводять різні підходи до формалізації поняття «кіберпростір», які мають своєрідні акценти залежно від аспекту, що розглядається. До них належать:

1) кіберпростір як середовище взаємодії — це концепція, в рамках якої кіберпростір визначається як середовище, що виникає завдяки взаємодії людей, програмного забезпечення та інтернет-послуг, що здійснюються через технологічні пристрої і мережі, під’єднані до цих пристроїв. Науковці підкреслюють абстрактність кіберпростору, адже він не має фізичної форми, але є важливим для взаємодії учасників віртуального середовища.

2) кіберпростір як сфера обміну даними — у цьому підході кіберпростір визначається як простір, що забезпечує використання електронних і електромагнітних засобів для запам'ятовування, модифікації та обміну даними через різні системи. Тут акцент робиться на технологічні процеси, що відбуваються в ньому.

3) кіберпростір як цифрова активність — цей підхід розглядає кіберпростір як включення всіх форм мережної та цифрової активності, що охоплює контент та дії з його обробки. Така перспектива підкреслює динамізм і взаємодію цифрових об'єктів у мережі.

4) кіберпростір як інфраструктура, доступна через інтернет — це визначення акцентує увагу на інфраструктурі, яка забезпечує доступ до інформаційних ресурсів через інтернет, що є важливим для обміну та зберігання даних.

5) кіберпростір як комунікаційне середовище — тут кіберпростір описується як система зв'язків між різними об'єктами кіберінфраструктури, включаючи комп'ютерні мережі, електронні обчислювальні машини, програмне забезпечення та інформаційні ресурси. Цей підхід орієнтований на розуміння кіберпростору як інтеграції різних технічних і програмних елементів, що забезпечують комунікацію між об'єктами [169, с. 75–86].

В. М. Фурашев визначає кіберпростір як специфічну форму співіснування матеріальних і нематеріальних об'єктів і процесів, які мають на меті породжувати, сприймати, зберігати, переробляти та обмінювати інформацію. Згідно з його концепцією, кіберпростір охоплює весь спектр інформаційних процесів, що здійснюються за допомогою різноманітних технологій і пристроїв, призначених для обробки та передачі даних [175, с. 162–175].

Науковець справедливо стверджує, що поняття «кіберпростір» та «інформаційний простір» є тотожними за своєю сутністю, хоча різні науковці можуть використовувати їх як окремі терміни. У його погляді, застосування будь-якого з цих понять не змінює самого процесу або явища, а може лише спричинити термінологічну плутанину, оскільки обидва ці терміни описують одну й ту ж саму реальність — простір для циркуляції інформації, в який входять як цифрові, так і традиційні форми інформаційних комунікацій [175, с. 162–175].

Питання визначення поняття «Інтернет» залишається проблематичним у правовому полі, оскільки ані в міжнародному праві, ані в національних законодавствах немає єдиного розуміння цього терміна. Як зазначає С.Ф. Гуцу, відсутність чіткого законодавчого визначення Інтернету створює правову невизначеність, зокрема у сфері кіберзлочинності [35, с. 114–118].

У науковій літературі також існують різні підходи до розуміння природи Інтернету, оскільки це поняття охоплює широкий спектр технологій і сервісів, які постійно змінюються. Зокрема, Інтернет можна розглядати як глобальну систему комп'ютерних мереж, що дозволяє користувачам обмінюватися інформацією в різних форматах, але існують й інші трактування, що включають в себе різні аспекти: технічний, соціальний і навіть правовий.

У зв'язку з цим, різні науковці та практики пропонують різні визначення Інтернету в контексті кіберзлочинності, але всі вони сходяться на тому, що Інтернет є потужним засобом як для здійснення правомірних дій, так і для вчинення кримінальних правопорушень. Це ускладнює розробку чітких та ефективних правових норм для протидії кіберзлочинності, оскільки відсутність єдиного визначення Інтернету перешкоджає виробленню універсальних підходів у правовому регулюванні кіберзлочинів.

Звернемося до чинного законодавства. Відповідно до Закону України «Про електронні комунікації», Інтернет визначається як всесвітня інформаційна система загального доступу, яка логічно пов’язана глобальним адресним простором та базується на інтернет-протоколі, що визначений міжнародними стандартами [140].

Це визначення підкреслює, що Інтернет є глобальною мережею, що забезпечує доступ до різноманітних інформаційних ресурсів і послуг. Проте важливо зазначити, що таке визначення, хоч і надає юридичну основу для розуміння Інтернету в контексті телекомунікацій, не завжди враховує всі нюанси, пов'язані з використанням Інтернету для вчинення правопорушень, зокрема кіберзлочинів. Також варто зауважити, що в міжнародному контексті поняття Інтернету може мати інші трактування, залежно від законодавства і нормативних актів, що використовуються в різних країнах або міжнародних організаціях.

Аналізуючи різні трактування поняття «Інтернет» у науковій літературі, можемо виокремити кілька основних ознак, які повторюються в більшості визначень. Серед них:

1) міжнародний рівень – Інтернет є глобальною мережею, яка об'єднує країни та континенти, даючи доступ до інформації та ресурсів на світовому рівні.

2) телекомунікаційна мережа – Інтернет складається з численних підключених мереж, що забезпечують передачу даних між користувачами та серверами по всьому світу.

3) загальне користування – Інтернет є відкритим і доступним для широкого кола користувачів, забезпечуючи доступ до різноманітних інформаційних ресурсів та сервісів без обмежень для більшості осіб.

4) засіб комунікації – Інтернет дозволяє людям здійснювати комунікацію в різних формах, таких як електронна пошта, соціальні мережі, чати, відеоконференції тощо.

5) обмін інформацією – Інтернет є основним інструментом для обміну даними, файлами, інформацією між користувачами та організаціями, сприяючи розвитку комунікації та інформаційних технологій [184, с. 78–82, 185, с. 403–405].

Отже, на сьогодні в Україні ще не сформовано єдиний понятійний апарат щодо середовища, в якому вчиняються кримінальні правопорушення, пов'язані з використанням цифрових технологій. Однак, це не є критичною проблемою, оскільки в науковій літературі часто існує консенсус щодо ототожнення понять «кіберпростір», «віртуальний простір» і «інформаційний простір», що дозволяє вільно застосовувати їх у контексті дослідження злочинності, пов'язаної з цифровими технологіями. Ми підтримуємо науковців у тому, що «віртуальний простір» є більш конкретним поняттям і однією з основних складових кіберпростору. Враховуючи те, що Інтернет є важливим інструментом для злочинців, що здійснюють шахрайства та інші

правопорушення в онлайн-просторі, використання терміну «віртуальний простір» для опису саме цих порушень є доцільним.

Досить розповсюдженим сьогодні є шахрайство у віртуальному просторі шляхом імітування продажу товарів. Як зазначають вчені, на сьогодні продаж товарів у віртуальному просторі охоплює понад 20 мільйонів користувачів [112, с. 153–155].

Це справді вражаючий показник, що підкреслює зростання популярності електронної комерції в Україні. З огляду на цей факт, можна стверджувати, що Інтернет став не лише каналом для взаємодії між підприємствами та споживачами, а й важливою складовою економічної діяльності в країні. 20 мільйонів користувачів — це суттєва частка населення, що активно користується інтернетом для здійснення покупок і взаємодії з різними підприємствами, що працюють у сфері онлайн-продажів.

Торгівля у мережі «Інтернет» здійснюється через різні платформи, кожна з яких має свої особливості та функціональні можливості для взаємодії між продавцями та покупцями, зокрема:

Сайти інтернет-магазинів – це найбільш поширена форма онлайн-торгівлі. Вони функціонують як віртуальні магазини, де продавець виставляє товари або послуги, а покупець може здійснити покупку через систему електронних платежів. Інтернет-магазини можуть бути як великими (наприклад, інтернет-гіганти типу Amazon чи eBay), так і невеликими, що спеціалізуються на конкретних товарах чи послугах.

Електронні дошки оголошень – це платформи, де користувачі можуть розміщувати свої оголошення про продаж товарів або послуг. Вони часто використовуються для продажу б/у товарів, а також для локальних угод. Популярними такими платформами є OLX, Avito тощо. На таких платформах часто трапляються випадки шахрайства, оскільки вони зазвичай не мають прямого контролю над угодами.

Віртуальні торгові центри – це платформи, які об'єднують кілька продавців, подібно до фізичних торгових центрів. На таких сайтах

користувач може переглядати пропозиції від різних магазинів або продавців, порівнювати ціни та умови доставки. Прикладом таких платформ є eBay, Amazon Marketplace, Etsy.

Згідно з матеріалами судово-слідчої практики, шахраї часто використовують певні платформи для здійснення кримінальних правопорушень, зокрема «Інтернет-аукціони» та «дошки оголошень», через їх доступність та особливості функціонування (35 % і 81 % відповідно).

На цих платформах часто відсутні системи захисту покупців, що робить їх вразливими до шахрайських схем. Враховуючи їх популярність і зростання онлайн-торгівлі, важливо підвищувати рівень обізнаності споживачів щодо ризиків, що виникають на таких платформах, а також розробляти більш ефективні методи регулювання та захисту від шахрайства у цьому сегменті інтернет-торгівлі.

У рамках електронного бізнесу відбувається постійна взаємодія між чотирма основними суб’єктами, кожен з яких має свою роль і функцію в цьому процесі:

Клієнти – це споживачі товарів або послуг, які здійснюють покупки в онлайн-середовищі. Клієнти можуть бути як індивідуальними споживачами, так і організаціями, що купують товари чи послуги для власних потреб чи подальшого перепродажу. Вони є кінцевими користувачами, і їхня взаємодія з бізнесом часто здійснюється через онлайн-магазини, платформи, аукціони тощо.

Бізнес-організації – це підприємства, які здійснюють свою діяльність за допомогою інформаційних мереж, виконуючи транзакції, надаючи товари та послуги через електронні платформи. Вони можуть бути як великими міжнародними компаніями, так і малими та середніми підприємствами, що працюють в рамках онлайн-торгівлі. Ці організації використовують інтернет для пошуку споживачів, продажу товарів, маркетингових стратегій, а також для здійснення фінансових операцій.

Фінансові установи – це організації, що забезпечують фінансову інфраструктуру для здійснення онлайн-транзакцій. В основному у цій діяльності беруть участь банки та платіжні системи, які забезпечують оплату товарів і послуг, а також захист фінансових потоків. Вони надають послуги з обробки електронних платежів, а також беруть участь у безпеці транзакцій через використання різних фінансових і технологічних інструментів.

Держава – це орган, який визначає правила та нормативи, що регулюють електронну комерцію. Держава встановлює закони та стандарти, що забезпечують законність угод, захист прав споживачів, безпеку онлайн-платежів, а також наглядає за виконанням цих норм. Окрім того, держава може сприяти розвитку електронного бізнесу через розвиток інфраструктури, надання податкових пільг для бізнесу або проведення заходів із захисту від кіберзлочинності [112, с. 153–155].

О.П. Письменна, О.С. Баранова та О.М. Шкринда правильно підкреслюють, що відносини між покупцем та продавцем у сфері електронної комерції за суттю не відрізняються від традиційних торгових відносин. Вони також регулюються тим же законодавством, яке застосовується до звичайних угод купівлі-продажу [132, с. 59–62].

Законодавчий підхід до регулювання електронної комерції в Україні спрямований на створення чіткої правової бази, яка забезпечує баланс інтересів як продавців, так і споживачів. Це включає в себе встановлення вимог до укладання онлайн-угод, визначення прав та обов'язків сторін, захист прав споживачів, а також усунення правових прогалин, які можуть виникати в умовах швидкого розвитку електронних технологій і онлайн-торгівлі.

Зокрема, українське законодавство враховує вимоги Європейського Союзу в цій сфері, що сприяє інтеграції в єдиний європейський ринок і забезпечує правову визначеність щодо електронних угод. Законодавчі ініціативи, які регулюють електронну комерцію, включають питання

електронного підпису, захисту персональних даних, відповідальності за порушення умов угод, а також механізми вирішення спорів [98].

Загалом такий підхід забезпечує правову прозорість і безпеку для всіх учасників ринку, що є важливим для розвитку електронної комерції в Україні.

Справді, розгляд інтернет-простору через призму права є складним і суперечливим, оскільки інтернет як глобальна, динамічна та децентралізована платформа стикається з традиційними юридичними концепціями та механізмами, які не завжди можуть адекватно регулювати новітні форми взаємодії. На сьогодні є наукові позиції, що відображають два основні підходи до правового регулювання інтернет-простору:

1) позиція про неактуальність застосування права в інтернеті – представники цієї групи вважають, що інтернет є відокремленою зоною, де діяти традиційні правові норми неможливо або недоцільно через відсутність єдиної юрисдикції, анонімність учасників і складність ідентифікації правопорушників. Крім того, швидкість розвитку технологій в інтернеті часто випереджає здатність державних інститутів створювати ефективне правове регулювання, що додає додаткові труднощі у забезпеченні правопорядку.

2) позиція щодо необхідності застосування права – друга група фахівців підкреслює, що навіть у такому середовищі, як інтернет, необхідно забезпечувати правовий захист і регулювання відносин. Вони вважають, що право має стати невід’ємною частиною цього простору, оскільки правові норми здатні захищати користувачів від зловживань, таких як шахрайство, порушення авторських прав, кіберзлочинність, а також встановлювати правовий порядок у сфері комерційних операцій, персональних даних, контенту тощо. Водночас, для ефективного регулювання права потрібно враховувати особливості інтернет-простору, зокрема глобальність, динамізм та анонімність, що ускладнюють застосування традиційних правових норм [191, с. 137–140]. З цієї точки зору правовий регулювання інтернету має

враховувати його специфіку, зокрема, необхідність застосування міжнародних угод, забезпечення права на приватність, а також визначення чітких механізмів для вирішення правових суперечок у віртуальному середовищі.

Збут товарів і послуг через інтернет здійснюється через різноманітні платформи, кожна з яких має свої особливості та переваги для продавців та покупців. Як зазначає В.Я. Капцош, існує кілька основних типів платформ, що використовуються для продажу віртуальних товарів, серед яких власні інтернет-магазини, електронні дошки оголошень, соціальні мережі та торгові центри. Власний інтернет-магазин є одним із найбільш ефективних способів представлення товару в інтернеті [56, с. 115–119].

Створення сайту дає змогу компанії не лише продемонструвати свої товари та послуги, але й активно працювати над брендингом, залученням клієнтів та вдосконаленням маркетингових стратегій. Однак для досягнення значних обсягів продажу потрібно активно просувати сайт у пошукових системах і регулярно покращувати його контент та структуру. Хоча це дозволяє зберегти контроль над усіма аспектами продажу, цей шлях потребує значних інвестицій у розробку, підтримку та рекламу. Електронні дошки оголошень представляють собою більш прості та дешеві платформи для публікації реклами. Такі ресурси дозволяють продавати товари, особливо вживані, та зручні для разових операцій. Хоча вони можуть бути ефективними для приватних осіб, для бізнесів вони мають обмежені можливості у зв'язку з простотою та великим обсягом реклами. Рейтинг оголошень залежить від того, чи є оплата за публікацію, що також може впливати на ефективність реклами. Соціальні мережі стали потужним інструментом для маркетингу і продажу товарів, особливо для малого бізнесу. Вони дозволяють продавцям взаємодіяти безпосередньо з клієнтами, формувати додаткові канали збуту та зміцнювати зв'язки з громадськістю. Проте, успішність продажів в соціальних мережах часто залежить від унікальності товару: чим більш стандартизованим є продукт, тим складніше

його продавати через цей канал. Крім того, ціна товару стає важливим фактором, особливо якщо товар не є унікальним або має високу конкуренцію на ринку. Торгові центри в Інтернеті – це великі платформи, що об'єднують тисячі компаній, дозволяючи продавати різноманітні товари. На таких платформах часто продають не приватні особи, а бізнеси, які хочуть з'явитися на великому ринку. Проте наявність щорічних платежів за публікацію на таких платформах іноді може бути більш витратним, ніж створення власного інтернет-магазину, який дозволяє забезпечити більше функціональних можливостей та індивідуальний дизайн [56, с. 115–119].

Популярність інтернет-покупок та зростання активності віртуальних ринків ставлять перед правоохоронними органами нові виклики, зокрема в частині захисту прав споживачів та протидію кримінальним правопорушенням, вчиненим за допомогою цифрових технологій. Враховуючи високий рівень зловживань, таких як шахрайства при покупках онлайн, фальсифікація товарів, а також порушення прав споживачів у віртуальному середовищі, виникає потреба в активнішій діяльності щодо моніторингу та захисту користувачів [144].

Розвиток електронної комерції в Україні має кілька етапів, починаючи з 2000-х років, коли основні платіжні системи та банки почали активно розвивати інфраструктуру для онлайн-платежів. Це стало основою для подальшого розширення інтернет-торгівлі та надання онлайн-послуг. Одним із важливих етапів стало виникнення платіжних шлюзів, які виступали посередниками між банками та інтернет-магазинами, що дозволило здійснювати безпечні та зручні трансакції.

Проте, незважаючи на активний розвиток електронної комерції, рівень розкриття кримінальних правопорушень, пов'язаних з купівлею-продажем товарів через Інтернет, залишається недостатнім. Це, в свою чергу, призводить до численних випадків шахрайства, фальсифікації товарів та порушення прав споживачів.

Наявність такої проблеми обумовлена декількома чинниками, зокрема, складність і анонімність онлайн-транзакцій, що ускладнює виявлення шахраїв та розкриття злочинів, невизначеність правової відповідальності за порушення, що виникають при укладенні угод в Інтернеті, низький рівень довіри користувачів до інтернет-магазинів через часті випадки обману [186, с. 351–353].

Згідно з українським законодавством, зокрема Законом України «Про електронну комерцію», електронна торгівля визначається як господарська діяльність, що здійснюється через інформаційно-телекомунікаційні системи і включає дистанційний продаж товарів, а також укладання електронних правочинів [146]. Це означає, що угоди, укладені в електронному форматі, мають таку саму юридичну силу, як і традиційні угоди, за умови дотримання відповідних вимог.

У випадку, якщо угода купівлі-продажу в Інтернеті супроводжується шахрайством, наприклад, через обман чи зловживання довірою, і покупець втрачає майно чи право на майно, це може бути кваліфіковано як шахрайство. Однак, незважаючи на чітке правове визначення, на практиці доведення таких кримінальних правопорушень в Інтернеті є значно складнішим, порівняно з традиційними способами шахрайства.

Згідно з роз’ясненням уповноважених органів, суб’єкти господарювання, які займаються торгівлею через мережу «Інтернет», зобов'язані дотримуватися вимог Правил продажу товарів на замовлення та поза торговельними або офісними приміщеннями**.** Ці правила регулюють умови продажу товарів дистанційно, зокрема через Інтернет, і встановлюють правові норми для захисту прав споживачів в таких угодах [136]. Незважаючи на наявність Правил продажу товарів на замовлення та поза торговельними або офісними приміщеннями, законодавче регулювання створення та діяльності інтернет-магазинів в Україні все ще потребує вдосконалення. Відсутність чітких вимог та недостатня регламентація в цьому напрямі створюють можливості для шахраїв, які можуть легко

створювати інтернет-магазини, а потім ліквідувати їх, не несучи відповідальності за обдурених споживачів.

Цей феномен, коли інтернет-магазини діють як фірми-одноденки, є серйозною проблемою для споживачів і несе велику небезпеку для ринку електронної комерції. Оскільки ці магазини можуть бути створені на короткий період, щоб отримати гроші від покупців і зникнути, забезпечення ефективного контролю за їх діяльністю стає надзвичайно важким.

Розрахунки у сфері електронної комерції можуть здійснюватися через різноманітні платіжні інструменти, зокрема електронні гроші, банківські картки, а також платіжні системи, як WebMoney, PayPal, QIWI, Moneybookers тощо. Законодавство України дозволяє різні способи оплати, проте це також відкриває можливості для зловживань, зокрема через труднощі в ідентифікації осіб, які здійснюють фінансові операції.

Важливість електронних платіжних систем в сучасній електронній комерції полягає в їх зручності та доступності для покупців. Однак ці платіжні системи мають й суттєві недоліки, зокрема з точки зору ідентифікації осіб. Система анонімних платежів, таких як WebMoney або QIWI, дозволяє шахраям знімати кошти без зазначення реальних імен або наявності реальної ідентифікації особи, що робить процес розслідування значно складнішим. У випадках шахрайства в Інтернеті, коли потерпілі переводять гроші через ці платіжні системи, стає надзвичайно важко ідентифікувати винуватців.

К. Д. Заяць справедливо зазначає, що зростання використання анонімних платіжних систем дійсно створює нові виклики для правоохоронних органів і знижує ефективність боротьби з шахрайством в електронній комерції. Це також створює додаткові труднощі у процесі відслідковування фінансових транзакцій та притягнення до відповідальності осіб, які стоять за кримінально протиправними операціями [50, с. 45].

Для зменшення можливостей для шахрайства в електронній комерції можна запропонувати такі заходи:

1) посилити вимоги до ідентифікації користувачів платіжних систем, зокрема зобов'язати їх надавати більше інформації про свої особисті дані;

2) контролювати анонімні транзакції через електронні платіжні системи, зокрема через введення правил, які вимагають певного рівня верифікації користувачів перед проведенням транзакцій;

3) забезпечити інтеграцію з правоохоронними органами, адже платіжні системи мають співпрацювати з державними органами для швидкого реагування на випадки шахрайства;

4) створення чітких правил для електронної комерції, оскільки для інтернет-магазинів та інших учасників ринку потрібно чітко визначити законодавчі вимоги щодо фінансових операцій та захисту споживачів від зловживань.

Аналізуючи норму Закону України «Про платіжні послуги», можна зробити висновок, що законодавець дійсно чітко визначив право користувачів електронних грошей на їх використання для оплати товарів, робіт і послуг, а також на переказ цих грошей іншим користувачам. Це дозволяє здійснювати обмін товарів на електронні гроші, що потім стають власністю продавця [146].

Однак важливо враховувати, що на такі операції також поширюються вимоги Закону України «Про захист прав споживачів», оскільки електронні гроші використовуються в рамках взаємодії між споживачами (покупцями) і продавцями або постачальниками товарів, робіт і послуг.

Згідно з вимогами законодавства, у разі здійснення покупок через Інтернет, важливою умовою є надання розрахункового документа, який підтверджує факт розрахункової операції між покупцем та продавцем. Це є обов'язковим як для покупок, здійснених за електронні гроші, так і для покупок через інші платіжні засоби.

Відповідно до п. 2 ст. 3 Закону України «Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг», суб'єкти господарювання, які здійснюють розрахункові операції, зобов'язані

надавати покупцям розрахунковий документ на суму проведеної операції. Це стосується не тільки товарів, придбаних у фізичних магазинах, а й товарів, що продаються через Інтернет. Розрахунковий документ має бути наданий у паперовій або електронній формі, зокрема:

1) при отриманні товару чи послуги покупець має право на отримання документа, який підтверджує здійснення розрахунку, включаючи всі платежі за товар чи послугу.

2) у разі повернення товару відповідно до законодавства продавець зобов'язаний повернути кошти або обміняти товар протягом 14 днів, за умови наявності підтвердження здійснення операції. Це особливо важливо для покупок, здійснених через Інтернет, де оплата може бути проведена через електронні платіжні системи.

3) у разі Інтернет-розрахунків (коли платіж здійснюється через електронні гроші або інші платіжні системи) розрахунковий документ має бути надісланий покупцеві на вказану електронну адресу або абонентський номер. Це підтверджує факт здійснення операції і служить підставою для подальших дій щодо повернення або обміну товару [143].

Отже, забезпечення вимог щодо надання розрахункових документів є важливим елементом захисту прав споживачів, оскільки він створює прозорість у фінансових операціях і надає можливість контролю за виконанням договору. Це також важливо для забезпечення прав покупців у випадках повернення товару або вирішення інших суперечок.

На сьогодні відсоток наданих розрахункових документів у випадках шахрайства в Інтернет-торгівлі є досить низьким – всього 8%.

Згідно зі ст. 675 Цивільного кодексу України, товар, переданий продавцем, повинен відповідати вимогам щодо якості на момент його передання покупцеві. Це забезпечує права споживачів на отримання товару, який відповідає умовам договору, що важливо для захисту від нечесних практик, зокрема у випадках шахрайства в інтернет-торгівлі. [178]. Однак, у випадку з шахрайськими схемами в Інтернеті, продавець часто не має наміру

дотримуватися цієї норми, а замість того пропонує фальсифікований або неналежної якості товар.

Електронні платіжні системи (ЕПС) є основними засобами для проведення фінансових операцій через Інтернет. Вони забезпечують зручний, швидкий та безпечний спосіб здійснення платежів та переказів, не потребуючи фізичної присутності клієнтів. Це значно полегшує онлайн-торгівлю, а також різноманітні інші операції, пов’язані з фінансами. Електронні гаманці є одним із основних інструментів, через які здійснюються ці трансакції. Вони дозволяють зберігати електронні гроші та здійснювати оплату за товари та послуги. Користувач може поповнювати свій електронний гаманець через різні способи, включаючи банківські перекази, кредитні картки, або за допомогою інших електронних платіжних інструментів. Найпопулярніші електронні платіжні системи, які Ви згадали, зокрема PayPal, справді є лідерами в світовій практиці платіжних операцій в Інтернеті. PayPal є найпоширенішим методом оплати для онлайн-покупок, завдяки його зручності, безпеці та широкій інтеграції з численними інтернет-магазинами та платформами для бізнесу. Інші системи, як WebMoney та E-Gold, також відіграють важливу роль у різних регіонах, однак PayPal залишається найбільш глобально поширеною системою, зокрема завдяки підтримці понад 230 мільйонів користувачів у 190 країнах. Це свідчить про високий рівень довіри до цієї платіжної системи та її зручність для проведення міжнародних операцій.

І.О. Воронов справедливо підкреслює, що недостатня нормативна урегульованість у сфері електронних гаманців створює можливості для їхнього використання в злочинних цілях. Віртуальні гаманці, зокрема ті, що використовуються для електронних грошей, мають низку властивостей, які можуть бути зловживаними для здійснення фінансових операцій, що виходять за межі законодавчого контролю [28, с. 275–287].

Отже, професійне шахрайство є глобальною проблемою, і боротьба з ним стає важливим аспектом правоохоронної діяльності в усіх країнах світу.

Водночас варто відзначити, що хоча конкретні результати боротьби з шахрайством можуть змінюватися в залежності 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.

Одним із ключових завдань правоохоронних органів є розробка та впровадження ефективних технологій розслідування шахрайських схем, що включають в себе відмивання коштів. Ці схеми можуть бути складними, і від їх виявлення залежить не лише боротьба з економічними злочинами, а й забезпечення стабільності фінансової системи.

Для цього необхідно активно застосовувати різноманітні механізми, що дозволяють відстежувати рух незаконних коштів, включаючи фінансові технології і аналітичні інструменти. Одним із важливих аспектів є застосування заходів щодо своєчасного арешту активів, що дозволяє заморозити незаконно отримані кошти до того, як вони будуть легалізовані або використані злочинцями.

Щоб зменшити ймовірність шахрайських дій, підприємствам і організаціям доцільно зміцнювати внутрішній контроль та впроваджувати незалежний аудит. Важливо також оптимізувати та вдосконалювати наглядові функції, щоб своєчасно виявляти та запобігати можливим зловживанням.

Покращення цих систем дозволяє не лише знизити ймовірність шахрайства, але й покращити загальну прозорість фінансових операцій, що є важливим для розвитку здорової економічної середовища [200, с. 121–129].

Віртуальний простір, як середовище для здійснення різноманітних правочинів, потребує чітких і детальних правових норм. Через швидкий розвиток електронної комерції, використання новітніх технологій, а також складність визначення юрисдикції у трансакціях через Інтернет, існують численні прогалини в законодавстві. Ці прогалини можуть призводити до

зловживань, зокрема шахрайських схем, і ускладнювати захист прав споживачів.

Зокрема, такі питання, як правовий статус електронних договорів, відповідальність за виконання зобов'язань у сфері електронної комерції, захист прав споживачів у мережі Інтернет, а також питання юрисдикції для вирішення спорів в міжнародному контексті, потребують удосконалення. Ураховуючи масштаби цієї проблеми, важливо впроваджувати сучасні механізми, що забезпечать ефективний контроль за правовідносинами у віртуальному просторі та дадуть змогу своєчасно реагувати на порушення прав громадян і підприємств у цьому середовищі [45].

Основні труднощі у доведенні шахрайства в Інтернеті полягають у таких аспектах:

1. Анонімність учасників. В Інтернеті важко ідентифікувати шахраїв через анонімність користувачів і можливість використання фальшивих даних.

2. Невизначеність щодо умов угоди. Інтернет-угоди часто укладаються на підставі стандартних умов, що можуть бути неправильно зрозумілі чи не належно представлені покупцям.

3. Технічні складнощі: Для збору доказів необхідно мати доступ до електронної переписки, транзакційних записів та іншої цифрової інформації, що може бути технічно складно або не завжди доступно.

4. Різноманітність платіжних систем і способів оплати. Оскільки оплата може здійснюватися через різні платіжні системи, включаючи електронні гаманці, криптовалюти тощо, це додає складнощів у процес розслідування.

Для ефективного розслідування таких кримінальних правопорушень важливо розуміти специфіку укладання електронних угод і порядок здійснення онлайн-розрахунків. Серед необхідних кроків для забезпечення належного правосуддя:

- Встановлення чітких алгоритмів для збору електронних доказів (наприклад, логів транзакцій, скріншотів сайтів, записів про угоди).
- Використання новітніх технологій для відстеження шахрайських схем (наприклад, блокчейн для перевірки транзакцій).
- Навчання правоохоронців для розпізнавання ознак шахрайства в Інтернеті та ефективного збору доказів.

Таким чином, хоча правові норми дозволяють кваліфікувати шахрайство в інтернет-торгівлі як злочин, для ефективного розслідування таких випадків необхідно враховувати технічні та юридичні особливості цього виду правочинів.

1.3. Сутність, ознаки та види шахрайства, вчиненого з використанням цифрових технологій

Швидкий розвиток технологій, особливо у сфері цифрових технологій, значно розширює як можливості для правопорушників, так і для органів правопорядку, які намагаються адаптуватися до нових умов. З одного боку, технології дають переваги для розвитку економіки та суспільства, 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, через комп’ютерні злочини, кібершахрайство та інші види протиправних діянь.

Серед науковців виникає необхідність уточнення понять «комп’ютерне кримінальне правопорушення» та «кіберзлочин». Ці терміни не завжди однозначно визначаються, що призводить до різних підходів у практиці застосування кримінально-правових норм, а також до необхідності оновлення законодавства для чіткої кримінально-правової оцінки таких правопорушень.

1) комп’ютерне кримінальне правопорушення зазвичай розглядається як будь-яке кримінальне правопорушення, вчинений з використанням

комп’ютерної техніки або на комп’ютерних системах, незалежно від того, чи стосується це власності, інформації чи іншої сфери.

2) кіберзлочин є більш вузьким поняттям, яке включає кримінально протиправні діяння, що безпосередньо здійснюються через Інтернет або інші комп’ютерні мережі, і можуть бути пов'язані з несанкціонованим доступом до інформації, хакерськими атаками, вірусними програмами тощо.

Погоджуємося з науковцями у тому, що розвиток цифрових технологій вимагає перегляду існуючих підходів до правової оцінки комп’ютерних та кіберзлочинів. У зв’язку з цим, важливо визначити нові правові норми та удосконалити існуючі для забезпечення ефективного протидії кримінально протиправним посяганням, що здійснюються з використанням цифрових технологій [58, с. 77–86; 188; 2]; необхідність здійснення подальших досліджень і вдосконалення правових норм, які регулюють ці злочини, забезпечуючи чітке відмежування та відповідне правове реагування на нові форми кримінальної діяльності в умовах інформаційних технологій [96; 60; 8; 62; 113; 121]; відсутність чіткої позиції щодо кримінально-правової кваліфікації несанкціонованих транзакцій у платіжних системах [59; 151].

Кібершахрайство охоплює широкий спектр шахрайських дій, що здійснюються за допомогою цифрових технологій. Воно може проявлятися в різних формах, від крадіжки персональних даних до маніпуляцій із фінансовими ресурсами в Інтернеті.

Кібершахрайство має різноманітні форми та методи здійснення, включаючи:

1. Фішинг – шахрайська практика, коли зловмисники маскуються під надійні установи (банки, інтернет-магазини, платіжні системи тощо) для того, щоб отримати конфіденційну інформацію (паролі, логіни, номери карток) через фальшиві електронні листи, вебсайти або SMS-повідомлення.

2. Вишинг (Voice phishing) – це вид фішингу, де шахраї використовують телефонні дзвінки для того, щоб під виглядом банківського

працівника або іншої установи отримати від жертви важливу інформацію, наприклад, паролі або номери карток.

3. Смішинг (SMS phishing) – шахрайство через текстові повідомлення, де злочинці надсилають посилання або просять повідомити персональні дані.

4. Малваре (Malware) – програмне забезпечення, яке встановлюється на комп'ютер або мобільний пристрій жертви без її відома. Це можуть бути віруси, трояни, шпигунські програми, які призначені для крадіжки даних, контролю над пристроєм або його пошкодження.

5. Скам (Scam) – загальний термін для шахрайських схем, таких як «Нагорода за виграш» чи «Чудова інвестиційна можливість», коли жертву вводять в оману для того, щоб вона передала гроші або інші активи шахраям.

6. Інтернет-торгівля фальшивими товарами – шахрайство через інтернет-магазини, де продаються неіснуючі або підроблені товари. Після отримання передоплати покупець не отримує товар.

7. Крадіжка особистих даних (Identity theft) – отримання зловмисниками особистої інформації (ім'я, адреса, номер паспорта, номер картки) з метою здійснення фінансових операцій або для інших незаконних цілей.

8. Фальшиві онлайн-оголошення та афери з орендою – шахраї пропонують оренду житла або автомобіля за зниженими цінами, вимагаючи передплату, але не надаючи товар або послугу.

9. Шахрайство з криптовалютами – афери, пов'язані з інвестиціями в криптовалюти, коли шахраї обіцяють великий прибуток від інвестицій в невідомі або фальшиві криптовалютні платформи.

10. Аферисти з фальшивими онлайн-платежами – використання підроблених вебсайтів для здійснення платежів, де шахраї отримують гроші за товар або послугу, яку насправді не існує.

11. Шахрайство з кредитними картками – незаконне використання чужих кредитних карток для здійснення покупок або переведення грошей.

12. Маніпуляції в соціальних мережах – використання платформ соціальних медіа для здійснення шахрайства, включаючи створення фальшивих профілів для введення в оману інших користувачів [10, с. 195].

13. Платіжні шахрайства через мобільні додатки – зловмисники створюють фальшиві додатки для мобільних пристроїв, що крадуть інформацію про банківські рахунки або платіжні дані.

Ці форми кібершахрайства постійно змінюються та вдосконалюються, оскільки злочинці шукають нові методи обману у відповідь на зміни в технологіях і методах безпеки [39].

Варто зазначити, що судова практика в цій галузі є незамінним джерелом для розуміння того, як застосовуються норми кримінального права до нових форм кримінальних правопорушень, що вчиняються за допомогою цифрових технологій.

Враховуючи специфіку таких кримінальних правопорушень, як шахрайство в інтернет-просторі чи кібератаки, аналіз судових рішень дозволяє: виявити, як на практиці кваліфікуються різні види кримінальних правопорушень, що вчиняються за допомогою цифрових технологій, і які принципи використовуються суддями під час розгляду таких справ; недоліки в законодавстві, що потребують уточнення або удосконалення для забезпечення більш ефективної боротьби з кіберзлочинністю; які види покарань застосовуються в цих справах і як вони відповідають тяжкості кримінальних правопорушень, а також чи є система покарань достатньо стримуючою для нових форм кримінально протиправної діяльності; виділити найбільш типові та важливі прецеденти, що можуть стати основою для подальшого розвитку правозастосування у галузі протидії кіберзлочинності [100].

Аналіз судових рішень, проведений на основі даних із Єдиного державного реєстру судових рішень, дозволяє зробити висновок про те, що кількість вищевказаних кримінальних правопорушень зменшується. Відзначена тенденція зменшення кількості вироків упродовж останніх років

та подальше скорочення цього показника в наступні роки вказує на декілька можливих причин, зокрема зміни в ефективності розслідувань, вдосконалення правоохоронної діяльності або трансформацію кримінально протиправних схем.

Згідно з отриманими даними, найбільш поширеними серед судових рішень є категорії «продаж товарів або надання послуг» (66 % від загальної кількості вироків) та «несанкціоновані транзакції» (35%). Це свідчить про значне поширення шахрайства через інтернет, де злочинці використовують сучасні технології для обману споживачів.

У категорії «продаж товарів або надання послуг» найбільш поширені випадки обману, пов’язані з продажем товарів або послуг, які фактично не існують. Як правило, такі шахрайства мають такі основні характеристики:

1. Фальшиві пропозиції товарів та послуг: наприклад, злочинці пропонують через інтернет «продаж» одягу, електроніки, меблів, туристичних путівок або навіть «оренду» квартир. Придбання товару або послуги зазвичай передбачає часткову або повну передплату, яку потім шахраї привласнюють.

2. Шахрайські пропозиції послуг: це можуть бути послуги з працевлаштування за кордоном, виготовлення меблів, допомога в отриманні кредитів або інші послуги, які ніколи не надаються після отримання коштів від споживачів.

3. Використання популярних онлайн-майданчиків: шахраї часто створюють акаунти або публікують пропозиції на популярних інтернет-ресурсах або онлайн-майданчиках, що дозволяє їм досягти ширшої аудиторії і здійснити більшу кількість обманів.

4. Створення фальшивих сайтів: у деяких випадках винні особи самостійно створюють спеціалізовані сайти або кілька сайтів для подальшого обману. Вони можуть використовувати такі ресурси для реклами своїх «товарів» або «послуг» та виглядати більш надійно.

Для здійснення шахрайських операцій з товаром або послугами злочинці використовують такі методи: 1) фальшиві оголошення, а саме створення рекламних оголошень, які виглядають як реальні пропозиції від справжніх продавців або компаній; 2) пропозиції із завищеними цінами: Іноді шахраї пропонують товари або послуги за дуже низькими цінами, що викликає у потенційних жертв бажання здійснити покупку; 3) маніпуляція з відгуками, оскільки часто використовуються фальшиві позитивні відгуки для підвищення довіри до шахрайських сайтів або акаунтів; 4) невизначені умови угоди: Невідомі або непрозорі умови договору про покупку або надання послуг, що дозволяє зловмисникам маніпулювати покупцями [49, с. 43].

Категорія «несанкціоновані транзакції» охоплює випадки, коли особи, які не є власниками карткових рахунків, здійснюють фінансові операції без дозволу власників карток, використовуючи їхні платіжні реквізити або інші шахрайські методи. Найбільш поширені варіанти таких кримінально протиправних дій включають:

1) Неавторизовані перекази коштів. У цьому випадку злочинці використовують реквізити платіжних карток інших осіб для здійснення безготівкових платежів або переказів. Це може бути реалізовано через онлайн-сервіси переказів, де злочинці без дозволу власників карток перераховують кошти на свої рахунки або рахунки спільників. Як приклад, у вироку Суворовського районного суду м. Одеси від 22.07.2018 згадано випадок, коли особа, маючи реквізити карток інших осіб, за допомогою онлайн-платежів переводила гроші на рахунки спільників, а ті знімали готівку через банкомати [21].

2) Виготовлення та використання підроблених карток. Це один із найбільш поширених методів шахрайства, коли злочинці створюють підроблені платіжні картки за допомогою отриманих реквізитів або підроблених даних. Такі картки можуть бути використані для несанкціонованих транзакцій, таких як покупки в інтернеті або в торгових точках.

3) Використання скімінгових пристроїв. Зловмисники використовують скімінгові пристрої для зчитування даних з магнітних стрічок платіжних карток під час їх проведення через банкомати або платіжні термінали. Після того як інформація з картки була скопійована, її можна використовувати для несанкціонованих транзакцій.

4) Отримання реквізитів через телефонні дзвінки. В цьому випадку злочинці можуть телефонувати потерпілим під виглядом співробітників банку або інших установ і просити надати реквізити платіжних карток, наприклад, для «екстреного поповнення рахунку». Використовуючи ці дані, вони здійснюють незаконні транзакції.

5) Спроби шахрайства з мобільними фінансами. Деякі злочинці замовляють копії сім-карт, щоб отримати доступ до мобільних фінансових рахунків або послуг, а потім використовують отриману інформацію для здійснення несанкціонованих операцій [18; 23; 22; 20].

Категорія «протиправна діяльність працівників банків» охоплює порушення, вчинені працівниками фінансових установ, які використовують своє службове становище для несанкціонованого доступу до коштів клієнтів та їх незаконного заволодіння. Це може включати:

1) Випуск додаткових платіжних карток. Наприклад, в одному з випадків, розглянутих у вироку Голосіївського районного суду м. Києва від 23.06.2014, працівник банку без відома клієнтів випускав додаткові платіжні картки для доступу до їхніх рахунків. Він використовував ці картки для незаконного заволодіння коштами клієнтів банку. Такий тип шахрайства є особливо небезпечним, оскільки працівник банку має доступ до конфіденційної інформації клієнтів та може здійснювати дії, які важко відслідкувати без додаткових перевірок [24].

2) Незаконне отримання кредитів. Ця категорія включає випадки, коли шахраї, використовуючи дані потерпілих або підроблені документи, отримують кредити на ім’я інших осіб без їх відома або дозволу. Один із таких випадків — це замах на шахрайство шляхом використання цифрових

технологій, коли зловмисники надсилають підроблені електронні копії документів для отримання кредиту. Це може стосуватися як фізичних осіб, так і юридичних осіб, коли кредити оформлюються на підставі фальшивих документів [17].

Категорія «незаконне отримання кредитів» охоплює кримінальні правопорушення, пов'язані з оформленням кредитів або замовленням матеріальних цінностей від імені потерпілих осіб без їх згоди чи відома. Такі правопорушення можуть включати:

1) Оформлення кредитів на третіх осіб. Злочинці використовують персональні дані потерпілих, включаючи паспортні дані, ідентифікаційні коди чи інші документи, для отримання кредитів. У таких випадках потерпілі не підозрюють про укладення кредитного договору до моменту, коли їм надходять вимоги щодо повернення коштів або інформація про заборгованість.

2) Замовлення матеріальних цінностей. Зловмисники оформлюють замовлення товарів чи послуг на ім'я потерпілих осіб. Наприклад, шахраї можуть замовляти дорогі технічні пристрої чи автомобілі, використовуючи фальшиві документи або отримані незаконним шляхом дані.

3) Використання підроблених документів. У випадку, розглянутому як замах на шахрайство, для отримання кредиту зловмисники надсилали електронні копії підроблених документів до фінансових установ. Ці документи могли включати фальшиві довідки про доходи, підроблені договори чи інші офіційні папери [17].

Останнім часом серйозною проблемою у сфері інформаційної та кібербезпеки є соціальний інжиніринг. Це психологічна маніпуляція, спрямована на те, щоб змусити жертву розкрити конфіденційну інформацію або вчинити певні дії, які йдуть на користь зловмиснику [197, с. 310]. У контексті шахрайства соціальний інжиніринг являє собою цілеспрямоване психологічне маніпулювання потерпілими для отримання конфіденційної інформації або змушення їх до вчинення певних дій, вигідних зловмисникам.

Цей метод базується на вразливостях людської психології, таких як довіра, страх, або бажання допомогти [194, с. 17]. Соціальний інжиніринг базується на використанні психологічних механізмів та вразливостей людської натури для досягнення особистої користі.

Прикладом є вирок Жовтневого районного суду м. Дніпра від 20.05.2022, де засуджено особу, яка створила фіктивний профіль на сайті знайомств. Після встановлення довірливих відносин шахрайка дізнавалася інформацію про потерпілих, їхнє матеріальне забезпечення та інші деталі. Потім вона вигадувала різні обставини для отримання грошових коштів, не маючи наміру їх повертати [16].

Соціальний інжиніринг є викликом для правоохоронних органів через складність доведення провини, а також через необхідність удосконалення механізмів розслідування таких злочинів і правового регулювання. Ефективна протидія вимагає не лише технологічних засобів захисту, але й підвищення рівня обізнаності громадян щодо ризиків маніпуляцій.

Такий підхід до шахрайства, як штучне створення ситуацій страху або паніки, є поширеним методом соціального інжинірингу. Зловмисники цілеспрямовано маніпулюють емоціями потерпілих, використовуючи страх за близьких чи власне майбутнє, щоб змусити їх діяти на користь злочинців.

Прикладом є вирок Перевальського районного суду Луганської області від 03.04.2014. У цій справі зловмисник, перебуваючи у місцях позбавлення волі, зателефонував потерпілій та повідомив, що її син затриманий за підозрою у скоєнні злочину. Він вимагав передачі грошей для «вирішення питання» про уникнення кримінальної відповідальності, вказавши, що кошти потрібно перерахувати на банківський рахунок. Залякана потерпіла виконала вимоги злочинця [19].

Інші випадки стосуються штучного створення ситуацій страху або паніки, що є поширеним методом соціального інжинірингу. Зловмисники цілеспрямовано маніпулюють емоціями потерпілих, використовуючи страх за близьких чи власне майбутнє, щоб змусити їх діяти на користь злочинців.

Прикладом є вирок Перевальського районного суду Луганської області від 03.04.2014. У цій справі зловмисник, перебуваючи у місцях позбавлення волі, зателефонував потерпілій та повідомив, що її син затриманий за підозрою у скоєнні злочину. Він вимагав передачі грошей для «вирішення питання» про уникнення кримінальної відповідальності, вказавши, що кошти потрібно перерахувати на банківський рахунок. Залякана потерпіла виконала вимоги злочинця.

У подальшому ми проаналізували кожну групу для того, щоб дослідити питання кримінально-правової кваліфікації, встановити особливості призначення покарання, визначити тенденції застосування звільнення від покарання з випробуванням з метою удосконалення виявлення і розслідування таких правопорушень.

У судових рішеннях, віднесених до категорії «продаж товарів», дії винних осіб не завжди отримували кримінально-правову оцінку як шахрайство, вчинене шляхом незаконних операцій з використанням цифрових технологій. За умови близьких обставин вчинення кримінальних правопорушень, з 439 судових рішень означеної категорії, названу кваліфікуючу ознаку було інкриміновано у 292 (67%). У третині досліджених вироків, дії осіб, які використовували для вчинення шахрайства торгівельні інтернет-майданчики пропонуючи неіснуючі товари та послуги з метою подальшого заволодіння передплатою, було кваліфіковано як звичайне шахрайство.

Аналіз судових рішень, пов’язаних із шахрайством у категорії «продаж товарів», виявив суттєві особливості у 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 шляхом незаконних операцій із використанням комп’ютерної техніки (ст. 190 ч. 3 КК України). У цих випадках зловмисники

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 (ст. 190 ч. 1-2 КК України). Це спостерігалося навіть за аналогічних обставин, коли злочинці застосовували інтернет-технології для отримання коштів від потерпілих.

Така ситуація щодо різного підходу до кваліфікації зумовлена такими факторами:

1) Розбіжності в судовій практиці та недостатня уніфікація тлумачення кваліфікуючих ознак суддями. У деяких випадках 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 у КК України.

Аналіз судових рішень у категорії «продаж товарів» виявив цікаву закономірність: у 14% випадків (21 вирок із 146), коли кваліфікуюча ознака «шляхом незаконних операцій з використанням електронно-обчислювальної техніки» не була інкримінована, суди додатково обґрунтовували свої рішення.

Суди наголошували, що сам факт використання інтернет-майданчиків або технічних засобів не завжди є вирішальним для кваліфікації кримінального правопорушення за ознакою застосування електронно-обчислювальної техніки. 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.

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 цифрових технологій. Це може спричиняти нерівність у підходах до кримінальної відповідальності в залежності від судового округу або складу суду. Саме тому, на нашу думку, для уникнення неоднакового тлумачення судами кваліфікуючих ознак, доцільно внести уточнення до статті 190 КК України щодо специфіки використання технічних засобів у шахрайських схемах. Тому нами запропоновано викласти ч. 4 ст. 190 КК України у такій редакції: «4. Шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням цифрових технологій, - карається позбавленням волі на строк від трьох до восьми років» А також доцільно додати примітку до статті, вказавши, що ч. 4 цієї статті може застосовуватись лише у разі використання як інструменту для реалізації незаконних операцій. Таку пропозицію підтримали й практичні працівники (Додаток А).

Аналіз судової практики, що стосується несанкціонованих транзакцій, демонструє значну тенденцію кваліфікації таких дій як крадіжка, а не шахрайство. Це може свідчити про проблеми в правозастосуванні та недостатньо чіткі критерії для розмежування різних видів кримінальних правопорушень у сфері цифрових технологій. За відповідними критеріями визначено 1324 вироки, що відповідали ним. На основі аналізу встановлено,

що із загальної кількості вироків (1257), близько 870 (69%) містять кваліфікацію несанкціонованих транзакцій як крадіжку.

Поточна судова практика демонструє, що більшість злочинів у категорії «несанкціоновані транзакції» кваліфікуються як крадіжка, що може свідчити про спрощений підхід до правозастосування у сфері кіберзлочинності. Для вдосконалення цієї практики необхідно враховувати технічні особливості таких кримінальних правопорушень і сприяти їх належній кримінально-правовій оцінці [173, с. 162].

Така позиція суддів обумовлена тим, що протиправна транзакція, здійснена з карткового рахунку потерпілої особи, розглядається судами як безпосереднє заволодіння майном. Грошові кошти на рахунку часто трактуються як «матеріальні цінності», які підпадають під ознаки крадіжки.

Проведений аналіз свідчить про суттєву несталість судової практики щодо кримінально-правової кваліфікації шахрайства, вчиненого із застосуванням комп'ютерних технологій. Це відображає недосконаліть нормативно-правової бази, відсутність чітких критеріїв розмежування окремих складів кримінальних правопорушень та неоднорідність у підходах судів.

Отже, на основі вищесказаного можемо зробити такі висновки:

1) присутня суттєва різниця у кваліфікації подібних правопорушень**.** Так, шахрайство при продажу товарів та послуг через інтернет-майданчики: у 67% випадків кваліфікується як шахрайство із використанням комп'ютерної техніки, у 33% – як звичайне шахрайство.

2) несанкціоновані транзакції з платіжними картками: у 85% випадків кваліфікуються як крадіжка і лише у 15% – як шахрайство.

3) недостатність інкримінування спеціальних кваліфікуючих ознак. Навіть у випадках, коли дії кваліфіковані як шахрайство, ознака «вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки» не інкримінується у 13% вироків.

4) проблеми кваліфікації дій працівників банків та використання технік соціального інжинірингу. Судова практика демонструє неоднозначність у підходах до таких дій, що свідчить про складність їх оцінки в межах чинного законодавства.

5) ліберальність реалізації кримінальної відповідальності, зокрема звільнення від покарання у справах про шахрайство, вчинене з використанням комп'ютерної техніки, становить 59%. Це значно перевищує рівень звільнення від покарання у справах про шахрайство в цілому – 32%, рівень звільнення від покарання у справах про кримінальні правопорушення проти власності – 42%, середній рівень звільнення від покарання за всі категорії справ – 42%.

Висновки до розділу 1

1. Зазначено, що термін «електронно-обчислювальна техніка», який використовується у Кримінальному кодексі України, є застарілим і давно вже не відповідає ні реаліям сьогодення, ні вимогам законодавства. Натомість використовуються терміни «інформаційні технології», «цифрові технології» у законодавстві і в практиці його застосування. Так, із набранням чинності Закону України «Про цифровий контент та цифрові послуги» у 2024 році впроваджені у використання терміни «цифрові послуги», «цифрові технології», «цифровий контент» . Саме тому пропонуємо замінити у КК України термін «електронно-обчислювальна техніка» на «цифрові технології».

2. Злочинці використовують Інтернет для здійснення різноманітних правопорушень, що додає нових складнощів у боротьбу з кримінально протиправною діяльністю, оскільки традиційні методи правозастосування часто виявляються малоефективними для вирішення проблем, пов'язаних з цифровим середовищем. Це підкреслює важливість адаптації правових та криміналістичних підходів до нових реалій, зокрема у боротьбі з такими

кримінальними правопорушеннями, які стають усе більш поширеними та складними у розслідуванні.

Згідно з матеріалами судово-слідчої практики, шахраї часто використовують певні платформи для здійснення кримінальних правопорушень, зокрема «Інтернет-аукціони» та «дошки оголошень», через їх доступність та особливості функціонування.

На цих платформах часто відсутні системи захисту покупців, що робить їх вразливими до шахрайських схем. Враховуючи їх популярність і зростання онлайн-торгівлі, важливо підвищувати рівень обізнаності споживачів щодо ризиків, що виникають на таких платформах, а також розробляти більш ефективні методи регулювання та захисту від шахрайства у цьому сегменті інтернет-торгівлі.

3. Проведений аналіз свідчить про суттєву несталість судової практики щодо кримінально-правової кваліфікації шахрайства, вчиненого із застосуванням цифрових технологій. Така ситуація зумовлена такими факторами:

1) Розбіжності в судовій практиці та недостатня уніфікація тлумачення кваліфікуючих ознак суддями. У деяких випадках 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 у КК України.

РОЗДІЛ 2
ОСОБЛИВОСТІ ДОКАЗУВАННЯ ШАХРАЙСТВА, ВЧИНЕНОГО З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

2.1. Обставини, що підлягають доказуванню у справах про шахрайство, вчинене з використанням цифрових технологій

Виявлення кримінального правопорушення є ключовим початковим етапом у процесі розслідування кримінальних правопорушень, адже саме цей етап забезпечує формування правових підстав для подальших слідчих (розшукових) та оперативно-розшукових дій. Виявлення таких діянь є підґрунтям для прийняття подальших рішень у кримінальному процесі. Помилки на цьому етапі можуть призвести до затримки в розслідуванні, втрати важливих доказів або навіть до відмови у реєстрації кримінального провадження. Тому якісна робота на етапі виявлення є запорукою успішного розкриття кримінального правопорушення та притягнення винних до відповідальності.

Виявлення та розслідування кримінального правопорушення є складним процесом, що охоплює сукупність дій, спрямованих на встановлення події кримінального правопорушення, виявлення особи, яка його вчинила, і забезпечення збирання доказів, які підтверджують її винуватість. Цей процес є невід’ємною частиною кримінального провадження, а його ефективність визначається якістю розшукової діяльності.

Варто зазначити, що виявлення та розслідування кримінального правопорушення не обмежується лише встановленням особи підозрюваного. Воно включає забезпечення доказів, що підтверджують вчинення кримінального правопорушення, а також дотримання законності всіх процесуальних дій. Ефективна взаємодія слідчих та оперативних підрозділів є ключовою для успішного завершення цього процесу.

У даному контексті робота слідчого та оперативних підрозділів по «гарячих слідах» є важливим етапом розслідування кримінального правопорушення, оскільки в цей період зберігається найбільша кількість невтрачених доказів, які можуть бути швидко зібрані та використані у процесі досудового розслідування. Основними завданнями, які вирішуються на цьому етапі, є:

1. Установлення просторово-часових зв'язків: аналіз розташування слідів кримінального правопорушенння, наприклад, слідів рук, ніг, транспортних засобів, визначення хронології події, що дає змогу відновити послідовність дій злочинця.

2. Ідентифікація та затримання особи злочинця: використання оперативної інформації, описів свідків, записів з камер спостереження, проведення заходів для виявлення злочинця в зоні найближчого пересування.

3. Виявлення та аналіз негативних обставин: встановлення фактів, які не відповідають звичайному перебігу подій, наприклад, незвичне положення тіла, відсутність типових слідів боротьби або слідів втечі, з'ясування причин наявності чи відсутності цих обставин для формування гіпотез щодо механізму вчинення кримінального правопорушення.

У підтримку цього важливою є позиція О. А. Самойленка, оскільки вона підкреслює специфічність розслідування кримінальних правопорушень у кіберпросторі, що суттєво відрізняються від традиційних кримінальних правопорушень. Особливості механізму вчинення таких правопорушень визначають ключові виклики для слідчих та оперативних підрозділів [157, с. 409].

Виявлення ознак кримінального правопорушення є першим і важливим етапом у процесі розслідування. Це може відбуватися кількома основними способами, кожен із яких має свої особливості:

1. Вжиття оперативно-розшукових заходів. До початку досудового розслідування оперативні підрозділи здійснюють заходи з виявлення кримінально протиправної діяльності. Це можуть бути спостереження,

прослуховування, аналітична обробка інформації або оперативні контакти. Результати таких заходів є підґрунтям для початку кримінального провадження.

2. Звернення громадян та представників державних організацій, а саме заяви та повідомлення про кримінальні правопорушення, які надходять від фізичних чи юридичних осіб, результати перевірок та контрольних заходів, які проводяться державними установами (наприклад, аудит, податкові перевірки), також можуть свідчити про наявність ознак кримінального правопорушення.

3. Безпосереднє виявлення слідчим, прокурором чи судом. Ознаки правопорушення можуть бути встановлені під час здійснення досудового розслідування за іншим провадженням або при розгляді кримінальної чи цивільної справи в суді. Це може бути виявлення фактів, які раніше не були предметом розгляду, але мають ознаки кримінально протиправної діяльності.

Згідно із чинним кримінальним процесуальним законодавством України, будь-яка процесуальна діяльність, пов’язана з розслідуванням кримінального правопорушення, може здійснюватися виключно в рамках досудового розслідування, яке розпочинається після внесення відповідних відомостей до Єдиного реєстру досудових розслідувань (ЄРДР) [91].

Цей процес регламентовано статтею 214 Кримінального процесуального кодексу України, яка визначає порядок дій для початку досудового розслідування [91].

Відомості про обставини, що можуть свідчити про вчинення кримінального правопорушення, мають бути отримані слідчим, прокурором або іншою уповноваженою особою. Такі відомості можуть надходити через заяви, повідомлення, а також інші джерела, які містять інформацію про кримінальне правопорушення.

Отримана інформація фіксується у відповідній заяві чи повідомленні, після чого слідчий або прокурор зобов’язані внести ці відомості до ЄРДР протягом 24 годин з моменту їх надходження.

Лише після внесення відомостей до ЄРДР можна здійснювати процесуальні дії, зокрема: проведення допитів; обшуків; проведення експертиз; інші дії, передбачені КПК України [91].

Особливо це стосується розслідування таких специфічних кримінальних правопорушень, як кібершахрайство, які часто потребують негайних та ретельних дій для збереження доказів, оскільки вони можуть бути швидко знищені або модифіковані в кіберпросторі.

Таким чином, внесення даних до ЄРДР є обов'язковою юридичною передумовою для початку розслідування будь-якого кримінального правопорушення в Україні, що забезпечує його легітимність і можливість використання здобутих доказів у суді.

Відповідно до Порядку ведення єдиного обліку заяв і повідомлень про кримінальні правопорушення та інші події, затвердженого наказом МВС України від 08.02.2019 № 100, а також Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України, затвердженої наказом МВС від 27.04.2020 № 357 (далі – Інструкція № 357), порядок дій правоохоронних органів при отриманні інформації про правопорушення чітко регламентований [53; 134].

Оперативний черговий органу (підрозділу) поліції або інша уповноважена службова особа, отримавши інформацію про вчинення кримінального правопорушення або іншу подію, зобов'язана негайно зареєструвати її в журналі єдиного обліку заяв і повідомлень про кримінальні правопорушення та інші події.

Реєстрація здійснюється за допомогою інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», що забезпечує централізовану обробку даних та уніфікацію процесу реєстрації.

Інформація про кримінальні правопорушення вноситься до єдиного обліку незалежно від способу її отримання: через особисте звернення

громадян; засобами зв'язку (телефон, електронна пошта); шляхом надходження офіційних документів.

Після реєстрації уповноважені особи зобов'язані вжити заходів відповідно до визначених процедур, зокрема передати інформацію слідчому або до іншого компетентного підрозділу для її перевірки і подальшого внесення до Єдиного реєстру досудових розслідувань (ЄРДР), якщо є ознаки кримінального правопорушення.

Типовий алгоритм попередніх дій та заходів групи реагування визначений низкою нормативних документів, зокрема: Інструкція № 357, яка егламентує порядок реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події, забезпечуючи координацію та оперативність дій групи реагування та Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України, затверджена наказом МВС від 07.07.2017 № 575 [53, 52].

Порядок єдиного обліку в органах поліції (наказ МВС України від 08.02.2019 № 100) визначає джерела інформації про кримінальні правопорушення та події, які можуть слугувати підставою для початку досудового розслідування. Ці джерела є основою для реєстрації заяв і повідомлень у журналі єдиного обліку та подальшого внесення даних до Єдиного реєстру досудових розслідувань (ЄРДР).

Як ми уже зазначали, основними джерелами інформації є:

1. Заяви (повідомлення) від осіб, які надходять до органів поліції чи посадових осіб, уповноважених приймати та реєструвати заяви.

2. Самостійне виявлення обставин кримінального правопорушення уповноваженими особами поліції з будь-яких джерел (наприклад, під час моніторингу мережі Інтернет).

3. Повідомлення про затримання підозрюваної особи під час вчинення кримінального правопорушення, замаху, або безпосередньо після його вчинення.

4. Анонімні повідомлення: дзвінки, листи чи інші способи повідомлення про можливі правопорушення.

Аналіз матеріалів кримінальних проваджень показує, що приводи для початку досудового розслідування з питань кібершахрайства розподіляються таким чином:

1. Заяви від громадян-жертв шахрайських дій – 60%. Найбільш поширений привід. Потерпілі звертаються після втрати грошей або завдання іншої шкоди.

2. Заяви про сумнівні вебресурси чи організації – 8%. Це можуть бути повідомлення про сайти, які імітують роботу інтернет-магазинів, але фактично займаються шахрайством.

3. Повідомлення від організацій чи представників влади – 12%. Наприклад, випадки, коли фінансові установи або держоргани виявляють підозрілі транзакції чи діяльність.

4. Анонімні повідомлення – 4%. Вони включають дзвінки на гарячу лінію чи листи з викладенням фактів шахрайства.

5. Самостійне виявлення кримінальних правопорушень працівниками поліції – 16%. Це можуть бути результати моніторингу інтернет-ресурсів, соціальних мереж, форумів тощо.

Такі статистичні спостереження дозволяють удосконалити роботу поліції у сфері запобігання та розкриття кібершахрайства. Зокрема:

- Підвищення обізнаності громадян щодо можливих ризиків.
- Акцент на моніторингу інтернет-ресурсів для своєчасного виявлення шахрайських схем.
- Посилення співпраці з підприємствами та організаціями, які можуть стати джерелом інформації про підозрілу діяльність.

Кримінальні правопорушення, вчинені за допомогою цифрових технологій, мають низку специфічних особливостей, які ускладнюють їх виявлення та протидію. Зокрема, інформація про такі діяння рідко надходить

від джерел, пов’язаних із безпосереднім затриманням підозрюваних осіб у момент вчинення кримінального правопорушення або одразу після нього.

На думку С.В. Самойлова, це зумовлено кількома чинниками. Кіберзлочинці використовують технології, які дозволяють приховувати свою особу, місце перебування і сліди кримінально протиправної діяльності (використання VPN, TOR, підроблених облікових записів, шифрування даних тощо). Багато кримінальних правопорушень у кіберпросторі вчиняються дистанційно, часто з використанням інфраструктури в іншій країні, що ускладнює оперативне реагування і затримання. Потерпілі або навіть установи можуть не одразу виявити факт шахрайства, особливо якщо йдеться про складні схеми обману або викрадення інформації. Це створює часовий розрив між кримінальним правопорушень і його виявленням. Жертви часто не повідомляють про шахрайство через сором, страх втратити репутацію чи брак довіри до правоохоронних органів. Кіберзлочинці використовують передові технології і методи, які роблять їх діяльність малопомітною для звичайних інструментів моніторингу та виявлення. Окрім цього, кібершахрайство нерідко має транскордонний характер, коли злочинці діють у різних юрисдикціях, що ускладнює координацію правоохоронних органів різних країн [160, с. 68].

На початковому етапі розслідування кібершахрайства основним завданням слідчого є отримання, вивчення та правова оцінка первинної інформації, яка надходить з різних джерел. Цей етап має важливе значення, оскільки він закладає основу для подальшого розслідування. Зокрема, від якості та повноти відомостей, внесених до ЄРДР, залежить хід розслідування, а також ефективність використання доступних слідчому інструментів.

На етапі оцінки первинної інформації слідчий стикається із законодавчими обмеженнями, які мають забезпечити правомірність і прозорість дій у досудовому розслідуванні. Згідно з чинним законодавством, проведення будь-яких процесуальних дій до внесення відомостей до ЄРДР є

забороненим. У разі порушення цієї вимоги посадова особа несе відповідальність, установлену законом.

Так, на початковому етапі розслідування важливе значення має правильна кваліфікація діяння. О. В. Тарасова піднімає проблематику правової кваліфікації кримінальних правопорушень, вчинених за допомогою цифрових технологій, яку піднімає, має суттєве значення для забезпечення єдності правозастосування та ефективності боротьби з такими кримінальними правопорушеннями

Зокрема, часто зустрічається різне розуміння сутності незаконних операцій з використанням електронно-обчислювальної техніки. Частина 4 статті 190 КК України передбачає відповідальність за шахрайство, вчинене шляхом використання електронно-обчислювальної техніки, але тлумачення цього терміна не є однозначним. Деякі суди вважають, що сам факт розміщення неправдивої інформації на сайті або отримання коштів через електронні платіжні системи є використанням електронно-обчислювальної техніки як засобу вчинення кримінального правопорушення. Інші ж суди не визнають це «незаконною операцією» і вважають, що такі дії слід кваліфікувати за менш тяжкими частинами ст. 190 КК України [167, с. 485–487].

Наприклад, досить часто перерахування грошей оцінюється як нейтральна операція. Перерахування потерпілими коштів на рахунок злочинця в електронній платіжній системі розглядається окремими судами як добровільна дія, що не може бути кваліфікована як шахрайство, учинене шляхом використання електронно-обчислювальної техніки. Це створює прогалину в правозастосуванні, адже саме електронні платіжні системи використовуються як інструмент для отримання кримінально протиправних доходів. На основі цього, вважаємо, що потрібно 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. Також необхідно розробити методичні рекомендації для

слідчих і суддів щодо розслідування та кваліфікації кримінальних правопорушень, пов'язаних із шахрайством в інтернеті. Врахувати специфіку кібершахрайства, яке часто реалізується через складні технологічні схеми, і забезпечити адекватність кваліфікації до рівня суспільної небезпеки цих діянь. Слід зазначити, що таку пропозицію підтримали й практичні працівники (Додаток А).

Проблематика, яка стосується конструкції складу кримінального правопорушення, передбаченого ч. 4 ст. 190 КК України, є актуальною, зокрема через недостатню деталізацію ознак, що враховують специфіку кібершахрайства. Це ускладнює як розслідування, так і судовий розгляд таких справ.

Кібершахрайство, як правило, включає цілий спектр дій, таких як реєстрація на сайтах, створення фіктивних оголошень, маніпуляції з платіжними системами. Однак ці елементи не завжди охоплюються змістом «незаконних операцій із використанням електронно-обчислювальної техніки».

Термін «електронно-обчислювальна техніка» є застарілим і не враховує сучасні технології, зокрема мобільні додатки, блокчейн-системи та інші інновації. Так, кримінально протиправні дії, вчинені у віртуальному просторі, безпосередньо зачіпають суспільні відносини у цьому середовищі, але законодавство не завжди в повній мірі врегульовує ці відносини. Кібершахрайство може реалізуватися через фішинг, шкідливе програмне забезпечення, соціальну інженерію тощо. Однак ці способи фактично не знаходять відображення у кваліфікаційних ознаках, через що виникають проблеми у доказуванні факту цих кримінальних правопорушень.

Саме тому необхідно уточнити поняття «електронно-обчислювальна техніка» у законодавстві, включивши до нього сучасні технології, такі як Інтернет, мобільні пристрої, програмне забезпечення, блокчейн тощо. Для цього потрібно додати до ч. 4 ст. 190 КК України кваліфікуючі ознаки, що охоплюють розміщення неправдивої інформації в інтернеті, використання

фальшивих електронних акаунтів, застосування методів соціальної інженерії тощо. Таку пропозицію підтримують практичні працівники.

Після оцінки первинної інформації визначення напрямів розслідування має особливе значення, оскільки це дозволяє сфокусуватися на конкретних обставинах, які підлягають доказуванню в кримінальному провадженні. У випадку з кримінальними правопорушеннями, вчиненими за допомогою цифрових технологій, важливо правильно визначити й оцінити ті елементи, які складають їх об’єктивну та суб’єктивну сторони.

Так, згідно з ч. 2 ст. 91 КПК України, доказування є процесом збирання, перевірки та оцінки доказів з метою встановлення обставин, які мають значення для кримінального провадження. Це включає в себе всі дії, що направлені на виявлення істини у справі та доведення фактів, які є важливими для кримінального процесу [91].

Предмет доказування, згідно з кримінальним процесуальним законодавством, складається з типових обставин, які визначаються в залежності від конкретного правопорушення, що розслідується. Кожне кримінальне провадження має свої особливості, оскільки межі доказування орієнтуються на конкретні кримінально-правові ознаки кримінального правопорушення [91].

У випадку з кібершахрайством, наприклад, ці обставини можуть включати факти, пов'язані з використанням цифрових технологій, електронних систем, онлайн-платежів та інших сучасних технологічних аспектів, які необхідно буде перевірити для підтвердження фактів кримінально протиправної діяльності. Така специфіка потребує проведення детального розслідування, оскільки інформація може бути зашифрована або видалена, а також бути складною для традиційних методів доказування.

Згідно з ч. 1 ст. 91 КПК України, доказуванню підлягають обставини, що мають значення для забезпечення справедливості у кримінальному провадженні. Це визначення передбачає основні категорії, які завжди повинні бути встановлені при розслідуванні будь-якого злочину, зокрема

обставини вчинення кримінального правопорушення, особа підозрюваного чи обвинуваченого, наслідки кримінального правопорушення тощо.

Водночас, є ще обставини, які не завжди мають пряме правове значення, але можуть суттєво вплинути на стратегію розслідування. Це може бути, наприклад, інформація про спосіб вчинення кримінального правопорушення, час та місце вчинення, інші зовнішні обставини, що дозволяють скласти більш точну картину подій, зібрати додаткові докази або зрозуміти мотиви злочинця. У цьому контексті доцільно говорити про «обставини, що підлягають встановленню», оскільки це уточнення дозволяє виокремити інформацію, яка має важливе значення для подальших тактичних дій у розслідуванні, навіть якщо вона не є частиною обов'язкових доказів.

Таке розмежування допомагає більш ефективно використовувати наявні ресурси та визначати пріоритети у розслідуванні, що особливо важливо в складних і технічно насичених справах, таких як кібершахрайство, де роль кожної деталі та обставини може мати вирішальне значення для встановлення істини.

Слід відмітити, що коло обставин, які підлягають доказуванню в кримінальному провадженні, тісно пов'язане з конкретним складом кримінального правопорушення, визначеним у відповідній нормі кримінального закону. Як показує правозастосовна практика, кожна норма кримінального закону передбачає певні елементи складу кримінального правопорушення (наприклад, об'єкт, об'єктивна сторона, суб'єктивна сторона), які визначають, які саме обставини мають бути встановлені в рамках розслідування.

Згідно з класичним підходом у правознавстві, кожне кримінальне правопорушення має відповідати на основні питання: «що?» — що саме сталося, який факт вчинення правопорушення? «де?» — де відбулося правопорушення, яке місце вчинення кримінального правопорушення? «коли?» — у який час чи в якій період відбулося кримінальне правопорушення? «ким?» — хто є винуватцем, хто є суб'єктом

кримінального правопорушення? «яким чином?» — яким способом було вчинене правопорушення?

Ці питання допомагають визначити обставини, що мають значення для кримінального провадження. Вони формують так звану «картину кримінального правопорушення», що включає в себе не лише конкретні факти, але й обставини, які можуть бути важливими для розуміння мотивації особи, спрямованості її дій, можливих наслідків тощо.

У випадку кібершахрайства, наприклад, ці обставини можуть включати не лише сам факт шахрайства (що сталося), але й технологічний процес вчинення кримінального правоопрушення (як саме злочинець використовував інтернет-ресурси), а також фактори, які можуть вказувати на його мотивацію та спосіб вчинення кримінального правопорушення. Кожен з цих аспектів має важливе значення для правильного кваліфікування діяння і ефективного розслідування [85, с. 94].

З цього приводу С. В. Чучко пропонує чітке розмежування обставин, що підлягають встановленню під час розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет. Ці обставини можна розглядати як різні аспекти, що допомагають виявити сутність злочину, а також визначити ключові фактори, що сприяють його вчиненню або впливають на кваліфікацію:

1) обставини, що стосуються події шахрайства, до яких відносяться:

Час та місце вчинення кримінального правопорушення, що допомагає визначити, коли і де відбувся факт шахрайства, а також може свідчити про зв'язок з іншими правопорушеннями;

Спосіб вчинення шахрайства, що може включати використання специфічних інтернет-платформ, фальшивих сайтів, маніпуляцій з платіжними системами тощо;

Засоби кримінального правопорушення, зокрема технічні засоби, які застосовувалися для введення потерпілих в оману, наприклад, підроблені веб-сторінки або фішингові техніки;

Сліди кримінального правопорушення, що можуть бути виявлені у цифрових даних (журнали транзакцій, електронні листи, записи на вебсайтах);

Предмет кримінального правопорушення (наприклад, неіснуючі товари, що продавалися через інтернет);

Обставини, що стосуються особи потерпілого та злочинця: У цьому випадку важливо встановити:

Ознаки суб'єкта кримінального правопорушення, включаючи фізичні характеристики (підозрюваного чи групу осіб), їх осудність та вік, що впливає на визначення кримінальної відповідальності;

Кількість злочинців, особливо в разі організованої групи, а також розподіл ролей серед учасників шахрайства;

2) причини правопорушення:

Наявність причинного зв'язку між діями винних і наслідками кримінального правопорушення. Наприклад, встановлення, чи дійсно шахрайські дії призвели до втрати коштів потерпілими;

Виявлення причин і умов, що сприяли вчиненню кримінального правоопрушення, зокрема технічних слабкостей інтернет-платформ, соціальних або економічних факторів, що полегшили вчинення шахрайства.

Заходи, що необхідно вжити для усунення цих умов і запобігання подібним правопорушенням у майбутньому (наприклад, посилення контролю за інтернет-торгівлею);

Вид і розмір шкоди, завданої кримінальним правопорушенням. Це включає не лише матеріальні збитки, але й потенційні моральні збитки для потерпілих.

Кваліфікуючі ознаки шкоди, що можуть бути підставою для підвищення чи зниження покарання.

Обставини, що обтяжують або пом'якшують покарання, наприклад, рецидив кримінального правопорушення чи обставини, що свідчать про каяття винного.

Обставини, що можуть виключати кримінальну відповідальність, як-от дії в межах правового виправдання чи наявність підстав для закриття провадження.

Обставини, що можуть вплинути на звільнення від кримінальної відповідальності (наприклад, визнання потерпілим) чи факти, що виключають вчинення іншого кримінального правопорушення [182, с. 108–109].

Це систематичне виокремлення обставин дозволяє слідчим та правоохоронцям зібрати та оцінити повний спектр даних, необхідних для ефективного розслідування та точного кваліфікування шахрайства в умовах використання цифрових технологій.

Т. В. Коршикова досліджує основні етапи досудового розслідування в кримінальному провадженні, пов’язаному з шахрайством, вчиненим з використанням електронно-обчислювальної техніки. Згрупування нею обставин, дозволяє правильно структурувати розслідування і зосередитися на ключових елементах: 1) обставини події кримінального правопорушення – це факти, які безпосередньо пов’язані з моментом і умовами вчинення шахрайства (наприклад, використання Інтернет-платформ для шахрайських схем); винуватість обвинуваченого – включає визначення форми вини (умисел чи необережність), мотивації та мети кримінального правопорушення, що допомагає сформулювати правильне обвинувачення; шкода, завдана правопорушенням – важливо зазначити вид і обсяг матеріальних втрат, що є критичними для визначення тяжкості кримінального правопорушення; характеристика особи підозрюваного – враховуються особисті дані, що можуть бути важливими для судового розгляду та визначення міри покарання; пом’якшення чи обтяження покарання – обставини, що можуть зменшити чи збільшити тяжкість покарання, наприклад, добровільне відшкодування шкоди або повторність злочинів; звільнення від кримінальної відповідальності – обставини, що можуть бути підставою для припинення кримінального провадження, як-от

закінчення терміну давності чи відсутність складу кримінального правопорушення; кримінально-правові заходи щодо юридичних осіб – застосування відповідних заходів до компаній, що стали співучасниками чи організаторами шахрайства [85, с. 96].

І. О. Коваленко пропонує детальний підхід до встановлення обставин у кримінальних провадженнях, пов'язаних з шахрайством у сфері використання банківських електронних платежів. До таких обставин науковець відносить: 1) обставини, що характеризують вчинення шахрайства: відомості про час і місце вчинення кримінального правопорушення, способи вчинення шахрайства, включаючи використання технічних засобів (наприклад, ботів, шкідливих програм), викрадених реквізитів карток, злом серверів або використання технічних прийомів для маніпуляцій з даними, засоби, які використовуються при вчиненні кримінального правопорушення, включаючи електронно-обчислювальну техніку, смартфони, програми для зламування даних, VPN, браузери тощо; 2) обставини, що стосуються характеристики осіб: визначення кількості правопорушників і їх ролі в вчиненні шахрайства, відомості про потерпілого, а також визначення їхньої причетності чи впливу на вчинення кримінального правопорушення; 3) причинно-наслідкові зв'язки: встановлення зв'язку між діями злочинців і результатами їхніх протиправних дій, з'ясування причин та умов, що сприяли вчиненню шахрайства (наприклад, слабкі місця в системах захисту або відсутність належного контролю); 4) обставини, що обтяжують або пом'якшують покарання: наявність підстав для закриття кримінального провадження або звільнення від відповідальності, визначення обставин, що можуть вплинути на тяжкість покарання, як-от спільна діяльність чи добровільне відшкодування шкоди; 6) кваліфікуючі ознаки: розмір і характер шкоди, завданої вчиненням шахрайства; 7) обставини, що вказують на кваліфікацію кримінального правопорушення, наприклад, його масштаб або повторність; 8) вид і розмір шкоди: оцінка матеріальних втрат, завданих шахрайськими діями в контексті

банківських електронних платежів, що може мати суттєве значення для визначення покарання та відповідальності [68, с. 107–108].

У відповідності до ст. 91 КПК України предмет доказування включає в себе обставини, що характеризують подію кримінального правопорушення, а також особисті обставини осіб, що беруть участь у кримінальному процесі. Однак варто підкреслити, що предмет доказування є більш широким, ніж просто елементи складу кримінального правопорушення, і охоплює всі фактори, що можуть мати значення для кримінального провадження. Саме тому розглянемо коло обставин, які підлягають доказуванню через призму кібершахрайств.

1. Подія кримінального правопорушення:

У ст. 91 КПК України зазначено, що предмет доказування охоплює подію кримінального правопорушення, що включає обставини, як-от час, місце, спосіб і інші обставини вчинення кримінального правопорушення. Зокрема, щодо шахрайства, це може стосуватися:

- Часу і місця, де було вчинено шахрайство (як у фізичному просторі, так і в кіберпросторі).
- Способу вчинення кримінального правопорушення, наприклад, через використання фішингових атак, вірусів, маніпуляцій з даними, зламування паролів тощо.
- Інших обставин, які можуть вплинути на кваліфікацію діяння (наприклад, використання спеціальних технічних засобів для обману чи знищення доказів).

2. Предмет доказування:

Хоча ст. 91 КПК України визначає обставини, що підлягають доказуванню, їх перелік є орієнтовним і не вичерпним. Це означає, що, залежно від конкретних обставин, можуть виникати інші важливі для кримінального провадження обставини, які потребують дослідження. Для кібершахрайств, наприклад, це можуть бути нові цифрові сліди, які залишаються в електронних платіжних системах, мережах чи в документах,

що зберігаються на сервері. Також, важливими є свідчення осіб, чиї акаунти були скомпрометовані або використані для проведення шахрайських операцій.

3. Особистісні якості осіб, що беруть участь у вчиненні кримінального правопорушення:

Врахування характеристик осіб, які вчинили шахрайство, є також важливим аспектом доказування у таких криміналдьних провадженнях. Наприклад, чи діяла особа в організованій групі, чи був у неї доступ до спеціалізованих знань або інструментів, які дозволяли їй здійснювати шахрайство. Також слід з'ясувати роль кожного учасника в схемі кримінального правопорушення, їх мотиви і мету. Важливо також розглядати особу потерпілого, оскільки його обізнаність в питаннях кібербезпеки, ступінь наївності чи інші особистісні характеристики можуть стати важливими в контексті встановлення певних обставин.

Слід зазначити, що перелік обставин є важливими елементами криміналістичної характеристики шахрайства, зокрема в контексті фінансових кримінальних правопорушень у банківській сфері. Зважаючи на поширеність таких кримінальних правопорушень, доцільно розглянути коло обставин, які необхідно встановити при їх розслідуванні:

1. Умови роботи підприємства, установи або організації та кредитно-фінансової установи: визначення організаційної структури установи, процедур і правил, що регулюють її діяльність, перевірка наявності внутрішніх політик та регламентів, пов'язаних з безпекою фінансових операцій, для оцінки слабких місць у захисті від шахрайства, оцінка рівня контролю за фінансовими операціями, а також наявність належних технологічних засобів захисту даних.

2. Коло службових прав і обов’язків осіб, що вчинили кримінальне правопорушення: встановлення, хто з працівників установи мав доступ до фінансових ресурсів, які були використані кримінально протиправним шляхом, аналіз посадових інструкцій та обов'язків особи, що вчинила

кримінальне правопорушення, для з’ясування можливості зловживання своїми повноваженнями.

3. Встановлення факту використання посадовою особою своїх службових повноважень всупереч інтересам служби: пошук доказів того, що особа використовувала свої службові повноваження в особистих чи корисливих цілях, зокрема для здійснення шахрайських операцій, виявлення можливих порушень внутрішніх політик організації або фінансових стандартів, що були використані для вчинення кримінального правопорушення.

4. Вчинення діяння з корисливої або іншої особистої зацікавленості: з'ясування, чи була мета кримінального правопорушення фінансова вигода або інші особисті інтереси (наприклад, політичні, бізнесові), дослідження мотивів посадових осіб, які могли спонукати їх на зловживання своїм службовим становищем.

5. Наявність причинового зв’язку між діями винного й наслідками, що настали: встановлення прямого зв’язку між діями особи (наприклад, надання неправдивої інформації, підробка документів) і результатами, що настали (збитки, фінансові втрати).

6. Встановлення факту заснування фіктивної фірми: виявлення фактів заснування фіктивних компаній або використання підставних осіб для проведення шахрайських фінансових операцій, аналіз документів, що підтверджують існування фірми, її зв’язки з іншими суб’єктами або фінансовими установами.

7. Обстановка вчинення кримінального правопорушення, зокрема встановлення місця і часу вчинення кримінального правопорушення, а також умов, що цьому сприяли (наприклад, уразливість певної банківської системи, несприятлива економічна ситуація, відсутність належного контролю).

8. Обставини, що характеризують особу обвинувачуваного: психологічний та соціальний портрет особи, яка вчинила кримінальне

правопорушення, дослідження мотиваційних факторів, які могли призвести до злочину.

9. Обставини, що сприяють вчиненню кримінального правопорушення: аналіз зовнішніх обставин, що могли сприяти скоєнню шахрайства, зокрема виявлення прогалин у правовому та технічному забезпеченні діяльності банку чи фінансової установи, оцінка слабкостей у внутрішньому контролі та системах безпеки.

10. Незаконність дій (бездіяльності) посадової особи: встановлення, у чому саме полягала бездіяльність посадових осіб (наприклад, не проведення належної перевірки фінансових транзакцій або неналежний контроль за обігом грошей), визначення, чи не було спеціальною бездіяльністю сприяння вчиненню кримінального правопорушення.

11. Час, місце й спосіб вчинення кримінально протиправних посягань: дослідження конкретних моментів, коли була вчинена бездіяльність або порушення (наприклад, під час переведення коштів, перевірки документів тощо), визначення методів і способів, які використовувала особа для ухилення від відповідальності.

12. Причиновий зв’язок між діями (бездіяльністю) і наслідками, що настали: з'ясування, чи існує прямий причинний зв’язок між діями або бездіяльністю особи та конкретними шкідливими наслідками (наприклад, фінансовими втратами для клієнтів чи установи).

13. Розмір збитку, заподіяного кримінально протиправними діями (бездіяльністю): оцінка фінансових втрат, завданих внаслідок шахрайства, та ступінь їх значущості для установи або постраждалих осіб, визначення економічних наслідків для організації, підприємства або банку, а також для всього фінансового сектору в цілому.

Збір і аналіз цих обставин є необхідними для розкриття і розслідування злочину, а також для формування обґрунтованих слідчих версій, що в свою чергу допомагає правильно кваліфікувати діяння особи та притягнути її до відповідальності.

Отже, з урахуванням вказаного підходу до розкриття кібершахрайств, можна виділити чотири основні групи обставин, які мають бути встановлені під час кримінального провадження. Це дозволить забезпечити комплексний підхід до розслідування та ефективно оцінювати всі аспекти кримінального провадження:

1. Обставини стосовно події кримінального правопорушення:

- Факт вчинення шахрайства в кіберпросторі: встановлення самого факту шахрайства, особливості його вчинення в цифровому середовищі.
- Час учинення шахрайства: тривалість та періодизація злочину, що допомагає визначити ключові моменти в схемі вчинення злочину.
- Просторові межі: визначення місця, де відбулося шахрайство, зокрема визначення джерела кібератак чи електронного втручання.
- Особа потерпілого: з'ясування даних про потерпілого для визначення шкоди та потенційних наслідків.
- Способи вчинення шахрайства: вивчення методів, через які здійснювався шахрайський вплив (наприклад, фішинг, соціальна інженерія, використання шкідливого ПЗ тощо).
- Предмет посягання: що саме стало об'єктом шахрайських дій (гроші, інформація, доступ до банківських рахунків тощо).
- Характер і розмір завданої шкоди: оцінка матеріальних і нематеріальних збитків для потерпілого, включаючи ймовірні майбутні наслідки.
- Джерела цифрових слідів: ідентифікація технічних слідів, які дозволяють відновити процес шахрайства (IP-адреси, логи серверів, інформація з браузерів тощо).

2. Інші обставини кримінального правопорушення:

2.1 Відомості про причинно-наслідковий зв’язок:

- Обставини, що сприяли вчиненню шахрайства: визначення факторів, які полегшили чи сприяли вчиненню кримінального

правопорушення, таких як слабкі місця в захисті інформаційних систем або соціальна вразливість потерпілого.

- Споріднені види кримінальних правопорушень: розгляд зв’язків з іншими злочинами, наприклад, використання електронних пристроїв або комп’ютерних мереж у інших правопорушеннях.
- Обставини посткримінальної діяльності: вивчення дій, що слідують після вчинення кримінального правопорушення, включаючи спроби приховати сліди, обертання коштів через інші платіжні системи, використання інтернет-майданчиків для відмивання грошей.

2.2 Відомості про свідків**:**

- Інформація про свідків, які можуть дати важливі свідчення для розкриття злочину, зокрема технічні фахівці, експерти з кібербезпеки чи користувачі, які стали жертвами шахрайства.

3. Обставини стосовно підозрюваного:

- Особа підозрюваного: з'ясування соціально-демографічних даних, психологічних характеристик, попередньої кримінальної історії.
- Винуватість, мотив і мета підозрюваного: встановлення того, чи є у підозрюваного намір скоєння шахрайства, що стало його мотивацією, а також які наслідки він прагнув досягти.
- Співучасть у вчиненні шахрайства: визначення ролі інших осіб, якщо шахрайство здійснювалося групою осіб, а також можливість участі у споріднених правопорушеннях.

4. Обставини, які можуть мати додаткове значення:

- Фактори, що впливають на тяжкість кримінального правопорушення: врахування обтяжуючих або пом'якшуючих обставин, таких як способи вчинення кримінального правопорушення або наявність добросовісного наміру.
- Підстави для закриття провадження чи звільнення від кримінальної відповідальності: визначення умов, що можуть призвести до

закінчення кримінального провадження, наприклад, через відсутність доказів, добровільне відшкодування шкоди чи амністію.

- Розмір процесуальних витрат: оцінка витрат, пов'язаних з проведенням розслідування та підтримкою судового процесу, що є важливим для визначення покарання або для оцінки ефективності роботи правоохоронних органів.

Цей комплексний підхід дозволяє не лише точно визначити обставини, що мають значення для розкриття кібершахрайств, але й ефективно відстежити технологічні аспекти злочину та забезпечити належне правове регулювання цього виду кримінальних правопорушень [26, с. 135-148].

Оцінка важливості встановлення обставин у процесі розслідування кібершахрайств є абсолютно обґрунтованою. Справді, точне визначення всіх релевантних обставин, таких як спосіб вчинення кримінального правопорушення, причини, що сприяли його вчиненню, та фактори, що можуть впливати на кваліфікацію діянь, є критично важливими для евективного і справедливого розслідування справи [92].

Отже, виходячи з вищесказаного, можемо зробити такі висновки. Оцінка слідчим первинної інформації — це перший крок, який безпосередньо визначає стратегічний напрямок всього розслідування. Оскільки йдеться про технологічно складні кримінальні правопорушення, ефективна оцінка повинна бути багаторівневою, з використанням специфічних технічних знань і навичок. Це включає в себе аналіз слідів, отриманих із цифрових пристроїв, перевірку даних про транзакції в системах електронних платежів, а також збір інформації від свідків чи потерпілих, які можуть бути недостатньо обізнані щодо технічних аспектів шахрайства.

Враховуючи швидкий розвиток технологій та зміну підходів до здійснення шахрайства в кіберпросторі, наукове осмислення обставин, які підлягають встановленню в рамках кримінального провадження, повинно включати новітні аспекти. Це включає в себе детальне вивчення нових типів кібератак (наприклад, шахрайства на основі штучного інтелекту), технологій,

які використовуються зловмисниками, а також нові види доказів, зокрема електронні сліди та цифрові відбитки.

При цьому важливе значення має вибір і застосування спеціалізованих інструментів для аналізу інформації, що буде визначати ефективність усіх подальших етапів розслідування. Це може включати в себе як інструменти для моніторингу мережевих активностей, так і спеціалізовані програмні засоби для відновлення видалених даних та аналізу цифрових доказів.

Теоретико-прикладні дослідження в цій сфері потребують уточнення і розвитку нових підходів до класифікації обставин, що можуть бути важливими для розкриття кібершахрайств. Це включає аналіз актуальних проблем, таких як дефініція нових видів цифрових злочинів, оцінка відповідних механізмів захисту прав потерпілих у кіберпросторі та інтеграція інноваційних технологій в процес розслідування. Отже, подальші наукові дослідження повинні зосереджуватися на вивченні змін, що відбуваються в сфері цифрових кримінальних правопорушень, а також на удосконаленні механізмів оцінки первинної інформації, що дозволяє органам правопорядку оперативно реагувати на нові загрози та забезпечувати належне правове реагування на кібершахрайства.

На основі проаналізованого початкового етапу та кола обставин, які підлягають доказуванню у кримінальних правопорушеннях, що вчиняються за допомогою цифрових технологій, можемо сформулювати важливі аспекти вдосконалення нормативного регулювання, які спрямовані на підвищення ефективності роботи слідчих та оперативних підрозділів у сфері доказування кібершахрайству.

1. Уніфікація окремих норм КПК України з розширенням спектру процесуальних дій до внесення відомостей до ЄРДР. Так, наразі КПК України забороняє проведення процесуальних дій до внесення відомостей до ЄРДР, що обмежує можливості ефективного реагування на первинну інформацію.Ця заборона ускладнює виявлення та фіксацію доказів, особливо

у випадках, коли швидка реакція є критично важливою (наприклад, збирання цифрових слідів).

З цією метою необхідно розширити перелік дозволених дій на етапі оцінки первинної інформації, наприклад:вилучення електронних даних для їх збереження, проведення консультацій із залученням експертів у сфері кібербезпеки; тимчасовий доступ до інформаційних систем для зупинення подальшого злочинного використання.

2. Консолідація норм КК України та нормативної бази з кібербезпеки. Так, Кримінальний кодекс України не враховує в повній мірі особливості кіберпростору і не синхронізований із нормативними актами про кібербезпеку. Тому відсутність єдиної термінології ускладнює розуміння і застосування норм.

Саме тому доцільно увести єдину термінологію, що відповідатиме міжнародним стандартам і практикам, наприклад, терміни «кіберзлочин», «електронні докази», «фішинг», «шахрайство у віртуальному середовищі» та узгодити норми КК із Законом України «Про основні засади забезпечення кібербезпеки України».

Запропоновані зміни сприятимуть спрощенню процесу оцінки первинної інформації та її обробки, усунуть правову невизначеність і покращать координацію між слідчими, оперативними підрозділами та іншими правоохоронними органами. Це дозволить адаптувати українське законодавство до сучасних реалій кіберзлочинності та забезпечити ефективний правозахист у кіберпросторі.

2.2. Джерела доказів у справах про шахрайство, вчинене з використанням цифрових технологій

Доказування у кримінальному процесі є ключовим аспектом, який забезпечує прийняття законних, обґрунтованих і справедливих процесуальних рішень. Допустимість доказів виступає однією з

найважливіших характеристик доказової бази, адже саме вона забезпечує дотримання прав і свобод учасників кримінального провадження, а також відповідність процесуальних дій вимогам закону.

Упродовж останніх років тематика доказування, зокрема його допустимості, отримала значну увагу у працях учених. В. М. Зінченко у праці «Достатність доказів у кримінальному провадженні» (2020) досліджується поняття та критерії достатності доказів. Автор акцентує увагу на зв'язку достатності з допустимістю доказів та їх значенням для прийняття кінцевих процесуальних рішень. Г. Р. Крет у монографії «Міжнародні стандарти доказування у кримінальному процесі України» (2020) аналізуються міжнародні підходи до доказування та їх адаптація у кримінальний процес України. Зокрема, автор наголошує на важливості дотримання міжнародних стандартів, що забезпечують справедливість і об'єктивність провадження. Б. В. Шабаровський у роботі «Перевірка доказів у кримінальному процесі України» (2019) розглядається процедура перевірки доказів, її вплив на їх допустимість і достовірність. Автор також звертає увагу на недоліки практичного застосування положень КПК України у цій сфері. Х. Р. Слюсарчук у праці «Стандарти доказування у кримінальному провадженні» (2017) аналізує різні підходи до стандартів доказування, включаючи міжнародну практику та вплив європейських стандартів на українське законодавство. А. С. Степаненко **у** монографії «Стандарт доказування «поза розумним сумнівом» у кримінальному провадженні» (2017) досліджується один із ключових стандартів доказування, який забезпечує об'єктивність судового розгляду та виносить вироки, що ґрунтуються на достатній доказовій базі. О. В. Литвин у праці «Кримінально-процесуальне доказування у стадії судового розгляду» (2016) аналізується специфіка доказування на етапі судового розгляду, включаючи процес оцінки допустимості та достовірності доказів судом. І. Л. Чупрікова **у** монографії «Допустимість доказів у світлі нового Кримінального процесуального кодексу» (2016) розкриваються зміни, внесені новим КПК, у сфері доказування. Особлива

увага приділяється питанням процесуального порядку збирання доказів і їх оцінки.

Попри значний розвиток теорії доказування, проблема цифрових доказів у кримінальному процесі залишається недостатньо врегульованою та дискусійною. Це пов'язано не лише із загальною новизною цього виду доказів, але й із низкою складних технічних та правових питань [109, с. 225]. Із такою тезою слід погодитися і зазначити, що розвиток цифрових технологій справді ускладнює процес збирання, фіксації та дослідження цифрових доказів. Це зумовлено, зокрема, специфікою їхньої природи, яка включає абстрактність, технічну складність і нестабільність даних. У цьому контексті особливої ваги набуває постійне вдосконалення професійної підготовки слідчих і прокурорів. Їм необхідно не лише опановувати сучасні методи збирання та обробки цифрових доказів, але й усвідомлювати важливість дотримання процесуальних вимог, що забезпечують допустимість таких доказів у суді. Лише за таких умов цифрові докази можуть бути ефективно використані для ефективного досудового розслідування.

Прийняття Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» від 15 березня 2022 року No 2137-IX стало важливим кроком у напрямку покращення нормативно-правового забезпечення використання електронних доказів у кримінальному процесі, зокрема для протидії кібератакам і розслідування кримінальних правопорушень «за гарячими слідами». Однак, незважаючи на внесені зміни, все ще існують проблеми, які потребують подальшого врегулювання [139] розглянути окремі з них та надати, як один з можливих, варіант їх вирішення.

Нині одним із недоліків чинного кримінального процесуального законодавства України є відсутність офіційного визначення поняття цифрових доказів. Ця проблема ускладнює їх застосування у кримінальних провадженнях, зокрема через відсутність уніфікованого підходу до таких доказів у практиці досудового розслідування та судового розгляду.

Інститут цифрових (електронних) доказів у кримінальному процесі України є важливим елементом сучасної правової системи, оскільки розвиток технологій та використання цифрових пристроїв значно змінили спосіб збору, зберігання та передачі доказів. Проблеми, що виникають у зв'язку з цифровими доказами, потребують уваги як з боку законодавців, так і з боку судових органів для забезпечення належної правової практики.

Проте у законодавстві, що регулює діяльність у інших сферах судочинства, це питання частково вирішено. Наприклад, у ч. 1 ст. 99 Кодексу адміністративного судочинства України (КАС України) зазначено, що електронними доказами можуть бути інформація в електронній формі, документи, файли, електронна переписка, відеозаписи, тощо [69]. Це положення закріплене у ч. 1 ст. 96 Господарського процесуального кодексу України [31] та ч. 1 ст. 100 Цивільного процесуального кодексу України [179].

Цифровими доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, які мають значення для справи. До них відносяться:

- Електронні документи (текстові файли, графічні зображення, плани, фотографії, відео- та аудіозаписи);
- Вебсайти (сторінки);
- Текстові, мультимедійні та голосові повідомлення**;**
- Метадані (дані про дані, які дозволяють встановити час створення, автора, пристрій тощо);
- Бази даних**;**
- Інші дані в електронній формі.

Ці види доказів є невід'ємною складовою сучасного судочинства, особливо у зв'язку зі стрімким розвитком цифрових технологій. Їх належне визначення та закріплення у кримінальному процесуальному законодавстві є необхідним кроком для підвищення ефективності досудового розслідування та судового розгляду.

Незважаючи на актуальність питання, чинний КПК України досі не містить офіційного визначення поняття «цифровий доказ». Така позиція є колізійною, враховуючи потребу в належному регулюванні збору, фіксації та оцінки таких доказів у сучасному кримінальному процесі.

Спроби законодавчого вирішення цієї проблеми вже здійснювались. Зокрема, у 2020 році було розроблено проєкт Закону про внесення змін до КПК України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів. У рамках цього проекту пропонувалося доповнити КПК визначенням поняття «електронний доказ», під яким розумілась: «інформація в електронній (цифровій) формі з відомостями, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [138]. Ця ініціатива мала на меті вдосконалити процесуальні аспекти використання цифрових доказів у кримінальному провадженні. Однак на момент поточної оцінки відповідні зміни так і не були внесені до законодавства, що створює прогалини в регулюванні даного питання.

Погоджуючись із зауваженням науковців, можна відзначити, що дійсно, в наданих визначеннях електронних доказів існує певний логічний недолік. Протиставлення понять «інформація», «дані» та «відомості» виглядає надмірним, оскільки в загальнонауковому контексті ці терміни часто використовуються як синоніми.

Згідно з класичним підходом, доказ — це інформація, яка має значення для розслідування кримінального правопорушення, і є об'єктивним засобом для встановлення істини у справі. Виходячи з цього, доповнення терміну «інформація» такими словами, як «дані» або «відомості», створює дублювання та введення в текст надмірних термінів, що може призводити до логічних неточностей.

Інформація, по суті, є синонімом даних, і в контексті доказів це не просто набір окремих відомостей, а систематизовані і організовані дані, які мають практичну цінність для розслідування чи судового процесу. Тому,

науковці правильно зазначають, що електронний доказ слід визначати просто як інформацію в електронній формі, оскільки це буде більш точним і логічним підходом, не завдаючи надмірних труднощів в інтерпретації поняття.

Таке визначення дозволяє чітко відокремити електронні докази від інших видів доказів, що можуть бути представлені в різних форматах, не зважаючи на застосування слів, які вже містять усю необхідну сутність [174, с. 99].

Проте в науці існують інші погляди на це поняття. Науковці розглядають цифрові (електронні) докази як інформацію в електронній формі, що створена, збережена або передана за допомогою електронних засобів і технологій, та має значення для встановлення обставин у кримінальному провадженні. Вони акцентують на специфіці технічної природи таких доказів, яка зумовлює їхній особливий процес збирання, обробки та збереження. Зокрема, підходи Д. М. Цехана, І. Г. Каланчі та А. В. Столітнього — мають свої переваги і недоліки.

Д. М. Цехан акцентує увагу на матеріальному носії, підкреслюючи важливість збереження цілісності даних у процесі їх вилучення і транспортування. Однак обмеження до «дискретної (цифрової) форми» може бути занадто вузьким, враховуючи розвиток технологій, наприклад, хмарних систем зберігання даних, які не мають фізичного носія у традиційному розумінні [177, с. 257].

Підхід І. Г. Каланчі та А. В. Столітнього охоплює ширший спектр джерел, визнаючи специфіку створення, передачі й зберігання електронної інформації. Цей підхід є ближчим до сучасної практики, але недостатньо враховує технічні аспекти, такі як необхідність забезпечення автентичності та цілісності даних [55].

Обидва підходи підтверджують, що цифрові докази мають бути доступними для сприйняття після відповідної обробки. Проте розбіжності у визначеннях свідчать про потребу уніфікації термінології для забезпечення

єдності правозастосування/ На практиці найбільш доцільним є комплексний підхід, який враховуватиме і технічну природу цифрових доказів, і їхній змістовний аспект як інформації, що має значення для справи.

В. М. Фігурський зазначає, що цифрові (електронні) докази визначаються як інформація, створена, оброблена, збережена або передана за допомогою аналогових чи цифрових сигналів, що має значення для кримінального провадження [174, с. 99]. Така позиція чітко відображає функціональну природу таких доказів та їхню релевантність до кримінального процесу.

Проте одночасна вказівка на електронний характер інформації та її знаходження на електронному носії є надлишковою. Як зазначають фахівці, це створює логічну суперечність та дублювання понять. Якщо інформація розміщена на електронному носії, це автоматично передбачає її електронний характер. Таке уточнення не додає суттєвих характеристик до дефініції, а лише перевантажує її структурно.

Для уникнення подібних логічних помилок важливо уникати дублювань у визначенні. Наприклад, «Цифровий (електронний) доказ — це інформація, створена, оброблена, збережена або передана за допомогою електронних засобів, яка має значення для кримінального провадження». Таке визначення є більш лаконічним і водночас охоплює всі ключові аспекти цифрових доказів, залишаючи простір для уточнення технічних характеристик у підзаконних актах або спеціальних методичних рекомендаціях.

Таким чином, можна сформулювати основні ознаки цифрових доказів, які дозволяють виокремити їх як специфічну категорію доказів у кримінальному процесі:

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, такими як можливість відновлення, копіювання без зміни первісного змісту, наявність метаданих та залежність від певних програмних і апаратних засобів для доступу.

На підставі аналізу можна запропонувати наступне визначення цифрових (електронних) доказів:

Цифровий (електронний) доказ — це інформація у цифровій формі, 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.

Практична значущість цифрових (електронних) доказів у кримінальному провадженні багато в чому визначається їх відповідністю критеріям допустимості, закріпленим у КПК України. Ці критерії забезпечують правомірність використання отриманих даних у процесі доказування. До них відносяться:

1. Належне джерело отримання доказів. Докази мають бути отримані із законного джерела, передбаченого КПК України. Для цифрових доказів це може бути сервер, комп’ютер, телефон, інші електронні пристрої чи носії, вебресурси, бази даних тощо. Використання неналежних джерел, наприклад, злому електронного пристрою без дозволу суду, може призвести до визнання доказів недопустимими.

2. Належний суб’єкт. Отримання цифрових доказів повинно здійснюватися уповноваженими суб’єктами, такими як слідчий, прокурор,

уповноважені органи. Дії сторонніх осіб, які не мають відповідних процесуальних повноважень, можуть поставити під сумнів легітимність доказів.

3. Належний спосіб збирання доказів**.** Процедури отримання цифрових доказів мають відповідати вимогам КПК України та не порушувати права людини. Наприклад, зняття інформації з електронного носія або серверу повинно проводитися за наявності ухвали слідчого судді та із дотриманням процесуальних норм щодо фіксації таких дій [34, с. 75–89].

Для слідчого, прокурора та інших учасників процесу ці критерії створюють правову основу, яка дозволяє визначити, чи можуть цифрові (електронні) дані використовуватись у процесі доказування. Неправильне застосування цих критеріїв або їх ігнорування призводить до визнання доказів недопустимими, навіть якщо вони підтверджують обставини, що мають значення для справи. У кримінальному процесі питання належного джерела отримання доказів є фундаментальним, оскільки саме від визначення такого джерела залежить правомірність використання доказів у судовому провадженні. КПК України встановлює перелік процесуальних джерел доказів, серед яких: показання (свідків, потерпілих, обвинувачених тощо), речові докази (об'єкти матеріального світу, які мають значення для справи), документи (записи, акти, звіти, електронні файли тощо), висновки експертів (результати спеціальних досліджень).

У науковій літературі сформувалося три основні підходи до вирішення проблеми визначення належного джерела отримання доказів, зокрема стосовно цифрових (електронних) доказів:

1. Традиційний підхід:

Цей підхід полягає в тому, що джерела цифрових (електронних) доказів мають чітко відповідати категоріям, визначеним у ст. 84 КПК України [9, с. 14]. Наприклад:

- Електронна пошта, текстові повідомлення, аудіо- чи відеофайли можуть розглядатися як документи.

- Метадані чи технічні характеристики пристроїв як складова речових доказів.

2. Розширений підхід:

Прихильники цього підходу вважають, що цифрові докази повинні бути визнані самостійною категорією процесуальних джерел доказів. Вони аргументують це специфікою цифрової інформації, яка може бути динамічною (змінюваною в реальному часі) та існує у віртуальному середовищі (наприклад, у хмарних сховищах або на вебсайтах). Науковці пропонують внести зміни до КПК України, аби адаптувати його до сучасних реалій [55, с. 186–188].

3. Інтегративний підхід:

Цей підхід намагається поєднати традиційний і розширений підходи. Згідно з ним, цифрові докази залишаються частиною визначених ст. 84 КПК джерел, але законодавець має надати роз’яснення або додаткові критерії щодо їхнього віднесення до певної категорії. Наприклад:

- Електронний файл може бути документом, але його зміст потребує оцінки через експертний висновок.
- Сервер або інший носій можуть бути джерелом речових доказів, якщо вони фізично вилучені [70, с. 420].

Таким чином, сучасна практика боротьби зі злочинністю в Україні має керуватися чинними положеннями кримінального процесуального законодавства. У межах такого підходу цифрові докази формально трактуються як різновид документів, зокрема, як електронного документа, що регулюється відповідними законодавчими актами, включаючи КПК України та Закон України «Про електронні документи та електронний документообіг».

Стаття 99 КПК України визначає поняття «документ» як джерело доказу та встановлює вимоги до нього у кримінальному провадженні. У її положеннях під документом розуміється матеріальний об’єкт, спеціально створений для збереження інформації, який містить зафіксовані за

допомогою письмових знаків, звуку, зображення тощо відомості, що можуть бути використані як докази фактів чи обставин, які встановлюються під час кримінального провадження.

Основними характеристиками документа як джерела доказу є:

1. Документ повинен бути матеріальним об’єктом, створеним із метою збереження інформації.

2. Інформація має бути зафіксована у формі письмових знаків, звуку, зображення або іншими засобами.

3. Документ може бути доказом, якщо містить відомості, які мають значення для встановлення фактів чи обставин у кримінальному провадженні.

Хоча ст. 99 КПК України прямо не визначає поняття цифрового доказу, включення електронних носіїв інформації до переліку джерел доказів відкриває можливість їх використання у кримінальному процесі. Це підтверджує гнучкість законодавства, яке може адаптуватися до викликів цифрової епохи.

Питання визначення джерела цифрових доказів у контексті чинного КПК України є предметом дискусій у наукових колах. Деякі дослідники вважають, що такі докази слід відносити до однієї з двох категорій, передбачених ст. 84 КПК України: документів або речових доказів. Для розмежування електронного документа та речового доказу в електронній формі пропонується аналізувати, що саме використовується як доказ: інформація — коли матеріальний об’єкт використовується виключно як носій, доказом вважається інформація, що зафіксована на ньому; матеріальний об’єкт — коли доказове значення має саме фізична форма об’єкта, а не інформація, яку він містить (наприклад, пошкоджений пристрій) [34, с. 83].

Цифрові докази мають розглядатися через призму інформації, яку вони містять, незалежно від носія:

Якщо електронний носій містить інформацію, що має значення для кримінального провадження, його слід кваліфікувати як документ у контексті ст. 99 КПК України. У випадках, коли сам носій (наприклад, пошкоджений пристрій) має значення для встановлення обставин, його можна розглядати як речовий доказ**.**

Ця позиція підкреслює, що доказова сутність завжди полягає в інформації. Матеріальний носій лише забезпечує фізичний доступ до цієї інформації. Таким чином, для правильного застосування поняття цифрових доказів у кримінальному провадженні важливо враховувати їхню інформаційну природу, що відповідає концепції доказів, закріпленій у чинному законодавстві.

Отже, точне визначення джерела цифрового доказу має ключове значення для забезпечення правомірності та ефективності кримінального провадження. Це дозволяє:

1) Обрати правильні процесуальні засоби і процедури. Відповідність дій щодо фіксації, вилучення та збереження доказів правилам, визначеним КПК України, є необхідною умовою для визнання доказів допустимими.

2) Забезпечити збереження інформації. Фіксація і вилучення доказів повинні проводитися таким чином, щоб уникнути їхньої модифікації, втрати або пошкодження. Це особливо важливо у випадках із цифровими доказами, де навіть незначна зміна може призвести до втрати їхньої доказової цінності.

3) Гарантувати належний рівень компетенції. Залучення спеціалістів у сфері інформаційних технологій і кібербезпеки під час роботи із цифровими доказами дозволяє виконати всі процесуальні дії у відповідності до стандартів. Це також допомагає уникнути процесуальних помилок, які можуть стати підставою для оскарження доказів у суді

Окрім цього, збирати цифрові докази повинен належний суб’єкт. Відповідно до положень КПК України, такими суб’єктами є уповноважені учасники кримінального провадження, зокрема:

Слідчий або дізнавач. Відповідно до ч. 1 ст. 214 КПК України, слідчий або дізнавач, призначений керівником органу досудового розслідування, є правомочним здійснювати кримінальне провадження або виконувати окремі процесуальні дії.

Якщо слідчий отримує інформацію про кримінальне правопорушення, який не входить до його компетенції (підслідності), він все одно зобов'язаний розпочати досудове розслідування. Відповідно до ч. 2 ст. 218 КПК України, у такому разі слідчий або дізнавач залишається належним суб'єктом до моменту визначення підслідності прокурором. Це забезпечує оперативність реагування на кримінальні правопорушення.

Значення належності суб'єкта для цифрових доказів:

1. Докази, зібрані неналежним суб'єктом, можуть бути визнані недопустимими в судовому процесі.

2. Тільки уповноважений суб'єкт може проводити процесуальні дії, пов'язані зі збиранням доказів, що забезпечує дотримання прав підозрюваних і потерпілих.

3. Слідчі та дізнавачі мають відповідну кваліфікацію та доступ до технічних засобів, необхідних для коректної фіксації цифрових доказів.

Слід зазначити, що під час збирання цифрових доказів уповноважені суб'єкти можуть залучати інших спеціалістів, зокрема експертів з цифрової криміналістики, працівників кіберполіції, технічних фахівців для вилучення даних із складних носіїв або хмарних сервісів. Дотримання вимоги про належного суб'єкта збирання цифрових доказів є необхідною умовою для забезпечення доказової сили таких матеріалів у судовому розгляді. Це допомагає уникнути процедурних помилок, які можуть бути підставою для визнання доказів недопустимими.

Розслідування кримінальних правопорушень, пов'язаних із використанням цифрових технологій, має свої особливості, зокрема в аспекті визначення місця вчинення кримінального правопорушення і територіальної підслідності.

У більшості випадків місцем вчинення таких правопорушень спочатку вважається місце реєстрації або проживання потерпілого. Це зумовлено тим, що саме в цій локації зазвичай фіксуються перші сліди кримінального правопорушення, наприклад:

- факт обману в разі шахрайства (отримання недостовірної інформації);
- доступ до банківських рахунків або персональних даних;
- виявлення збитків, пов’язаних із кіберзлочинністю [86].

Однак це визначення є попереднім, і подальше розслідування може уточнити фактичне місце вчинення кримінального правопорушення.

Коли слідчий встановлює місце перебування підозрюваного або пристрою, з якого здійснено кримінальне правопорушення (наприклад, за допомогою аналізу IP-адреси), виникає потреба в передачі кримінального провадження до іншого органу досудового розслідування. Відповідно до ст. 218 КПК України, це питання вирішується прокурором.

Якщо під час розслідування шахрайства було встановлено, що злочинець використовував IP-адресу, зареєстровану в іншому регіоні, після ідентифікації пристрою та встановлення особи підозрюваного матеріали провадження можуть бути передані за місцем фактичного вчинення злочину або проживання підозрюваного.

При вирішенні питань підслідності у межах досудового розслідування надзвичайно важливо враховувати регламентовану процедуру дій слідчого відповідно до положень ст. 218 КПК України.

Слідчий протягом п’яти днів з моменту отримання інформації, яка свідчить про невідповідність підслідності, зобов’язаний письмово повідомити прокурора. До моменту, поки прокурор офіційно не визначить іншу підслідність, слідчий продовжує здійснювати досудове розслідування.

Законодавство та практика визначають кілька категорій осіб, які можуть бути уповноваженими на здійснення окремих процесуальних дій:

Слідчий (дізнавач), якому доручено окремі процесуальні дії**.** Згідно з ч. 6 ст. 218 КПК України, це можливо за постановою слідчого іншого органу досудового розслідування іншої територіальної юрисдикції або за вказівкою прокурора.

Члени слідчої чи спільної слідчої групи: члени слідчої групи, сформованої в межах п. 1 ч. 2 та ч. 4 ст. 39 КПК України та чени спільної слідчої групи (ст. 571 КПК України), яка може бути створена для розслідування злочинів міжнародного характеру чи інших складних випадків, що вимагають міждержавної співпраці.

Слідчий, який на момент проведення дій виконував свої обов'язки. Це включає осіб, які на час виконання конкретних процесуальних дій перебували на посаді, виконували трудові обов'язки та не перебували у відпустці чи на лікарняному [90].

До переліку уповноважених суб'єктів, які можуть здійснювати процесуальні дії, слід додати прокурора (процесуального керівника у кримінальному провадженні) відповідно до п. 4 ч. 2 ст. 36 КПК України, прокурор має право самостійно здійснювати окремі процесуальні дії та оперативного працівника, який може діяти за дорученням слідчого (дізнавача) або прокурора згідно з частинами 2 і 3 ст. 41 КПК України.

Проте на практиці виникають проблеми. Клопотання про тимчасовий доступ до речей і документів (ст. 160 КПК України) можуть подавати лише визначені сторони кримінального провадження. У разі подання клопотання неналежним суб'єктом, наприклад, оперуповноваженим, слідчий суддя має підстави для відмови в його задоволенні. Якщо клопотання подається іншим слідчим у межах кримінального провадження, до нього має бути додано постанову про призначення нового слідчого. У разі роботи групи слідчих, необхідно додати постанову про призначення групи слідчих для підтвердження правомірності підписання клопотання одним із них. Це ж стосується і прокурора, який погоджує клопотання або подає його самостійно. Якщо клопотання подається оперативним працівником, який не є

учасником кримінального провадження, це суперечить вимогам закону. Наслідком такого порушення є відмова слідчого судді в задоволенні клопотання**.**

Законодавець чітко визначив коло осіб, які мають право подавати клопотання, зокрема, про тимчасовий доступ до речей і документів. Важливо, щоб клопотання подавалося саме тим слідчим або прокурором, які здійснюють досудове розслідування або є процесуальними керівниками в конкретному кримінальному провадженні [172].

Належний спосіб збирання цифрових (електронних) доказів є ключовим аспектом кримінального процесу, оскільки від правильності їх отримання і обробки залежить допустимість таких доказів у суді. Це стосується не лише фізичних, але й електронних доказів, які мають свою специфіку.

Згідно зі ст. 93 КПК України, існують такі законні способи збирання доказів стороною обвинувачення:

1. Надання доказів добровільно учасником кримінального провадження. Це ситуація, коли особа, що має докази, надає їх без примусу. Такі докази є добровільними, але також повинні бути оглянуті та належним чином зафіксовані.

2. Витребування доказів. Витребування доказів здійснюється через звернення до компетентних органів або осіб, які володіють відповідними документами чи іншими доказами. Це може включати запити до банків, інтернет-платформ або інших установ, що володіють електронною інформацією.

3. Проведення слідчих (розшукових) дій. Зокрема, до таких дій належать: огляд — це процедура, коли слідчий або дізнавач безпосередньо перевіряють предмети або інформаційні носії (наприклад, комп'ютери, флеш-накопичувачі), що можуть містити важливі для справи електронні докази; обшук — при проведенні обшуку в осіб або на об'єктах, що можуть містити електронні докази, зокрема комп'ютерні пристрої, сервери, телефони.

4. Проведення негласних слідчих (розшукових) дій. Це включає використання технічних засобів для збору доказів без знання осіб, яких це стосується. До таких дій належать, наприклад, прослуховування телефонних розмов або доступ до електронної пошти чи інших онлайн-ресурсів. Важливо, щоб ці дії проводились із дотриманням законних процедур і на підставі дозволу суду.

Після отримання електронного документа на носії інформації, слідчий або дізнавач зобов'язані оглянути його. Це включає перевірку вмісту файлів, а також зафіксування всіх процесуальних дій, що здійснюються під час огляду, і обов'язкову фіксацію результатів огляду в протоколі. Огляд носіїв інформації, таких як комп'ютери, мобільні телефони, жорсткі диски, має бути проведений з особливою увагою, оскільки навіть незначні помилки у процедурі збору доказів можуть призвести до їх недопустимості.

Під час збирання цифрових доказів слідчий має дотримуватися процедур, що гарантують цілісність та незмінність даних. Це досягається за допомогою таких заходів, як створення резервних копій даних (зокрема, образів дисків) і використання криптографічних засобів для фіксації часу збирання доказів.

Для забезпечення допустимості цифрових доказів у суді необхідно вжити заходів для їх збереження від змін чи пошкоджень. Зберігання цифрових доказів повинно здійснюватися на спеціальних носіях з обмеженим доступом, зокрема в цифровому вигляді у вигляді файлів, за допомогою яких можна здійснити перевірку їх оригінальності.

Згідно з кримінальним процесуальним законодавством, сторона захисту, потерпілий та їх представники мають певні права щодо збирання електронних доказів, однак ці права мають обмеження і умови, які відрізняються від прав сторони обвинувачення.

Сторона захисту, потерпілий і їх представники можуть отримувати або витребувати цифрові документи від різних органів, установ і осіб, таких як органи державної влади, органи місцевого самоврядування, підприємства,

установи, організації, службові та фізичні особи. Це дозволяє їм отримувати документи, які можуть бути важливими для їхньої оборони або визначення обставин кримінального правопорушення. Наприклад, сторона захисту може витребувати цифрові документи, які підтверджують невинність підзахисного. Потерпілий може запросити електронні документи, що підтверджують збитки або факти, які мають значення для справи [183, с. 63].

Однак сторона захисту, потерпілий та їх представники не можуть самостійно проводити слідчі (розшукові) дії. Вони можуть тільки ініціювати проведення таких дій через подачу відповідного клопотання. Це клопотання може стосуватися проведення таких дій, як огляд документів, обшук чи виїмка інформації з носіїв даних та проведення негласних слідчих дій, таких як прослуховування або отримання доступу до електронних комунікацій. Однак, якщо клопотання про проведення цих дій задовольняється, ініціатором процесуальних дій не буде сторона захисту чи потерпілий, а суб'єктами, що безпосередньо виконують ці дії, є слідчий, дізнавач або прокурор [91].

Сторона захисту може ініціювати отримання доказів або слідчі дії, якщо це є важливим для захисту підзахисного. Проте, якщо органи розслідування не задовольняють клопотання захисту, вони можуть звертатися до суду для отримання дозволу на відповідні дії. Потерпілий також може ініціювати слідчі (розшукові) дії для збору доказів на свою користь, зокрема витребувати документи або інші цифрові докази, що можуть підтвердити його заяви про збитки чи обставини кримінального правопорушення.

Хоча сторони захисту та потерпілий мають право ініціювати деякі процесуальні дії, на відміну від сторони обвинувачення, вони не можуть безпосередньо збирати докази, проводити обшуки, або негласні слідчі (розшукові) дії. Це може здійснюватися тільки під контролем або за участю органів досудового розслідування чи прокуратури. Таким чином, основна роль сторони захисту та потерпілого полягає в ініціюванні процесуальних

дій, тоді як фактичне збирання доказів, у тому числі цифрових, здійснюється органами, що здійснюють кримінальне провадження, зокрема слідчими, дізнавачами або прокурорами.

У кримінальному провадженні, де є потреба в збиранні цифрових доказів, важливо дотримуватись чіткої процедури, визначеної КПК України. Особливо це стосується таких процесуальних засобів, як витребування та отримання доказів від органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, а також тимчасового доступу до речей і документів. Зазначені дії є необхідними для забезпечення допустимості доказів у кримінальному провадженні, однак їх неналежне виконання може призвести до відмови в їх прийнятті або визнанні недопустимими.

Витребування електронних документів чи іншої інформації від фізичних і юридичних осіб є важливою частиною кримінального процесу. Водночас, відповідно до ч. 2 ст. 93 КПК України, слідчий або прокурор, звертаючись до суду з клопотанням про тимчасовий доступ до документів чи речей, має зазначити, що ці документи або речі знаходяться або можуть знаходитися у володінні фізичних чи юридичних осіб.

Однак, на практиці іноді виникають випадки, коли слідчі не виконують ці вимоги належним чином. Вони можуть подати клопотання, в якому не доводять наявність документів чи речей у володінні певних осіб або організацій. Таке порушення процесуальних вимог може призвести до недопустимості доказів, що збираються.

Важливим є порядок звернення до суду з клопотанням про тимчасовий доступ до документів чи речей. Згідно з чинним законодавством, клопотання має містити конкретну інформацію про документи або речі, до яких планується доступ. У разі недотримання цієї вимоги клопотання може бути відхилене, а відповідно й зібрані докази можуть бути визнані недопустимими [91].

Якщо слідчий або прокурор не доводить суду, що речі або документи, до яких вимагається доступ, знаходяться у володінні конкретної фізичної чи юридичної особи, суд має право відмовити у задоволенні клопотання. Це є важливою гарантією того, що права та інтереси учасників кримінального процесу будуть належним чином захищені.

Клопотання про тимчасовий доступ до цифрових доказів, таких як електронні документи, записи на носіях інформації, також потребує суворого дотримання вимог законодавства. У випадку, коли слідчий не надає достатньо доказів про володіння відповідними доказами у конкретних осіб, суд може визнати такі клопотання непідтвердженими і відмовити в їх задоволенні. Це підкреслює важливість правильної підготовки та обґрунтування кожного клопотання щодо збирання доказів [46].

Судова практика показує, що у деяких випадках слідчі не забезпечують необхідний рівень обґрунтування своїх клопотань. Такі помилки можуть призвести до відмови в задоволенні клопотань, а відповідно — до невикористання зібраних доказів. Наприклад, слідчі іноді не надають достатніх доводів щодо того, що запитувані документи чи речі дійсно знаходяться у володінні конкретної особи, що є необхідною умовою для того, щоб доступ до них був наданий. Таким чином, процес збирання електронних доказів є вкрай чутливим до процедурних помилок, і кожен етап, від подачі клопотання до отримання доказів, має бути чітко відповідно до вимог КПК України. Недотримання цих вимог може призвести до відмови в задоволенні клопотання і, як наслідок, до втрати важливих доказів для розслідування [46].

Інформація, яка є предметом охорони за ст. 162 КПК України, є дуже важливою при розслідуванні різних кримінальних правопорушень, зокрема шахрайства, вчиненого із використанням цифрових технологій. Такі дані можуть включати не лише зв'язки між абонентами, але й деталі про маршрути передавання повідомлень або операцій, які можуть бути використані для ідентифікації підозрюваних осіб.

Оскільки ці дані можуть містити особисту та конфіденційну інформацію, слідчі та прокурори повинні дотримуватися чіткої законної процедури при отриманні доступу до таких відомостей. Наприклад, вони мають отримати судовий дозвіл на доступ до банківської таємниці чи інформації від телекомунікаційних операторів, підтвердивши, що ці відомості можуть бути необхідними для розслідування та доведення злочину.

Невиконання вимог ст. 93 КПК України, яка регулює порядок отримання документів та речей, може призвести до того, що зібрані дані не будуть визнані допустимими в суді, що, у свою чергу, ускладнює процес доведення злочину. Це підкреслює важливість дотримання всіх процесуальних норм при роботі з цифровими доказами, особливо коли йдеться про конфіденційну інформацію, що може мати великий вплив на результат кримінального провадження.

Як свідчить судова практика, одним із найбільш поширених порушень при поданні клопотань про тимчасовий доступ до речей і документів, що містять охоронювану законом таємницю (наприклад, банківську чи інформацію про зв’язок абонента), є недостатнє або неповне обґрунтування слідчим неможливості отримати ці докази іншими способами. Це порушення є важливим, оскільки ч. 6 ст. 163 КПК України вимагає від слідчого чи прокурора надати суду аргументацію, що існуючі способи збору доказів не можуть бути використані для доведення конкретних обставин справи.

Згідно з цією нормою, при поданні клопотання про тимчасовий доступ до речей та документів, що містять охоронювану законом таємницю, слідчий повинен довести неможливість іншими способами отримати ті самі докази. Якщо це обґрунтування відсутнє або є непереконливим, суд може відмовити в задоволенні клопотання.

Наприклад, у випадках, коли слідчий звертається до суду за дозволом на доступ до банківських рахунків або телефонних розмов, він повинен чітко продемонструвати, чому інші джерела доказів або методи збору інформації (як-от допити свідків чи використання іншої документації) не можуть дати

відповідь на питання, що розслідуються. Якщо ж такого обґрунтування не надається, суд може визнати зібрані таким чином докази недопустимими.

Судова практика показує, що навіть за наявності в слідчого формальних підстав для клопотання, без належного обґрунтування відсутності інших способів отримання доказів, суди часто відмовляють у задоволенні таких клопотань. Це підкреслює важливість ретельного дотримання вимог КПК України та обґрунтування всіх етапів процесу отримання доказів [172].

Отже, складність вирішення проблеми допустимості цифрових доказів у кримінальному процесі обумовлена їх специфічною технічною природою, що створює ряд унікальних викликів для правозастосовчої практики [153, с. 140-150].

Для підвищення ефективності використання цифрових доказів у кримінальному процесі необхідно удосконалити процедури збору і фіксації таких доказів. Законодавець повинен чітко регламентувати порядок збору, верифікації, збереження та передачі електронних доказів. Важливо також запровадити єдиний стандарт процесуального оформлення електронних доказів, який би включав обов'язкову перевірку їх автентичності через спеціалізовані технічні засоби (наприклад, алгоритми хешування).

Як ми уже зазначали, на сьогодні КПК України не містить чітких положень щодо джерел отримання електронних доказів, а також відсутнє визначення поняття цифрових доказів у контексті доказування кримінальних правопорушень. Це призводить до певних складнощів і невизначеностей при їх використанні в кримінальному процесі.

Незважаючи на відсутність прямого нормативного визначення, практика, зокрема судова, дозволяє формулювати певні правила щодо джерел отримання цифрових доказів і їх допустимості. Суди визначають допустимість цифрових доказів на основі загальних принципів допустимості доказів у кримінальному процесі, враховуючи такі фактори, як:

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 [135];

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 і здійснюється на визначених об'єктах, що не суперечить нормам законодавства щодо необхідності отримання 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 [150].

Незважаючи на ці практичні приклади, відсутність чіткої регламентації джерел отримання цифрових доказів у КПК спричиняє правову невизначеність і може призвести до неоднозначних рішень у судовій практиці. Це створює необхідність у подальшому вдосконаленні законодавства, включаючи:

- Чітке визначення поняття цифрових доказів, зокрема, що саме може вважатися цифровим доказом (записи телефонних розмов, відеозаписи, дані з електронних пристроїв тощо).
- Встановлення конкретних норм щодо джерел отримання цифрових доказів, що дозволить уникнути порушень прав осіб і забезпечить прозорість у процесі збору доказів.
- Розробка детальних правил для автентифікації і захисту цифрових доказів від маніпуляцій, що є критично важливим у разі їх використання в судовому процесі.

Законодавче визначення джерел отримання цифрових доказів та чіткі критерії їхньої допустимості допоможуть забезпечити більшу правову визначеність і ефективність кримінальних проваджень, зокрема в боротьбі з кіберзлочинністю.

На нашу думку, доцільно внести статтю до КПК України, визначити джерела цифрових доказів. Вони охоплюють як офіційно надані цифрові документи, так і докази, отримані через застосування технічних засобів та заходів розслідування. До них слід віднести:

1. Цифрові документи та інші електронні докази — надання таких доказів офіційними установами або через доступ до інформації на сервері дозволяє забезпечити легітимність їх використання.

2. Записи автономних систем — відображення таких доказів, як записи з камер відеоспостереження чи реєстраторів, є важливим для фіксації подій, що мають юридичне значення, і зниження ризику маніпуляцій з такими доказами.

3. Цифрові докази, отримані через слідчі (розшукові) дії або негласні слідчі (розшукові) дії — цей пункт є важливим для забезпечення ефективного збору доказів під час розслідування, зокрема при використанні технічних засобів для збору інформації, що мають великий доказовий потенціал.

4. Цифрові докази, отримані через заходи забезпечення або запобіжні заходи — включення цього пункту дозволяє врахувати ситуації, коли цифрові докази стають доступними внаслідок застосування судових або слідчих рішень, що забезпечують збереження даних до моменту їх дослідження.

5. Цифрові докази, отримані за допомогою технічних засобів (фото-, кінозйомка, відеозапис) — цей пункт охоплює сучасні технології, які використовуються для фіксації та зберігання доказів, що мають ключове значення для розслідування, і не потребують додаткових затверджень, якщо

їх отримання відбувається відповідно до вимог закону (ст. 245-1 КПК України).

6. Цифрові докази, отримані в результаті тимчасового вилучення майна (ст. 168 КПК України) — такий пункт важливий для визначення правил обробки даних, які можуть бути вилучені під час тимчасового доступу до електронних пристроїв.

Запропоновані пункти щодо джерел цифрових доказів охоплюють широкий спектр джерел, включаючи 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 дозволить забезпечити більш ефективний і оперативний процес збору доказів, зокрема в умовах розвитку інформаційних технологій і зростання кіберзлочинності.

Додавання цієї статті до Кримінального процесуального кодексу України, зокрема в контексті змін, які відбулися після ухвалення Закону України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування», може стати важливим кроком у вдосконаленні правового поля та підвищенні ефективності кримінальних проваджень. Таку пропозицію підтримують й практичні працівники (Додаток А).

Окрім цього, 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 доцільно доповнити частину 4 статті 99 КПК таким змістом: «Копія цифрового доказу, виготовлена слідчим, дізнавачем без участі спеціаліста у разі відсутності оригіналу цифрового доказу, може бути

визнана судом допустимою, якщо відсутні ознаки втручання з метою зміни відомостей після моменту виготовлення копії».

Це доповнення забезпечить правову визначеність у ситуаціях, коли оригінал цифрового доказу втрачений або неможливо його зберегти, але копія була виготовлена з дотриманням належних процедур без маніпуляцій з даними. Такий підхід дозволить врахувати реальні умови, в яких зберігаються електронні дані, і водночас убезпечить кримінальний процес від використання фальсифікованих доказів.

Окрім цього, дізнавачі, як і слідчі, повинні мати чітко визначені законні підстави для використання різноманітних ресурсів, зокрема інформаційно-телекомунікаційної системи досудового розслідування при зборі і дослідженні електронних доказів.

Саме тому введення формулювання «дізнавачем» після слів «виготовлені слідчим», є логічною та необхідною для узгодження нормативних актів і забезпечення єдиної правової практики. Це дасть змогу чітко визначити повноваження дізнавачів щодо виготовлення копій або дублікатів документів (в тому числі цифрових доказів) і їх використання в процесі кримінального провадження.

2.3. Використання спеціальних знань у справах про шахрайство, вчинене з використанням цифрових технологій

Призначення судових експертиз є важливим інструментом при розслідуванні 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, таких як підроблені документи, печатки, підписи чи інші предмети, що мають юридичну значимість.

Згідно з Інструкцією про призначення та проведення судових експертиз, затвердженою наказом Міністерства юстиції України № 53/5 від 08.10.1998, криміналістичні експертизи включають кілька основних напрямків, що можуть бути застосовані при розслідуванні шахрайств:

Експертиза документів – для виявлення підробок, зміни або фальсифікації документів, що використовуються шахраєм для створення ілюзії законності своїх дій. Це може включати 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 при підробці договорів, кредитних угод або інших важливих юридичних документів.

Для ефективного розслідування таких справ, експертні висновки є важливими доказами у судовому процесі. Вони допомагають встановити факти, що можуть бути використані для визначення причетності особи до шахрайства, а також сприяють більш точному розумінню механізмів скоєння злочину.

Узагальнений аналіз матеріалів кримінальних проваджень про шахрайство свідчить, що судові експертизи є невід'ємною частиною

розслідувань; їх призначають у 92% випадків. Це підтверджує важливість наукових та технічних досліджень у встановленні фактичних обставин злочинів.

За результатами судово-слідчої практики, слідчі використовують різні види експертиз для розслідування шахрайств. Найбільшу частку серед них займають криміналістичні експертизи, оскільки шахрайства часто пов'язані з підробленням документів, фальсифікацією підписів та іншими маніпуляціями з матеріальними доказами.

Розподіл призначених експертиз виглядає таким чином:

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

2. Технічні експертизи документів — 31%. Вони важливі для виявлення змін в документах, таких як підробки, виправлення, або інші втручання, які можуть свідчити про шахрайство.

3. Комп'ютерно-технічні 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.

4. Дактилоскопічні експертизи — 4%. Цей вид експертизи допомагає ідентифікувати особу, яка залишила відбитки пальців на документах чи інших предметах, що можуть бути пов'язані зі кримінальним правопорушенням.

5. Трасологічні експертизи — 4%. Вони дозволяють виявити сліди, що можуть бути залишені злочинцем при здійсненні шахрайства, наприклад, на місці вчинення кримінального правопорушення.

6. Товарознавчі експертизи — 3%. Використовуються для оцінки фальшивих товарів чи матеріальних доказів, пов'язаних із шахрайськими діями, наприклад, підробленої продукції.

7. Економічні експертизи — 2%. Ці експертизи важливі для виявлення фінансових маніпуляцій, несанкціонованих операцій або інших економічних злочинів, пов'язаних із шахрайством.

8. Психологічні експертизи — 1%. Це рідший, але інколи необхідний вид експертизи, який використовується для оцінки психічного стану осіб, які вчинили шахрайство, що може вплинути на їхню здатність усвідомлювати свої дії чи нести за них відповідальність.

Ці показники підтверджують, що більшість шахрайств здійснюється за допомогою різноманітних документів — від письмових і графічних до електронних. Це є важливою ознакою, оскільки документи часто виступають основним засобом підтвердження або фальсифікації фактичних обставин у шахрайських схемах. Враховуючи цей фактор, на початковому етапі розслідування необхідно чітко встановити спосіб підробки документа, що дозволить слідчим зібрати точнішу інформацію для подальшого розслідування, а саме:

1. Визначити вид підробленого документа. Це може бути письмовий документ (контракти, угоди, розписки), графічний (підроблені підписи або печатки) чи електронний документ (фальшиві електронні листи, файли або інші цифрові дані). Кожен вид вимагає різних методів дослідження та виявлення ознак підробки.

2. Виявити спосіб підробки. Важливо не лише визначити, що документ є підробленим, а й встановити, яким саме способом була здійснена підробка, чи використовувалися технічні засоби (наприклад, сканери та принтери), чи відбулося внесення змін до оригінальних файлів за допомогою комп'ютерних програм (для електронних документів).

3. Ідентифікувати винуватців. Встановлення способу підробки дозволяє не лише розкрити механізм шахрайства, а й визначити коло осіб, які могли бути причетні до виготовлення підроблених документів. Наприклад, технічні експертизи можуть виявити конкретні принтери чи сканери, використані для

виготовлення фальшивок, а почеркознавча експертиза — зв’язати підроблений підпис з конкретною особою.

4. Підготовка до висунення версій і подальших слідчих (розшукових) дій. Розуміння способу підробки документа є важливим для формулювання версій щодо того, як саме було вчинене шахрайство. Наприклад, якщо підроблені документи були використані для отримання кредиту або оформлення майна, слідчі можуть перевірити, яким чином ці документи потрапили до відповідних органів і які особи задіяні в цьому процесі.

Таким чином, своєчасне і правильне встановлення способу підробки документа на самому початку розслідування є важливим кроком у розслідуванні шахрайства та дозволяє правильно визначити напрямок подальших дій слідчого, що в свою чергу, сприяє ефективному розслідуванню та залученню винних осіб до відповідальності.

Слід зазначити, що Інструкція про призначення та проведення судових експертиз та експертних досліджень, затверджена наказом Міністерства юстиції України від 08.10.1998 № 53/5, не містить чітких положень щодо особливостей аналізу електронних документів. Відсутність визначеності призводить до різних підходів експертів під час їх дослідження.

У той же час Державна фіскальна служба України у своєму листі від 05.05.2016 № 10089/6/99-99-14-03-03-15 чітко зазначає обов’язок платників податків, які використовують електронні документи, забезпечувати їх друковані копії на вимогу контролюючих органів. Цей підхід базується на законодавстві про електронні документи та електронний документообіг і відображає прагнення контролюючих органів до більшої прозорості та доступності документів у традиційній паперовій формі під час перевірок.

Експерти опираються на застарілі нормативні документи, які не враховують особливості електронних документів, тоді як контролюючі органи адаптувалися до сучасних умов. Відсутність оновлення Інструкції призводить до розбіжностей у підходах, що може ускладнювати судову та адміністративну практику. Актуалізація нормативно-правових актів, які

регулюють електронний документообіг, необхідна для узгодження позицій між експертними та контролюючими органами. На нашу думку, це забезпечить єдині підходи до оцінки електронних документів, підвищить ефективність експертиз і документальних перевірок та мінімізує правові ризики для учасників процесу.

За стадіями виготовлення документи, в тому числі і електронні, діляться на оригінали, дублікати, копії і виписки. Для електронного документа такі поняття, як «оригінал», «дублікат», «копія» є умовними, оскільки у всіх цих випадках електронний документ залишається оригіналом.

Експерту необхідно оцінити, чи можливо отримати доступ до документа з конкретного носія, чи потрібні спеціальні технічні засоби або паролі. Для кожного типу носія важливо перевірити цілісність документа (відсутність змін) шляхом аналізу метаданих або використання криптографічних методів. Вибір обладнання та програм для роботи з конкретним носієм даних є визначальним у процесі експертизи.

Врахування типу носія є важливим, оскільки електронний документ, хоча й не має традиційної матеріальної форми, усе ж пов'язаний із фізичним носієм, що забезпечує його збереження і доступність для аналізу.

Дослідження електронного документа як об’єкта економічної експертизи вимагає врахування його зовнішньої форми та персоніфікуючих атрибутів, що роблять документ унікальним і дозволяють ідентифікувати його серед інших.

Зовнішня форма визначає спосіб фіксації та подання інформації в документі. Її особливостями є:

1. Рукописна форма. Рідкісний спосіб створення електронних документів, який виник з поширенням пристроїв із сенсорними панелями, таких як планшети. Це вимагає спеціального програмного забезпечення для розпізнавання рукописного тексту (наприклад, OCR — Optical Character Recognition). Вона не досліджувалася широко в експертній практиці, але може мати значний потенціал у майбутньому.

2. Виготовлення за допомогою технічних засобів. Це найпоширеніший спосіб створення електронних документів. Документи мають цифровий формат і зазвичай генеруються текстовими редакторами, програмами для обробки таблиць або іншими застосунками.

3. Персоніфікуючі атрибути електронного документа. Персоніфікація дозволяє виокремити конкретний документ серед маси інших за допомогою таких характеристик:

1. Ім’я файлу - може бути індивідуальним (призначеним творцем) або автоматично створеним програмним забезпеченням. Воно дозволяє швидко ідентифікувати документ, якщо він зберігається разом з іншими файлами.

2. Формат файлу - визначає програмне забезпечення, яке може відкрити та обробити документ (наприклад, .docx, .xlsx, .pdf). Формат впливає на можливість внесення змін, перегляду чи аналізу документа.

3. Розмір файлу. Він відображає обсяг пам’яті, яку займає документ, і є важливим показником для виявлення змін у документі (наприклад, збільшення розміру може свідчити про додаткову інформацію чи редагування).

4. Дата і час створення або редагування - важливий атрибут, що дозволяє встановити хронологію подій, пов’язаних із документом.

Атрибути використовуються для визначення автентичності документа та відповідності його до конкретної справи. Зіставлення метаданих із заявленими обставинами може допомогти виявити маніпуляції. Експерт визначає, чи відповідає спосіб створення (рукописний чи технічний) заявленим обставинам справи. Аналіз дати, часу, розміру та формату файлу дозволяє визначити, чи були внесені зміни в документ, і якщо так, то коли.

Вивчення зовнішньої форми електронного документа та його атрибутів є основою для проведення комплексної експертизи, що дозволяє забезпечити його точну ідентифікацію, автентичність і використання у правовій сфері.

Електронний документ, окрім персоніфікуючих реквізитів, може мати захисні та посвідчувальні реквізити, що відіграють важливу роль у забезпеченні його автентичності, цілісності та правового статусу. До таких реквізитів належить, зокрема, електронний цифровий підпис (ЕЦП).

Закон України «Про електронний цифровий підпис» визначає ЕЦП як результат криптографічного перетворення електронних даних, який: підтверджує цілісність документа, ідентифікує підписувача та забезпечує юридичну силу.

Наявність ЕЦП підтверджує, що документ створений та підписаний конкретною особою, а його зміст залишається незмінним. Ідентифікація носія допомагає встановити джерело походження документа. Аналіз ЕЦП і захисних механізмів дозволяє визначити, чи були внесені зміни до документа після його підписання. Документи з ЕЦП вважаються дійсними згідно з вимогами Закону України «Про електронні документи та електронний документообіг».

Отже, захисні та посвідчувальні реквізити, такі як ЕЦП, підвищують надійність електронних документів, роблять їх придатними для використання в судово-експертній практиці, а також забезпечують їх юридичну силу та ідентифікацію. Ідентифікуючі ознаки носія також мають велике значення, оскільки дозволяють встановити джерело і місце зберігання документа.

Проблема достовірності та доказової сили електронних документів залишається однією з ключових у сучасному правовому регулюванні. У зв'язку з відсутністю конкретних критеріїв достовірності електронних доказів у процесуальному законодавстві, виникають труднощі в їх оцінці і використанні в судовій практиці.

Варто зазначити, що встановлення достовірності цифрових доказів у судовій практиці є складним і багатогранним процесом, який залежить від типу електронного документа та його контексту. Використання різних підходів демонструє спробу адаптувати чинні правила до особливостей

електронних документів. Проте кожен з методів має свої переваги та недоліки.

Однією з ключових складових розслідування кіберзлочинів є комп'ютерно-технічна експертиза, оскільки дозволяє визначити технічний аспект кримінального правопорушення, пов'язаний з використанням комп'ютерних засобів і технологій. Вона включає в себе дослідження комп'ютерної техніки, програмного забезпечення, а також комп'ютерних носіїв інформації з метою встановлення важливих фактів, що можуть мати значення для кримінального процесу.

Основні завдання комп'ютерно-технічної експертизи:

1. Визначення статусу об'єкта як комп'ютерного засобу. Експерт може підтвердити, чи є певний пристрій комп'ютерним засобом, наприклад, сервером, персональним комп'ютером, планшетом чи смартфоном, що має важливе значення для розслідування злочину, пов'язаного з комп'ютерними технологіями.

2. Виявлення та дослідження ролі комп'ютерної техніки у кримінальному провадженні. Експерти проводять аналіз того, яким чином комп'ютерні системи і програмне забезпечення використовувалися в рамках злочину. Це може включати виявлення злочинних дій, таких як несанкціонований доступ до даних, використання комп'ютерних систем для шахрайства, хакерських атак або інших кіберзлочинів.

3. Отримання доступу до інформації на електронних носіях. Важливою складовою комп'ютерно-технічної експертизи є відновлення даних з комп'ютерних носіїв, таких як жорсткі диски, флеш-накопичувачі, CD/DVD диски, а також відновлення видалених файлів, що можуть бути важливими для розслідування. Це може включати у себе збереження слідів кримінального правопорушення або встановлення часу і місця вчинення правопорушення.

4. Дослідження програмного забезпечення. Комп'ютерно-технічна експертиза також може включати аналіз програмного забезпечення, яке

могло бути використано при вчиненні злочину (наприклад, шкідливі програми, трояни, віруси або спеціалізовані інструменти для отримання несанкціонованого доступу до комп'ютерних систем).

Основними етапами комп'ютерно-технічної експертизи є:

1. Первинний огляд техніки та носіїв. На цьому етапі експерт визначає, чи є пристрій або носій інформації відповідним об'єктом дослідження, перевіряє його стан, конфігурацію та наявність слідів злочину.

2. Збирання і збереження цифрових доказів. Це включає створення точних копій даних з пристрою або носія інформації для подальшого аналізу, що гарантує збереження автентичності доказів.

3. Аналіз даних і встановлення обставин у кримінальному провадженні. Після збереження доказів проводиться безпосереднє дослідження даних з метою встановлення фактів, які можуть бути важливими для кримінального процесу. Це може включати виявлення історії доступу до файлів, встановлення часу та місця вчинення кримінального правопорушення, аналіз логів та метаданих.

4. Формулювання висновку. Після проведеного дослідження експерт формулює висновок, який містить оцінку об'єктів дослідження, результатів експертизи та їх значення для розслідування.

Комп'ютерно-технічна експертиза може бути використана для вирішення численних питань, що виникають у ході розслідування кіберзлочинів, таких як:

- Встановлення факту несанкціонованого доступу до комп'ютерних систем або даних.
- Підтвердження або спростування наявності шкідливого програмного забезпечення на комп'ютерах або серверних системах.
- Виявлення доказів кібершахрайства, зокрема у випадках підробки документів, використання фальшивих електронних підписів, створення фальшивих фінансових операцій тощо.

- Визначення джерела кібератаки чи інтернет-шахрайства, а також встановлення осіб, причетних до кримінально протиправної діяльності.

У випадку розслідування кіберзлочинів, комп'ютерно-технічна експертиза є незамінним інструментом для збору та аналізу цифрових доказів, що мають вирішальне значення для доказування вини осіб, що вчинили кримінальне правопорушення [73].

Такий підхід дозволить скоротити час, потрібний для проведення дослідження [72, с. 101].

До видів носіїв інформації, які широко використовуються в комп'ютерних та інформаційних системах, належать:

1. Накопичувачі на жорстких магнітних дисках (HDD). Це традиційні пристрої для зберігання інформації, де використовується магнітний запис. Вони складаються з одного або кількох дисків, покритих магнітним матеріалом, та головок для читання/запису інформації. Накопичувачі HDD використовуються для зберігання великих обсягів даних, однак мають обмеження у швидкості доступу до даних через механічні рухомі частини.

2. Твердотілі накопичувачі (SSD, Solid State Drive). Це сучасні пристрої зберігання інформації, що не містять рухомих частин. Вони використовують мікросхеми пам'яті для збереження даних, що значно покращує швидкість доступу до інформації, зменшує енергоспоживання і підвищує надійність порівняно з HDD. Твердотілі накопичувачі стали стандартом для більшості сучасних комп'ютерів та мобільних пристроїв завдяки високій швидкості та довговічності.

3. USB флеш-накопичувачі. Це портативні пристрої зберігання даних, які використовують флеш-пам'ять для збереження даних і підключаються до комп'ютерів або інших пристроїв через USB-порти. Вони є дуже популярними завдяки компактним розмірам, зручності використання та здатності зберігати великі обсяги даних. USB флеш-накопичувачі часто використовуються для перенесення файлів між пристроями.

4. Карти пам'яті. Це маленькі носії інформації, які також використовують флеш-пам'ять. Вони застосовуються для зберігання даних в портативних пристроях, таких як мобільні телефони, цифрові камери, планшети та інші пристрої. Карти пам'яті підключаються до комп'ютера або іншого обладнання через спеціалізовані адаптери або картрідери. Існують різні формати карт пам'яті, наприклад, microSD, SD, CF та інші [73].

Завдання пошуку і визначення вірусів, а також інших шкідливих програм у процесі комп'ютерно-технічної експертизи є важливим та складним аспектом, що вимагає особливих навичок і знань у галузі комп'ютерної безпеки та програмування. Це необхідно зробити, адже існує велика кількість шкідливих програм (вірусів, троянів, руткітів, червів тощо), кожна з яких має різні методи приховування, поширення і функціонування. Ці програми можуть бути скритими, завдяки чому їх виявлення вимагає високої точності та використання спеціалізованих інструментів для аналізу.

Одним із завдань комп'ютерно-технічної експертизи є виявлення шкідливих програм, про які не відомо раніше. Нові види вірусів можуть бути створені для певних цілей, і вони часто змінюють свій код, що ускладнює їх виявлення за допомогою традиційних методів аналізу. Програмний код шкідливих програм може бути також обфускований (маскований), що ускладнює його аналіз.

Після виявлення шкідливого програмного коду його необхідно аналізувати на предмет його функцій і мети. Це може включати розшифровку коду, запуск його в безпечному середовищі (пісочниця) для спостереження за поведінкою програми, а також вивчення її взаємодії з операційною системою та іншими програмами. Не завжди можна з впевненістю сказати, що на носії немає шкідливих програм, особливо якщо вони були змінені або замасковані.

Слід зазначити, що для пошуку вірусів та шкідливих програм використовуються різні методи та інструменти, зокрема антивірусні програми, системи для моніторингу мережевого трафіку, а також інструменти для аналізу програмного коду та виявлення аномалій. Однак

навіть з усіма цими інструментами, виявлення та класифікація нових видів шкідливих програм залишається складним завданням, яке потребує висококваліфікованих фахівців.

Виявлення програм, що призначені для несанкціонованого втручання в роботу комп'ютерних мереж, потребує вивчення мережевого трафіку і взаємодії між пристроями. Ці програми можуть бути спрямовані на крадіжку інформації, підготовку до атак або інші кримінально протиправні дії. Для їх виявлення важливо не лише мати доступ до носія інформації, але й мати можливість моніторити саму мережу [72, с. 101].

Для збереження доказової інформації надзвичайно важливо забезпечити правильний збір, транспортування і зберігання об'єктів, що підлягають експертизі. Найпоширенішими помилками є неправильне відключення техніки (наприклад, вимкнення без створення образу даних), недостатнє документування стану комп’ютера чи мережі на момент вилучення, втрата або пошкодження цифрових доказів під час транспортування. У такому випадку залучення кваліфікованого фахівця, який має досвід роботи з комп’ютерними носіями, допоможе мінімізувати ризики втрати інформації.

Окрім цього, недоліком у призначенні експертиз часто є неправильне чи некоректне формулювання питань, що ускладнює отримання релевантних відповідей. Слідчим доцільно залучати експертів на етапі формування питань, оскільки вони краще розуміють технічні аспекти об’єкта дослідження.

Тому питання мають бути сформульовані так, щоб експерт міг надати однозначну і точну відповідь. Наприклад: «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?.

Учасники судочинства часто не мають достатніх знань для правильної постановки питань. У таких випадках необхідно проконсультуватися з

експертом, який може допомогти уточнити, які питання є доцільними з технічної точки зору.

Ми вважаємо, що розробка уніфікованих підходів до формулювання питань може спростити процес. Так, створення методичних рекомендацій для слідчих та суддів, які включають приклади найбільш поширених питань і алгоритм їх постановки може позитивно вплинути на процес досудового розслідування.

У зв'язку з цим необхідно:

1) регулярно оновлювати методичні посібники та інструкції відповідно до змін у сфері кібербезпеки та появи нових видів кіберзлочинів.

2) залучати до розробки рекомендацій фахівців у галузі інформаційних технологій, цифрової криміналістики та юриспруденції для врахування багатосторонніх аспектів експертного дослідження.

3) розробляти практичних курсів з основ цифрової криміналістики, включаючи роботу з комп'ютерними носіями, методи виявлення шкідливого ПЗ та способи збору цифрових доказів.

4) підтримувати міжнародної співпраці та обмін досвідом із зарубіжними експертами у сфері кібербезпеки та судової експертизи.

Окремо потрібно звернути увагу на участь спеціаліста при розслідуванні кримінальних правопорушень, вчинених за допомогою цифрових технологій.

Відповідно до ст. 71 КПК України, спеціаліст може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок, та може бути залучений для надання безпосередньої технічної допомоги [91]. Особливого значення використання спеціальних знань набуває під час проведення таких слідчих (розшукових) дій як слідчий огляд та обшук, оскільки вони пов'язані безпосередньо з виявленням, дослідженням та вилученням комп'ютерного обладнання і його програмного забезпечення [106, с. 113].

Відповідно до КПК України спеціаліст має право: 1) ставити запитання учасникам процесуальної дії з дозволу сторони кримінального провадження, яка його залучила, чи суду; 2) користуватися технічними засобами, приладами та спеціальним обладнанням; 3) звертати увагу сторони кримінального провадження, яка його залучила, або суду на характерні обставини чи особливості речей і документів; 3-1) викладати у висновку відомості, що мають значення для кримінального провадження і щодо яких йому не були поставлені запитання; 4) знайомитися з протоколами процесуальних дій, в яких він брав участь, і подавати до них зауваження; 5) одержувати винагороду за виконану роботу та відшкодування витрат, пов'язаних із його залученням до кримінального провадження; 6) заявляти клопотання про забезпечення безпеки у випадках, передбачених законом; 7) надавати висновки з питань, що належать до сфери його знань, під час досудового розслідування кримінальних проступків, у тому числі у випадках, передбачених частиною третьою статті 214 цього Кодексу; 8) надавати довідки з питань, що належать до сфери його знань, у випадках, передбачених частиною третьою статті 245-1 цього Кодексу [91].

Залучення спеціалістів під час розслідування кіберзлочинів має важливе значення, оскільки завдяки допомозі спеціаліста можливо визначити індивідуальний кримінальний почерк кіберзлочинця, вид та характеристики розроблених ним програм, які були використані ним у злочинній діяльності тощо. Також, на нашу думку, важливим є залучення ІТ-фахівців для допомоги слідчим та спеціалістам у розслідуванні кіберзлочинів, оскільки сфера захисту від кіберзлочинності стрімко та динамічно розвивається, що зумовлює потребу у підвищенні ефективності боротьби з кіберзлочинами та пошуку нових форм співпраці між правоохоронними органами та суспільством.

Спеціальні знання відіграють ключову роль у розслідуванні кіберзлочинів, оскільки вони дозволяють ефективно виявляти, аналізувати та

документувати цифрові докази, що є критичними для встановлення фактів правопорушення та притягнення винних до відповідальності.

Висновки до розділу 2

1. Встановлено, що оцінка слідчим первинної інформації — це перший крок, який безпосередньо визначає стратегічний напрямок всього розслідування. Оскільки йдеться про технологічно складні кримінальні правопорушення, ефективна оцінка повинна бути багаторівневою, з використанням специфічних технічних знань і навичок. Це включає в себе аналіз слідів, отриманих із цифрових пристроїв, перевірку даних про транзакції в системах електронних платежів, а також збір інформації від свідків чи потерпілих, які можуть бути недостатньо обізнані щодо технічних аспектів шахрайства.

Враховуючи швидкий розвиток технологій та зміну підходів до здійснення шахрайства в кіберпросторі, наукове осмислення обставин, які підлягають встановленню в рамках кримінального провадження, повинно включати новітні аспекти. Це включає в себе детальне вивчення нових типів кібератак (наприклад, шахрайства на основі штучного інтелекту), технологій, які використовуються зловмисниками, а також нові види доказів, зокрема електронні сліди та цифрові відбитки.

2. Для підвищення ефективності використання цифрових доказів у кримінальному процесі необхідно удосконалити процедури збору і фіксації таких доказів. Законодавець повинен чітко регламентувати порядок збору, верифікації, збереження та передачі електронних доказів. Важливо також запровадити єдиний стандарт процесуального оформлення електронних доказів, який би включав обов'язкову перевірку їх автентичності через спеціалізовані технічні засоби (наприклад, алгоритми хешування).

3. Основні аспекти значення спеціальних знань у розслідуванні кримінальних правопорушень у сфері цифрових технологій:

Залучення спеціалістів. Участь експертів з інформаційних технологій та кібербезпеки під час слідчих дій забезпечує правильне поводження з цифровими доказами, що мінімізує ризик їх пошкодження або втрати.

Проведення судових експертиз. Спеціальні знання необхідні для проведення комп'ютерно-технічних експертиз, які включають аналіз комп'ютерних систем, мереж та даних з метою виявлення слідів кримінально протиправної діяльності.

Аналіз методів вчинення кримінальних правопорушень. Розуміння сучасних технологій та методів, які використовуються кіберзлочинцями, дозволяє слідчим ефективніше виявляти та розслідувати такі правопорушення.

Підготовка та навчання персоналу. Постійне підвищення кваліфікації слідчих у сфері інформаційних технологій сприяє більш ефективному розслідуванню кіберзлочинів.

РОЗДІЛ 3
НАПРЯМИ ВДОСКОНАЛЕННЯ ДОКАЗУВАННЯ У СПРАВАХ ПРО ШАХРАЙСТВО, ВЧИНЕНЕ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ, В УМОВАХ СЬОГОДЕННЯ

3.1. Проблеми доказування у справах про шахрайство, вчинене з використанням цифрових технологій

На початковому етапі розслідування шахрайств важливим є визначення алгоритму дій сторони обвинувачення, яке базується на характері та обсязі наявних даних. Процес доказування шахрайства є багатоетапним і охоплює кілька ключових аспектів:

1) подія шахрайства:

- встановлення часу, місця та способу вчинення кримінального правопорушення;

- дослідження дій, що входять до механізму шахрайства, включаючи використання обману чи зловживання довірою.

2) винуватість конкретної особи:

- збір доказів, які підтверджують причетність підозрюваного до вчинення шахрайства;

- аналіз поведінки, дій та зв’язків підозрюваного, які могли бути спрямовані на досягнення кримінально протиправного результату;

3) мотиви вчинення кримінального правопорушення:

- з’ясування особистої зацікавленості підозрюваного (матеріальної вигоди, особистих мотивів тощо);

4) обставини, що впливають на відповідальність:

- розгляд обтяжуючих або пом’якшувальних обставин, таких як попередня судимість чи добровільне відшкодування шкоди;

5) характер і розмір завданої шкоди:

- оцінка матеріальної та нематеріальної шкоди, завданої потерпілим;

- документування наслідків кримінального правопорушення (фінансові втрати, порушення ділової репутації тощо);

6) обставини, що сприяли вчиненню шахрайства:

- аналіз факторів, які полегшили вчинення кримінального правопорушення (відсутність належного контролю, недоліки у захисті інформації тощо).

Усі ці аспекти розслідування мають бути забезпечені відповідними доказами, зокрема документами, свідченнями потерпілих, показаннями свідків, матеріалами відео- чи аудіофіксації, а також результатами експертиз. Такий комплексний підхід дозволяє всебічно і повно встановити обставини шахрайства, забезпечуючи об’єктивність судового розгляду.

Відповідно до статей 214 і 237 КПК України [91], огляд місця події є ключовою первинною та невідкладною слідчою (розшуковою) дією, яка здійснюється для:

1) виявлення слідів кримінального правопорушення:

- пошук доказів, які можуть свідчити про характер і спосіб вчинення кримінального правопорушення;

- виявлення слідів, що можуть ідентифікувати зловмисника (відбитки пальців, сліди взуття, залишки речовин тощо);

2) виявлення речових доказів:

- фіксація та вилучення предметів, які можуть мати доказове значення (знаряддя кримінального правопорушення, документи, особисті речі потерпілого або підозрюваного);

3) з’ясування обстановки кримінального правопорушення:

- аналіз і фіксація розташування об’єктів, слідів, предметів у межах місця події;

- встановлення деталей, які можуть вказувати на механізм вчинення кримінального правопорушення або поведінку учасників;

4) встановлення інших обставин, які мають значення:

- оцінка умов, які могли сприяти вчиненню кримінального правопорушення або вплинути на його характер;

- вивчення просторових, часових і фізичних умов, за яких могло бути вчинено кримінальне правопорушення.

Законодавством також виділяються особливості проведення огляду:

- Огляд має проводитися невідкладно після внесення відомостей до Єдиного реєстру досудових розслідувань (ст. 214 КПК України).

- Залучення спеціалістів (експертів, криміналістів) є обов'язковим у випадках, коли необхідні спеціальні знання для фіксації чи вилучення доказів.

- Огляд проводиться у суворій відповідності до процесуальних норм із обов'язковим складанням протоколу, який містить детальний опис місця події, виявлених об'єктів, їх розташування та супроводжується схемами, планами, фототаблицями або відеозаписами.

Таким чином, огляд місця події забезпечує належне документування і збереження доказової бази, формуючи основу для подальшого розслідування та доведення обставин справи в суді.

Огляд місця події в процесі розслідування шахрайств, вчинених у віртуальному просторі, має суттєву специфіку через особливості кіберпростору [103, с. 23].

До особливостей «кіберпростору» можна віднести: віртуальність, дислокацію інформації, динамічність і нестабільність даних.

Віртуальність характеризує кіберпростір як штучно створене середовище, де інформація зберігається, передається та обробляється в цифровій формі, переважно з використанням двійкового коду. Інформація в кіберпросторі існує у вигляді файлів, кодів, баз даних, які можуть знаходитися на фізичних чи віртуальних носіях.

Під дислокацією інформації розуміється зберігання інформації на жорстких дисках, логічних кластерах, серверах (data center), онлайн-сховищах (cloud storage), флеш-пам'яті, зовнішніх картах пам'яті тощо. Носії

можуть фізично знаходитися в будь-якій точці світу, включаючи країни з різними правовими режимами доступу до інформації.

Динамічність і нестабільність даних як одна із особливостей кіберпростору характеризується тим, що дані у віртуальному просторі легко видалити, змінити, перемістити або зашифрувати.

Огляд місця події в кіберпросторі має свою специфіку, до якої відноситься: локалізація об'єктів огляду, використання технічних засобів, фіксація стану носіїв, вивчення слідів кримінального правопорушення, міжнародна співпраця, правова безпека.

Локалізація об'єктів огляду розуміється як ідентифікація пристроїв і систем, на яких зберігається потенційно значуща інформація; встановлення фізичного розташування серверів, пристроїв та мереж, залучених до шахрайської діяльності.

Використання технічних засобів характеризується залученням експертів у галузі інформаційних технологій для аналізу цифрових носіїв, використанням спеціалізованого програмного забезпечення для зчитування, копіювання та аналізу даних.

Фіксації стану носіїв притаманне документування всіх дій із пристроями (збереження їх фізичного стану та цифрової структури), створення точних копій носіїв, що підлягають дослідженню, із дотриманням правил цифрової криміналістики.

Вивчення слідів кримінального правопорушення характеризується аналізом логів роботи системи (історії змін, з’єднань, доступів), виявленням IP-адрес, електронних поштових скриньок, акаунтів у соціальних мережах або на онлайн-платформах, що використовувались у шахрайстві.

Варто зауважити, що міжнародна співпраця застосовується у випадках, коли дані знаходяться на серверах за кордоном, потрібна взаємодія з правоохоронними органами інших країн.

Забезпечення дотримання законодавства під час збору, вилучення та аналізу інформації (процедури повинні відповідати нормам КПК України та міжнародним стандартам) гарантує правову безпеку.

Таким чином, огляд місця події у розслідуванні шахрайств у кіберпросторі потребує не лише технічного оснащення та спеціальних знань, а й чіткої процесуальної організації для забезпечення юридичної вагомості отриманих доказів.

Утворення індивідуальної слідової картини в контексті шахрайств у кіберпросторі створює низку проблем для їх виявлення, дослідження та використання як доказів у кримінальному провадженні. Ці труднощі обумовлені особливостями електронних слідів і динамічним характером віртуального середовища.

Особливості індивідуальної слідової картини включає в себе: недовговічність інформації; технічну складність фіксації, швидкість дій злочинця.

Для фіксації недовговічної інформації, особливо в режимі реального часу, необхідно застосовувати спеціальні заходи:

- технічний моніторинг;
- програмне забезпечення;
- збереження цифрових доказів;
- залучення експертів.

Дуже важливу роль у розслідуванні кримінальних правопорушень в кіберпросторі відіграє своєчасність, що запобігає втратам інформації та сприяє підвищенню ефективності процесу доказування.

Отже, своєчасність виявлення і фіксації слідів у кіберпросторі має вирішальне значення для забезпечення належного доказування у кримінальних провадженнях, пов’язаних із шахрайствами.

Сліди кримінальних правопорушень у кіберпросторі зазвичай виникають у результаті неправомірного зовнішнього або внутрішнього впливу на телекомунікаційні системи, окремі електронні пристрої, програми

або комп'ютерну інформацію. Вони характеризуються внесенням змін до структури або змісту комп'ютерної інформації. Сліди кіберзлочинів, хоч і мають специфічний характер, можуть бути ефективно ідентифіковані та використані в доказовій базі завдяки застосуванню сучасних методів цифрової криміналістики, своєчасності дій та залученню фахівців у цій галузі [129, с. 62].

Фіксація виявлених слідів є основоположним етапом під час розслідування шахрайств, вчинених із використанням інформаційних технологій. Це обумовлено необхідністю перетворення цифрових артефактів, невидимої інформації та слідів кіберзлочинів на докази, які можуть бути використані в судовому процесі.

Роль фіксації слідів у розслідуванні кримінальних правопорушень, вчинених за допомогою цифрових технологій, полягає у збереженні доказів з метою уникнення їхньої модифікації, знищення або спотворення; забезпеченні автентичності, що гарантує незмінність зібраних даних після їх вилучення, побудові доказової бази, де виявлені сліди слугують основою для формування системи доказів, що підтверджує факт кримінального правопорушення та встановлює причетність конкретних осіб до його вчинення.

Вдосконалення комп’ютерної техніки та цифрових носіїв інформації ставить нові виклики перед судовими експертами, які працюють з цифровими доказами. Зокрема, збільшення обсягів даних для аналізу, використання складних систем захисту інформації та впровадження новітніх технологій у пристрої створюють необхідність у застосуванні сучасних методів і інструментів. Тому експерти, що працюють в даній галузі повинні вміти визначати ключові аспекти для аналізу серед величезного обсягу інформації, використовувати логічні схеми для пошуку зв'язків між різними типами даних, мати поглиблені знання з розуміння принципів функціонування комп’ютерних систем, мереж та цифрових пристроїв, використовувати новітні інструменти у вигляді сучасного програмного

забезпечення для вилучення, аналізу та відновлення даних (наприклад, EnCase, FTK, X-Ways).

Набір таких знань та вмінь дозволяє забезпечити якісну експертизу навіть у складних випадках, зберігаючи актуальність доказової бази для вирішення справ у суді [51, с. 95–96].

В. Коршенко акцентує увагу на тому, що розвиток цифрових технологій та розширення спектра питань, які потребують експертного дослідження, призвели до змін у структурі судових експертиз в Україні.

До 2006 року для розв'язання питань, пов'язаних із дослідженням комп’ютерно-технічних засобів, телекомунікаційних систем, електронних пристроїв і програмного забезпечення, застосовувалася судова комп’ютерно-технічна експертиза. Однак, у зв'язку зі стрімким розширенням предмета експертних досліджень, постало питання про необхідність чіткішої спеціалізації в цій галузі [84, с. 198].

В Україні спостерігаються значні труднощі у використанні спеціальних знань як під час виявлення слідів кіберзлочинів, так і під час проведення експертних досліджень. Ці проблеми негативно впливають на ефективність розслідування протиправних діянь у сфері інформаційних технологій.

До основних проблем в цій сфері належать:

- Низький рівень навичок аналізу даних. Експертам і слідчим часто бракує спеціалізованої підготовки в аналізі цифрових слідів. Відсутність регулярного навчання та тренінгів з новітніх методів дослідження кіберзлочинів.

- Незабезпеченість обладнанням. Недостатня кількість сучасних програмно-апаратних комплексів для аналізу цифрових слідів. Відсутність доступу до ліцензованих програм для проведення глибокого аналізу інформації (наприклад, для відновлення видалених даних чи аналізу шифрованих файлів).

- Недоліки на етапі вилучення об’єктів дослідження. Неналежне пакування або транспортування цифрових носіїв оперативними та слідчими

підрозділами. Недотримання процедурного порядку вилучення інформації, що може призвести до втрати її доказової цінності.

- Проблеми збереження доказів. Відсутність умов для правильного зберігання цифрових носіїв. Ризик пошкодження або втрати інформації через недбалість чи брак технічних засобів для зберігання [51, с. 95–96].

На нашу думку, наслідками зазначених вище проблем може бути:

- зниження якості експертних висновків, що призведе до написання неточних або недостатньо обґрунтованих висновків.

- сумніви у допустимості доказів. Через недоліки на етапі вилучення та транспортування суд може визнати такі докази непридатними.

- ускладнення розслідування. Неефективність експертних досліджень може затягнути процес і вплинути на можливість встановлення осіб, причетних до вчинення кримінального правопорушення.

Ми вважаємо, що доцільно було б запропонувати такі напрями вдосконалення експертної діяльності в сфері кіберзлочинів:

- підвищення кваліфікації фахівців з організацією регулярних тренінгів, семінарів та курсів для слідчих, оперативників та експертів та залученням міжнародних експертів для обміну досвідом;

- оснащення сучасним обладнанням (закупівля програмних продуктів для аналізу цифрових слідів, таких як EnCase, FTK та інших), а також забезпечення лабораторій необхідними апаратними комплексами;

- стандартизація процедур вилучення та зберігання доказів, що дотягнеться за допомогою впровадження уніфікованих інструкцій для слідчих щодо вилучення, пакування та транспортування цифрових носіїв, а також розробка інфраструктури для зберігання цифрових доказів;

- розвиток співпраці з міжнародними організаціями у вигляді спільної роботи з міжнародними експертними центрами для отримання методик і технологій дослідження.

Реалізація зазначених заходів може значно підвищити якість розслідування кіберзлочинів та ефективність судових експертиз в Україні.

Мобільні телефони, включаючи смартфони та фаблети, є ключовими джерелами цифрових доказів у розслідуванні кібершахрайств. Водночас вони вимагають особливого підходу при вилученні та обробці, щоб уникнути втрати важливої інформації. Типові помилки, які виникають під час вилучення та упакування мобільних телефонів, можуть значно ускладнити розслідування.

Типові помилки під час роботи з мобільними телефонами:

- Невмикання «режиму польоту», що призводить до відсутності ізоляції телефону від мобільних операторів та мереж Wi-Fi і дозволяє злочинцю дистанційно видаляти або змінювати дані.

- Вимикання телефону без попереднього огляду. Це може призвести до активації механізмів захисту (наприклад, PIN-коду), ускладнюючи доступ до пристрою.

- Витягнення SIM-карти на ввімкненому телефоні. У більшості сучасних телефонів така дія запускає автоматичне перезавантаження, що блокує доступ до пристрою. У випадку використання біометричних способів розблокування (відбиток пальця, розпізнавання обличчя), ці методи можуть стати недоступними.

- Втрачена можливість дослідження телефону через біометричне блокування. Якщо телефон вже був розблокований за допомогою відбитка пальця чи розпізнавання обличчя, слід негайно здійснити резервне копіювання або зняття даних, оскільки після перезавантаження доступ до таких методів розблокування буде втрачено [71, с. 103].

Пропонуємо рекомендації для мінімізації помилок, що виникають у процесі розслідування кібершахрайств:

- Забезпечення спеціалізованої підготовки для спеціально уповноважених суб’єктів. Оперативні співробітники повинні мати чіткі інструкції щодо вилучення мобільних пристроїв і поводження з ними.

- Забезпечення використання спеціального обладнання (наприклад, сумок або кейсів із захистом від сигналів (Faraday Bags) для ізоляції телефонів від зовнішніх впливів).

- Фіксація процесу вилучення. Оформлення детального протоколу, включаючи фото- та відеофіксацію всіх дій з пристроєм.

- Проведення консультацій з експертами. У складних випадках залучення спеціалістів із цифрової криміналістики.

Впровадження цих підходів допоможе зберегти доказову базу та підвищити якість розслідування кримінальних правопорушен, вчинених за допомогою цифрових технологій.

Ще однією проблемою, яка може виникати на практиці, є вилучення мобільного телефону. Це є критичним етапом у розслідуванні шахрайств, вчинених із використанням мобільних пристроїв, адже будь-які помилки можуть призвести до втрати важливих цифрових доказів або їх пошкодження.

Основними кроками для забезпечення належної фіксації цифрових доказів (правильного вилучення мобільного телефону) є:

1) Розблокування телефону. Якщо телефон використовує біометричні методи захисту, такі як відбиток пальця або система розпізнавання обличчя, його потрібно розблокувати, щоб мати доступ до всіх функцій та даних. Важливо розблокувати телефон без впливу сторонніх осіб чи мереж, щоб не знищити або не змінити дані.

2) Переведення в «Режим польоту». Після розблокування телефон повинен бути переведений у «Режим польоту», щоб припинити можливість відправки чи отримання сигналів або даних, що можуть порушити цілісність інформації або допомогти зловмисникам видалити сліди.

3) Зміна налаштувань екрану та безпеки. У налаштуваннях телефону потрібно встановити параметр «Вимикання екрану» на значення «Ніколи», щоб запобігти автоматичному блокуванню чи зміні стану пристрою. Встановлення параметра «Блокування екрану / Режим очікування» на

«Ніколи» допомагає уникнути блокування пристрою, що може бути активовано після періоду неактивності. Зниження яскравості до мінімуму допоможе зберегти заряд акумулятора, що має велике значення для тривалого збереження даних без необхідності підзаряджання.

4) Зарядка пристрою. Для забезпечення безперервної роботи телефону та збереження всіх відкритих даних важливо підключити мобільний пристрій до зовнішнього джерела живлення, наприклад, до Power Bank.

5) Упаковка телефону. Після того як телефон належно підготовлений, його слід упакувати в спеціальний пакет, який блокує радіохвилі (наприклад, Faraday bag) [71, с. 103].

У разі вилучення мобільного телефону в рамках розслідування, зокрема з використанням зовнішнього носія живлення (Power Bank), важливо правильно документувати всі дії, щоб уникнути будь-яких питань щодо законності та обґрунтованості використання таких пристроїв.

Опис вмісту пакета, в якому вкладено зовнішній носій живлення, має бути чітким і точним, щоб уникнути будь-яких суперечок або питань під час судового розгляду.

Під час проведення телекомунікаційних експертиз експертам необхідно оперувати великим обсягом різноманітної довідкової інформації з різних галузей комп'ютерних наук та технологій. Це включає як технічні аспекти роботи з комп'ютерними системами, так і специфіку телекомунікаційних мереж, програмного забезпечення, криптографії, а також методи захисту та відновлення даних. На сьогодні в Україні відсутня централізована, упорядкована база даних для телекомунікаційних експертиз. Це дійсно створює певні складнощі для експертів, які змушені працювати з різноманітними джерелами інформації, часто розкиданими по численних Інтернет-ресурсах, що не завжди є надійними або достовірними. Це підвищує ризики помилок і невірних висновків у результатах досліджень.

Часто експерти використовують документи, інструкції або довідкову літературу, що можуть бути застарілими, неточними або навіть не

відповідають стандартам, необхідним для проведення конкретних досліджень.

Ще однією проблемою у доказуванні кіберзлочинів є використання несертифікованих або невідомих технічних засобів і програмного забезпечення. Це може поставити під сумнів точність результатів дослідження, оскільки механізми роботи таких інструментів можуть бути не до кінця вивченими або навіть небезпечними для даних.

Важливо використовувати лише сертифіковане обладнання та програмне забезпечення, яке перевірене та відповідає вимогам стандартів для судових експертиз [84, с. 198].

Для подолання зазначених вище проблем доцільно запропонувати такі напрями:

- Створення централізованої бази даних для телекомунікаційних експертиз, що включає в себе розробку та впровадження національної або міжнародної бази даних, яка містила б перевірену та актуальну інформацію для судових експертів. Це сприяло б стандартизації досліджень і допомогло б уникнути розбіжностей в інтерпретації технічних даних.

- Створення національних стандартів для комп'ютерно-технічних і телекомунікаційних експертиз (встановлення чітких стандартів і методичних рекомендацій для проведення телекомунікаційних експертиз). Це включало б використання сертифікованого програмного забезпечення та технічних засобів, а також обов'язкову перевірку джерел інформації.

- Підвищення кваліфікації експертів і забезпечення їх доступом до новітніх наукових досліджень. Регулярні тренінги і підвищення кваліфікації експертів допомогли б їм залишатися в курсі нових технологій і методів дослідження. Також, важливим є доступ до наукових і технічних публікацій, які можуть допомогти в подоланні технологічних проблем.

- Забезпечення надійного документування та сертифікації програмного забезпечення і технічних засобів. Сертифікація використовуваних технічних засобів та програмного забезпечення з метою

забезпечення точності результатів досліджень. Це дозволяє не тільки підвищити надійність досліджень, але й збільшити довіру до результатів експертизи.

Таким чином, для покращення якості телекомунікаційних експертиз важливо створити єдину нормативну основу, надійно документувати всі етапи досліджень та використовувати тільки сертифіковане обладнання і програмне забезпечення.

У методології проведення телекомунікаційної експертизи можуть застосовуватися різноманітні методи, характерні для інших видів експертиз, які апробовані та ефективні для роботи з цифровими доказами. Це дозволяє забезпечити всебічне та точне дослідження об'єктів, що є частиною кримінальних проваджень, зокрема шахрайств у кіберпросторі. До методів, що використовуються в телекомунікаційній експертизі належать: метод візуального дослідження, спостереження, органолептичні методи, вимірювання, порівняння, тестування.

Застосування цих методів дозволяє створити багатогранну картину досліджуваного об'єкта і забезпечити достовірність висновків у процесі розслідування кіберзлочинів. Крім того, ефективне використання класичних методів у цифровій експертизі потребує постійного вдосконалення підходів і розширення методології відповідно до швидко змінюваного технологічного середовища. [82, с. 224–230].

Поширенню кібершахрайств сприяють кілька ключових факторів, серед яких важливим є ускладнення ідентифікації осіб, які вчиняють такі правопорушення. Завдяки анонімності Інтернет-простору, зокрема використанню фальшивих ідентифікаційних даних, VPN-сервісів, а також різноманітних технологій маскування (наприклад, криптовалют або анонімних платіжних систем), виявлення та затримання правопорушників стає значно складнішим.

Додатково, відсутність адекватних реакцій з боку правоохоронних органів є ще однією причиною того, що кібершахрайства часто не

розслідуються або закриваються на ранніх етапах. Це може бути пов'язано з кількома чинниками: складність і тривалість розслідування; недостатня правова база; цивільно-правовий характер порушення: неохочість потерпілих звертатися до правоохоронців.

Для ефективної боротьби з кібершахрайствами необхідно розвивати правову та технічну інфраструктуру, вдосконалювати підготовку кадрів у галузі кібербезпеки, а також забезпечити адекватне законодавче реагування на цифрові злочини. Це включає в себе кращу інтеграцію правоохоронних органів із міжнародними структурами та зміцнення механізмів кримінально-правового реагування на кіберзлочини.

Проблеми, які виникають під час розслідування кібершахрайств, часто пов'язані з відсутністю належного зв'язку між використанням спеціального обладнання для отримання інформації про платіжні інструменти та подальшою їх підробкою для незаконного отримання матеріальних благ. Встановлення причинно-наслідкового зв'язку в таких випадках є важким через кілька факторів: технічна складність (наприклад, зловмисники можуть використовувати різноманітні технології, такі як фішинг, віруси чи інші способи, що ускладнюють ідентифікацію джерела витоку даних); відсутність достатніх доказів (наприклад, якщо інформація про платіжний інструмент була вкрадена через фішингові сайти або з використанням зловмисного програмного забезпечення, це може призвести до втрати прямого доказу або до неможливості точно визначити момент кримінального правопорушення); однобічність досудового розслідування (наприклад, на виявленні злочинного використання платіжних карток, не звертаючи належної уваги на попередні етапи: отримання даних або підготовку шахрайства); складність відстеження зв’язків між зловмисниками (наприклад, використання різних акаунтів, фальшивих ідентифікацій, VPN та інших інструментів для анонімізації своїх дій також ускладнює процес розслідування; невідповідність між нормативною базою і новими методами злочинів (наприклад, у деяких

випадках наявні закони та методи розслідування не встигають за швидким розвитком технологій і новими схемами шахрайства) [190, с. 43].

Поширеність і недостатня ефективність механізму тимчасового доступу до речей і документів, зокрема в контексті кримінальних проваджень, пов’язаних з кібершахрайствами, є важливою проблемою, яку відзначають практичні працівники (Додаток А). Ось деякі ключові аспекти, що підтверджують цю думку:

- Неефективність наявних процедур: 93% опитаних практичних працівників вважають норму ст. 166 КПК України неефективною, оскільки процес тимчасового доступу до документів та речей часто затягується. Цей захід є важливим, але повільним і залежить від численних додаткових кроків, таких як необхідність присутності представника організації, у володінні якої знаходяться потрібні документи чи матеріали (наприклад, банківських установ, операторів телекомунікаційних послуг). Це ускладнює процес і збільшує час, необхідний для збору важливої інформації, що може вплинути на успішність розслідування, особливо в кіберзлочинах.

- Відсутність чітких термінів: У КПК України відсутні чіткі вказівки щодо терміну, протягом 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.

- Штучні бар'єри у 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 випадку кримінальних розслідувань.

- Законодавчі прогалини щодо банківської таємниці: Стаття 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, необхідний для отримання доступу до важливих доказів.

Усі ці фактори вказують на необхідність вдосконалення законодавчих норм та процедур для забезпечення більш ефективного доступу до ключових доказів, що є особливо важливим у розслідуваннях, пов'язаних із сучасними формами шахрайства в кіберпросторі [137].

Завищена формалізація стандарту доказування, закладеного в норми кримінального процесуального законодавства, зокрема у статтю 166 КПК України, є серйозною перешкодою для оперативного та ефективного розслідування кримінальних правопорушень. Основні проблеми, що випливають із такого підходу, включають: затягування часу; створення ризику втрати доказів; обмеження ефективності розслідування; абсурдність стандарту з позиції мети провадження.

Проблема надмірної гуманізації законодавства в Україні, яка акцентує увагу на захисті прав правопорушника, викликає суттєві дискусії серед теоретиків і практиків. За нинішніх умов це стає однією з причин низької ефективності правосуддя, особливо в аспекті відновлення прав потерпілих.

Теорія відновного правосуддя акцентує увагу на відновленні справедливості, а не на покаранні, і пропонує підхід, який є альтернативою традиційному каральному правосуддю. Важливість відновного підходу полягає у: відновленні довіри (потерпілі отримують можливість почути вибачення та побачити реальну відповідальність з боку правопорушника) та зменшенні рецидивів (правопорушники, які пройшли через відновне правосуддя, частіше усвідомлюють наслідки своїх дій і рідше вчиняють повторні злочини).

Відновне правосуддя не тільки забезпечує справедливість, а й сприяє створенню умов для гармонійного вирішення конфліктів, зцілення потерпілих і інтеграції правопорушників у суспільство.

Зміна законодавства з метою забезпечення ефективного досудового розслідування та дотримання принципів наступальності й дієвості є важливим кроком для підвищення результативності боротьби з кіберзлочинністю, зокрема шахрайством у телекомунікаційній сфері.

На нашу думку, впровадження таких змін в законодавстві сприятиме:

- прискоренню процесу розслідування кримінальних правопорушень, пов’язаних із кіберзлочинністю;

- підвищенню ефективності збору доказів, що сприятиме встановленню осіб, причетних до злочинів, і притягненню їх до відповідальності;

- зменшенню випадків уникнення відповідальності через недостатню оперативність слідчих дій.

Звичайно відповідні законодавчі зміни потребують обговорення за участю правників, слідчих, суддів і експертів у сфері захисту прав людини для забезпечення комплексного та ефективного підходу.

Тим самим треба внести зміни у ст. 166 КПК України, виклавши її в такій редакції: «У разі невиконання ухвали про тимчасовий доступ до речей і документів прокурор, слідчий, дізнавач із метою відшукання та вилучення зазначених в ухвалі речей і документів вправі невідкладно провести обшук. У такому разі прокурор, слідчий, дізнавач за погодженням із прокурором зобов’язаний невідкладно після здійснення таких дій звернутися до слідчого судді із клопотанням про проведення обшуку».

Розслідування кіберзлочинів, пов'язаних із динамічними IP-адресами, складне через специфіку їх використання. Динамічні IP-адреси, на відміну від статичних, регулярно змінюються, що створює труднощі в ідентифікації конкретного користувача або пристрою в мережі.

Динамічні IP-адреси виділяються провайдерами Інтернет-послуг (ISP) із загального пулу на обмежений час (наприклад, на час сеансу підключення або згідно з DHCP-налаштуваннями). Після завершення сесії IP-адреса може бути призначена іншому користувачеві.

Щоб встановити особу, яка використовувала певну динамічну IP-адресу, необхідно звернутися до провайдера. Провайдер може надати журнали (лог-файли), у яких зберігається інформація про те, якому користувачеві і в який момент було виділено конкретну адресу. Запити до провайдера, як правило, вимагають відповідного дозволу (наприклад, судового рішення).

Використання проксі-серверів, VPN або анонімайзерів може додатково ускладнювати встановлення кінцевого користувача. Спеціальні технології, такі як NAT (Network Address Translation), також можуть приховувати справжню IP-адресу користувача [30].

IP-адреса є важливим, але недостатньо точним показником для однозначної ідентифікації конкретного комп'ютера. Вона дає напрямок для розслідування, але потребує доповнення іншими джерелами даних.

обов'язковий облік користувачів із прив'язкою до номера мобільного телефону може значно полегшити розслідування шахрайських дій, здійснених через Інтернет. Таким чином, хоча обов'язковий облік користувачів через номери мобільних телефонів може стати ефективним інструментом для боротьби з шахрайствами в Інтернеті, важливо, щоб ця система була добре збалансована і враховувала як безпеку, так і захист персональних даних користувачів.

На нашу думку, запровадження обмежень на продаж SIM-карт лише за наявності паспорта громадянина України або іншого документа, що посвідчує особу, для іноземців та осіб без громадянства, є досить доцільним і обґрунтованим заходом для підвищення рівня безпеки та боротьби з кіберзлочинністю, зокрема шахрайствами, що здійснюються через мобільні телефони.

Вимога надавати паспорт або інші документи, що посвідчують особу при покупці SIM-карт, має значний потенціал для зменшення рівня анонімності у сфері мобільного зв'язку, що допоможе ефективніше боротися з шахрайськими діями та іншими кримінальними правопорушеннями в

Інтернеті. Проте для успішної реалізації цієї ініціативи необхідно забезпечити належний рівень захисту персональних даних та інтеграцію з існуючими правовими механізмами.

Розслідування шахрайств у кіберпросторі дійсно має свої специфічні особливості, зокрема, пов'язані з характером цифрових слідів, які залишаються після вчинення кримінального правопорушення. Наведемо приклад ключових аспектів, що характеризують першочергові та подальші слідчі дії під час таких розслідувань:

1) Цифрові сліди можуть бути швидко стерті або змінені: інформація, яка зберігається в комп'ютерних системах, може бути видалена за допомогою спеціальних програм або технік (наприклад, за допомогою методів шифрування, очищення дисків чи використання спеціальних програм для видалення слідів). Деякі цифрові сліди, як-от історія браузера або кеш, можуть зникати після завершення сесії або перезавантаження пристрою. Це означає, що час має критичне значення для фіксації слідів. Затримка в часі може призвести до втрати ключових доказів, тому швидкість реагування на інцидент є важливою для успіху розслідування.

2) Для виявлення і фіксації цифрових слідів необхідні глибокі технічні знання в галузі комп'ютерної криміналістики та кібербезпеки. Тому важливо, щоб слідчі мали доступ до спеціалізованих експертів або криміналістичних лабораторій, що можуть надати необхідну підтримку. Розслідування може включати різні етапи: аналіз жорстких дисків, логів серверів, мережевого трафіку, перевірку електронної пошти, соціальних мереж, мобільних пристроїв тощо. Фахівці з кібербезпеки допомагають правильно зібрати та зберегти цифрові докази, дотримуючись всіх стандартів і процедур, щоб забезпечити їх допустимість в суді.

3) Виявлення цифрових слідів.

4) Протоколювання та збереження доказів. Оскільки цифрові докази є дуже чутливими до змін, їх треба правильно протоколювати і зберігати. Порушення процедури може призвести до дискредитації доказів у суді. Для

фіксації доказів необхідно використовувати спеціалізовані програми і методи, щоб зберегти цілісність даних, наприклад, шляхом створення образів дисків або збереження потоку даних без змін.

5) Для збору цифрових доказів використовуються спеціалізовані інструменти, такі як: програми для аналізу мережевого трафіку (наприклад, Wireshark); програми для аналізу жорстких дисків та відновлення даних (наприклад, EnCase, FTK); інструменти для аналізу мобільних пристроїв та телефонних номерів; програми для моніторингу і фіксації активності в Інтернеті.

Також слідчі можуть використовувати аналітичні інструменти, які допомагають встановити зв'язки між різними цифровими слідами та визначити логічну послідовність дій зловмисників.

6) Однією з особливостей шахрайств у кіберпросторі є намагання зловмисників зберігати свою анонімність. Вони можуть використовувати проксі-сервери, VPN або інші інструменти для маскування своєї IP-адреси, що ускладнює відстеження джерела атаки. Однак, правильне використання логів та інформації з різних джерел може допомогти у подоланні цих труднощів, дозволяючи встановити, де і коли було вчинено кримінальне правопорушення.

7) Часто шахрайства у сфері цифрових технологій мають міжнародний характер. Це означає, що для виявлення та фіксації доказів слідчим може знадобитися співпраця з іншими країнами та міжнародними організаціями. Важливо, щоб такі розслідування проводилися відповідно до міжнародних угод і стандартів (наприклад, Конвенція Ради Європи про кіберзлочинність або Європейська конвенція про взаємну допомогу).

8) Оскільки цифрові докази можуть бути знищені, змінені або викрадені (наприклад, через атаку на систему або маніпуляції з даними), дуже важливо застосовувати належні заходи безпеки під час збору та зберігання доказів, щоб уникнути їх підробки чи втрати.

У процесі розслідування шахрайств у кіберпросторі основною складністю є нестабільність і швидка зміна цифрових слідів, що вимагає від слідчих високого рівня професіоналізму та наявності спеціалізованих знань і інструментів. Своєчасне виявлення, фіксація та збереження цифрових доказів є критично важливими для успішного розслідування і доведення провини зловмисників у суді.

Розслідування шахрайств у кіберпросторі справді ставить перед уповноваженими органами серйозні виклики, які значно ускладнюють процес виявлення та доведення злочинів у цій сфері. Задача ефективного розслідування шахрайств у кіберпросторі вимагає постійного вдосконалення процесуальних норм, залучення висококваліфікованих фахівців та належного технічного забезпечення. Оскільки ці злочини стають все більш складними і різноманітними, важливо забезпечити розвиток відповідних методик та ресурсного забезпечення для правоохоронних органів. Крім того, необхідна міжнародна співпраця для вирішення транснаціональних проблем у сфері кіберзлочинності.

Тому позиція активної протидії кіберзлочинам на етапі превенції є надзвичайно важливою, оскільки запобігання кримінальним правопорушенням завжди є ефективнішим, ніж боротьба з наслідками вже вчинених кримінальних правопорушень. Підвищення обізнаності громадян щодо шахрайств в Інтернеті є ключовим елементом такої стратегії [107].

Цифрові технології, зокрема криптовалюта, створюють нові виклики для правової системи. В Україні, як і в багатьох інших країнах, правовий статус криптовалют не до кінця визначений, що ускладнює їх правове регулювання, зокрема у контексті боротьби з кримінальними правопорушеннями. Криптовалюта є новим викликом для правової системи, і її використання в кримінальних правопорушеннях вимагає оперативного реагування та правового регулювання.

Криптовалюти стали важливою частиною глобальної економіки, і їх вплив на фінансові ринки зростає з кожним роком. На сьогодні існує більше

ніж 2000 видів криптовалют, і загальна вартість цих цифрових активів продовжує зростати. Вартість ринку криптовалют, яка за останній рік збільшилася в п’ять разів, є свідченням того, що цей сектор привертає увагу як інвесторів, так і широкої громадськості. Криптовалюти продовжують розвиватися, привертаючи інтерес як інвесторів, так і регуляторів. Станом на сьогодні, їхня популярність та роль у глобальній економіці важко переоцінити. Незважаючи на те, що багато країн ще шукають оптимальні способи регулювання цієї нової форми цифрових активів, потенціал криптовалют і технології блокчейн продовжують змінювати фінансові ринки та систему обміну цінностями у світі.

Україна є однією з лідерів у використанні віртуальних активів серед населення, і цей факт підтверджують як статистичні дані, так і активний розвиток криптовалютної індустрії в країні. За даними Міністерства цифрової трансформації України, країна займає передові позиції за рівнем застосування криптовалют серед населення, а українська спільнота блокчейн-розробників є однією з найбільших у світі. Це демонструє великий потенціал України в галузі цифрових технологій і криптовалют, а також підвищений інтерес до цього сектору серед громадян і підприємств.

Європол у своїх звітах неодноразово підкреслював серйозні ризики, пов'язані з використанням технології блокчейн, зокрема у контексті кримінальної діяльності. У звіті за 2020 рік Європол зазначив, що криптовалюти і блокчейн-технології стали популярними інструментами в організованій злочинності, що ставить під загрозу не лише безпеку окремих користувачів, а й стабільність фінансових систем.

Silk Road став однією з найбільш відомих і масштабних платформ для нелегальної торгівлі в Інтернеті, яка використовувала криптовалюту, зокрема Bitcoin, для анонімних фінансових транзакцій. На цьому ринку продавалися наркотики, зброя, підроблені документи та інші незаконні товари. Загальний обіг ринку дійсно становив мільйони доларів на рік, і його робота тривала до 2013 року, коли його закрили внаслідок операції ФБР [74].

Проте навіть після закриття Silk Road аналогічні платформи, які використовують криптовалюту для анонімних транзакцій, продовжують існувати. Вони дозволяють зловмисникам уникати традиційних методів відстеження, що ускладнює боротьбу з незаконними операціями в Інтернеті. Зокрема, такі платформи все ще популярні для торгівлі наркотиками, підробленими документами та іншими забороненими товарами.

Криптовалюта стала невід'ємною частиною сучасної фінансової системи та економіки, що спричинило необхідність її правового регулювання, а також чіткої класифікації в контексті кримінальних правопорушень. Оскільки криптовалюта активно використовується в різних сферах, зокрема для легальних фінансових операцій, так і для здійснення кримінальних діянь, визначення її правового статусу має важливе значення для ефективної боротьби з криптозлочинністю.

Криптозлочинність охоплює такі правопорушення, як відмивання грошей, фінансування тероризму, крадіжка криптовалюти, шахрайства та інші злочини, пов'язані з використанням анонімних криптовалютних платформ. Одним із ключових викликів для правозастосування є те, що технологія блокчейн, на якій базується криптовалюта, забезпечує високий рівень анонімності та прозорості одночасно. Відсутність централізованої системи зберігання даних та дистрибуція транзакцій серед багатьох користувачів ускладнює можливість відстеження і запобігання злочинам.

Відсутність чітких і всебічних правових норм щодо блокчейн-технологій та криптовалют значною мірою послаблює потенційні переваги цих інновацій і одночасно створює серйозні кримінологічні ризики. Блокчейн, незважаючи на свою прозорість та безпеку, без належного регулювання може використовуватися для нелегальних цілей.

Відсутність належного правового регулювання створює не лише правові, а й кримінологічні ризики, які можуть серйозно обмежити розвиток блокчейн-технологій та криптовалют в рамках легальних економічних систем. Важливо, щоб держави активно працювали над створенням

національних та міжнародних правових стандартів, які забезпечать баланс між захистом інтересів користувачів і державних інститутів та стимулюванням інновацій.

Криптовалюта має низку специфічних властивостей, які роблять її привабливою для використання в незаконних цілях, а її особливості можуть значно ускладнювати боротьбу з криптозлочинністю. Криміногенні властивості криптовалюти включають: анонімність, швидкість, дешеві та незворотні переклади; заплутані ланцюжки транзакцій; відсутність статусу криптовалюти, правил для бірж і пунктів обігу та ідентифікації власника криптовалютного гаманця; доступ з будь-якої точки світу через Інтернет; можливість для використання як «сховища» або здійснення міжнародних переказів грошових коштів; відносна безпека; можливість створення валют, повністю «заточених» під відмивання грошей; відсутність керівного органу.

Таким чином, ці особливості роблять криптовалюту потужним інструментом для злочинців, дозволяючи їм уникати традиційного фінансового контролю, що створює серйозні кримінологічні ризики. Тому питання правового регулювання та міжнародного співробітництва в боротьбі з криптозлочинністю стає все більш актуальним.

Фінансові моніторингові органи, зокрема Державна служба фінансового моніторингу України, акцентують увагу на зростаючих ризиках, пов'язаних з використанням криптовалют для відмивання грошей. Оскільки криптовалюти дозволяють здійснювати швидкі, анонімні та дешеві транзакції, це створює значні проблеми для фінансових установ, правоохоронних органів і спеціальних підрозділів, таких як фінансові розвідки.

Покращення правового регулювання криптовалют, удосконалення процедур ідентифікації учасників транзакцій, а також розвиток технологій для моніторингу криптовалютних операцій є ключовими напрямками для зменшення кримінологічних ризиків, пов'язаних із відмиванням грошей.

Використання криптовалют в протиправних фінансових схемах стало помітною тенденцією останніх років. Організовані злочинні угруповання активно використовують криптовалюти як інструмент для легалізації незаконно отриманих доходів, особливо якщо ці доходи були отримані в готівковій формі. Такий процес може включати кілька етапів, від приховування джерела коштів до їх легалізації через фінансові схеми.

Особливо поширеним є використання криптовалют у контексті шахрайства в сфері IT-технологій.

Таким чином, зростання випадків використання криптовалют у кримінальних фінансових схемах ставить перед державами і міжнародними організаціями важливі завдання з удосконалення правового та технічного моніторингу цієї нової сфери.

Відсутність правового статусу криптовалют в Україні, їх децентралізована природа та анонімність розрахунків створюють серйозні проблеми для контролю і регулювання цієї сфери. Водночас, ці фактори роблять криптовалюти ідеальним інструментом для організації злочинних схем, таких як шахрайства, відмивання грошей або фінансування нелегальних операцій.

Для зменшення цих ризиків Україні, як і багатьом іншим державам, потрібно впровадити чіткі правові рамки, що регулюють криптовалюти, а також розробити ефективні механізми для контролю за їх використанням, зокрема в боротьбі з фінансовими злочинами.

Ще один важливий аспект сучасної кримінальної економіки – відмивання грошей через онлайн-казино та інші азартні ігри. Цей метод використовується як для легалізації незаконних доходів, так і для усунення слідів злочинної діяльності. Справді, азартні ігри стали популярним каналом для таких схем, і, за деякими оцінками, саме через онлайн-казино відмивається велика частина «брудних» віртуальних грошей. Розглянемо основні чинники, які роблять ці сервіси привабливими для злочинців.

Сайти азартних ігор є важливим інструментом у схемах відмивання грошей, і для боротьби з цими явищами потрібно посилювати міжнародне співробітництво, розробляти нові правові та технічні механізми для контролю цієї сфери.

Використання ігрових валют як способу зберігання вартості криптовалюти стало ще одним інноваційним методом, який злочинці використовують для відмивання грошей та легалізації незаконно здобутих доходів. Це явище отримало популярність через ряд факторів, які роблять цей процес вигідним і менш помітним для правоохоронців.

Аналіз наукової літератури та судової практики дозволяє зробити висновок, що злочини, пов'язані з обігом криптовалюти, мають кілька характерних рис, що допомагають класифікувати їх як окрему категорію правопорушень. Виокремлені ознаки дають чітке розуміння специфіки цих злочинів і створюють основу для подальших досліджень та розробки правових підходів до їх кваліфікації та боротьби з ними.

Кримінальні правопорушення, що пов’язані з обігом криптовалют, мають три ключові ознаки:

1) електронна природа діянь, де криптовалюта виступає як предмет або спосіб вчинення кримінального правопорушення;

2) використання віртуальних мереж для здійснення правопорушень, що надає злочинцям анонімність і можливість уникати традиційного моніторингу;

3) мотив майнової та особистої вигоди, що є основною рушійною силою для більшості таких правопорушень.

Ці ознаки повинні враховуватись як під час кваліфікації таких кримінальних правопорушень, так і при розробці заходів для протидії кримінальним правопорушенням у цій сфері.

На сьогоднішній день спостерігається тенденція зростання кількості кримінальних правопорушень, пов'язаних із використанням криптовалют. Відзначається не лише кількісне збільшення таких злочинів, але й якісні

зміни в їх характері та складності. Це створює серйозні виклики для правоохоронних органів і судової системи, а також підкреслює необхідність адекватного правового регулювання цієї сфери [54].

Таким чином, зростання криптозлочинності та відсутність чіткої правової бази для регулювання криптовалют створюють серйозні ризики для економіки та безпеки країни. Необхідно розробити та прийняти законодавчі ініціативи, які б забезпечили чітке визначення правового статусу криптовалют та створення системи їх регулювання, що допоможе ефективно боротися з новими формами кримінальних правопорушень у цій сфері.

Питання про місце криптовалюти серед ознак складу кримінального правопорушення є складним і потребує детального аналізу, з огляду на специфіку цієї нової технології та її застосування у правовому полі. З кримінально-правової точки зору криптовалюта може мати різні статуси залежно від контексту вчиненого правопорушення.

З точки зору кримінального права, криптовалюта може бути визнана як засобом, так і предметом кримінального правопорушення в залежності від того, який саме злочин вчиняється. Вона може бути предметом правопорушення, якщо безпосередньо заволодівають криптовалютою, або засобом вчинення кримінального правопорушення, якщо використовується для проведення незаконних фінансових операцій. Водночас, вкрай важливо, щоб законодавство визначило чіткий правовий статус криптовалют, що дозволить правозастосовним органам правильно трактувати їх роль у складі кримінального правопорушення.

Зростання частки криптовалют у схемах відмивання грошей з 5% у 2015 році до понад 40% у 2018 році свідчить про необхідність вжиття більш ефективних заходів регулювання криптовалютного ринку. Важливо розробити механізми контролю за криптовалютними транзакціями, запровадити обов'язкову ідентифікацію учасників ринку, а також посилити міжнародну співпрацю для боротьби з фінансовими кримінальними правопорушеннями, пов'язаними з криптовалютами.

Злочинці використовують різні методи для легалізації протиправно здобутих коштів через криптовалюти завдяки анонімності, високій швидкості та мінімальному регулюванню ринку криптовалют. Ці способи легалізації коштів, такі як однорангові транзакції, використання криптомати, мікшерів, нелегальних обмінних сервісів та азартних онлайн-ігор, підкреслюють потребу в більш ефективному регулюванні криптовалютного ринку і посиленні міжнародної співпраці у боротьбі з фінансовими злочинами [54].

У 2017 році правоохоронці викрили міжрегіональну злочинну групу, яка незаконно заволодівала великими сумами грошей через обман та здійснювала їх легалізацію через криптовалюти.

Цей випадок демонструє, як використання криптовалют дозволяє кримінальним групам створювати складні схеми для легалізації коштів, отриманих злочинним шляхом. Тому виникає потреба у більш чітких і ефективних механізмах контролю за криптовалютними операціями, а також у посиленні міжнародної співпраці для боротьби з таким видом злочинності.

Влітку 2020 року кіберполіція викрила та припинила існування двадцяти незаконних онлайн обмінників. Цей випадок вказує на необхідність посилення контролю за криптовалютними операціями, зокрема через онлайн-обмінники та інші подібні сервіси, які не підлягають регулюванню. Крім того, варто зазначити, що існуюча анонімність та відсутність чіткої правової регламентації створюють численні можливості для використання криптовалют у кримінальних цілях, зокрема у кіберзлочинності та відмиванні грошей. Тому важливими є не лише внутрішні механізми контролю, а й міжнародна співпраця для виявлення та ліквідації таких незаконних мереж [54].

Отже, на нашу думку, визнання криптовалюти предметом кримінальних правопорушень, зокрема у випадках кримінальних правопрушень проти власності, є необхідним кроком для забезпечення належної кримінально-правової оцінки цих злочинів. Це не лише дозволить правоохоронним органам більш ефективно протидіяти використанню

криптовалют у кримінальних схемах, а й створить підґрунтя для належного правового регулювання цього швидко зростаючого сектора економіки.

3.2. Зарубіжний досвід доказування у справах про шахрайство, вчинене з використанням цифрових технологій

Кіберзлочинність, включаючи шахрайство, що здійснюються через Інтернет, є глобальною проблемою, що вимагає координації між різними країнами для забезпечення ефективного розслідування та притягнення винних до відповідальності.

Для ефективної протидії інтернет-шахрайствам необхідна гармонізація національних законодавств із міжнародними стандартами, створення спільних механізмів співпраці між країнами, а також розробка чітких стандартів для роботи з електронними доказами. Система комплексної боротьби, яка включає як законодавчі, так і практичні заходи, стане важливим кроком до зменшення глобального рівня інтернет-шахрайств [61; 162].

Вивчення досвіду зарубіжних країн, які успішно протидіють шахрайствам у сфері електронної комерції, є важливим етапом у вдосконаленні національної практики боротьби з кіберзлочинністю. Досвід таких країн може допомогти виявити ефективні стратегії, механізми розслідування та правове регулювання, які можна адаптувати до умов України. Вивчення досвіду розвинутих зарубіжних країн у боротьбі з інтернет-шахрайствами та його адаптація в національному законодавстві може стати важливим кроком для підвищення ефективності розслідування таких злочинів в Україні. Спільні міжнародні зусилля, вдосконалення правових механізмів і технічних засобів допоможуть ефективно реагувати на зростаючу проблему кіберзлочинності у сфері е-комерції [133, с. 33]. О. І. Кривенко підкреслює, що однією з найбільших проблем у боротьбі з інтернет-шахрайствами є значні відмінності в підходах до цієї проблеми в

різних країнах. Ці відмінності можуть бути спричинені різними правовими системами, рівнем технологічного розвитку, законодавчими нормами та інституційними можливостями. Тому для ефективної боротьби з інтернет-шахрайствами необхідно враховувати ці відмінності та адаптувати стратегії національного законодавства, правоохоронної діяльності та міжнародної співпраці до конкретних умов кожної країни. Гармонізація міжнародних норм і взаємодія між державами з питання боротьби з кіберзлочинністю допоможе створити більш ефективну систему захисту від інтернет-шахрайств на глобальному рівні [87, с. 210].

Досвід США у боротьбі з шахрайствами в сфері електронної комерції є важливим прикладом для розробки універсальних механізмів запобігання кримінальним правопорушенням у цій галузі. США активно займаються розробкою комплексних стратегій та механізмів для протидії шахрайствам в інтернеті, зокрема у сфері е-комерції, що дозволяє забезпечити ефективну боротьбу з шахрайськими схемами, захистити споживачів і підтримувати довіру до електронних торгових платформ. Наслідування американського досвіду в боротьбі з шахрайством в е-комерції дозволяє створити ефективну модель для запобігання кримінальним правопорушенням у цій сфері. Важливо, щоб країни, які прагнуть підвищити рівень кібербезпеки, адаптували ці підходи відповідно до своїх національних потреб, законодавчих особливостей і технологічних можливостей [79, с. 221]. Система протидії інтернет-шахрайствам у США, зокрема через Федеральне бюро розслідувань (ФБР) та створений в його складі Центр скарг на інтернет-злочинність (IC3), є ефективним прикладом того, як держава може організувати боротьбу з кіберзлочинністю. Цей центр відіграє ключову роль у зборі та обробці скарг про інтернет-шахрайства, надаючи жертвам злочинів можливість повідомляти про порушення через онлайн-форму. Система, організована ФБР США через Центр скарг на інтернет-злочинність, є ефективним інструментом для боротьби з інтернет-шахрайствами. Вона забезпечує громадянам доступ до подачі скарг, надає їм важливу інформацію

для захисту від шахраїв і є важливою складовою національної стратегії у боротьбі з кіберзлочинністю. Цей досвід може бути корисним для країн, які прагнуть удосконалити свою систему реагування на інтернет-злочини та захисту прав громадян у кіберпросторі [87].

У США була створена ефективна система протидії шахрайствам в електронній комерції завдяки спільній роботі правоохоронців, представників бізнесу, громадськості та науковців. У результаті цієї співпраці були розроблені конкретні превентивні заходи, що дозволяють мінімізувати ризики шахрайства в інтернет-торгівлі та підвищити рівень безпеки онлайн-платформ. Види превентивних заходів, що мінімізують ризики шахрайства:

1) регулярний аудит безпеки сайту;

2) перевірка відповідності стандарту PCI DSS. Цей стандарт регулює обробку платіжних карток і є обов'язковим для забезпечення захисту даних платіжних карток від шахрайства. Всі інтернет-магазини, які обробляють платежі картками, повинні відповідати вимогам PCI DSS;

3) перевірка підозрілої активності;

4) використання служби перевірки адрес (AVS). Система AVS перевіряє, чи збігається адреса виставлення рахунку клієнта з адресою власника картки. Це є частиною багатошарового захисту від шахрайства, що допомагає блокувати підозрілі транзакції;

5) використання CVV2 та CVC2 кодів. Ці захисні коди на платіжних картках додають додатковий рівень захисту. Банк використовує ці коди для підтвердження ідентичності клієнта під час онлайн-платежів;

6) використання протоколу HTTPS. Протокол HTTPS забезпечує цілісність і конфіденційність даних під час їх передачі між веб-сайтом і користувачем. Це забезпечує три основні рівні захисту: шифрування даних, їх цілісність і аутентифікацію сайту;

7) зберігання обмеженої кількості інформації;

8) обмеження на покупки з одного облікового запису;

9) перевірка збігу IP-адреси та адреси картки;

10) використання програм для боротьби з шахрайством.

Система превентивних заходів для захисту інтернет-магазинів від шахрайств у США є прикладом ефективної боротьби з кіберзлочинністю в електронній комерції. Вона включає використання передових технологій і інтеграцію з аналітичними платформами для моніторингу та виявлення шахрайських дій. Така практика є важливим елементом для забезпечення безпеки користувачів та підвищення довіри до онлайн-торгівлі [79, с. 222].

Боротьба з фішингом у США є важливим елементом у протидії кіберзлочинності та захисту прав споживачів. Позитивний досвід США в цьому напрямі може слугувати прикладом для інших країн, зокрема й для України.

У США для боротьби з фішингом створено різноманітні програми та заходи, включаючи активне співробітництво з бізнес-сектором та державними установами, а також застосування спеціалізованих технологій для виявлення фішингових атак. Одним із важливих інструментів є система реагування на інтернет-злочинність, що дозволяє користувачам повідомляти про фішингові сайти та інші кіберзагрози.

В Україні, у свою чергу, за підтримки Державного департаменту США, реалізується Національна програма сприяння безпеці електронних платежів і карткових розрахунків Safe Card, що сприяє підвищенню рівня захисту онлайн-платежів і боротьбі з шахрайством, включаючи фішинг.

У рамках цієї програми Українська міжбанківська асоціація членів платіжних систем ЕМА запустила проєкт, спрямований на ліквідацію шахрайських сайтів. Основна мета проекту – виявлення і блокування фішингових ресурсів, які використовуються для крадіжки особистих даних користувачів та їх фінансових коштів. Завдяки цьому проекту, Україна також має можливість зміцнити свою боротьбу з фішингом, надаючи користувачам інструменти для захисту від шахраїв, а також стимулюючи бізнес-сектор до впровадження безпечних платіжних систем. Успіх цього проекту є важливим кроком для підвищення довіри до електронних платіжних систем і

забезпечення безпеки фінансових транзакцій в країні [122; 40, с. 94; 154, с. 216-220]. Так, США вважаються однією з найбільш постраждалих країн від кібершахрайств, що ставить їх на передову у розробці та впровадженні відповідних норм та стратегій для боротьби з кіберзлочинністю.

У 2015 році США прийняли Національну стратегію кібербезпеки, яка визначила кібербезпеку як ключову складову національної безпеки. Ця стратегія включає ряд важливих норм і заходів, спрямованих на захист від кібератак, які можуть мати серйозні наслідки для державних, приватних та громадських структур. Важливим аспектом цієї стратегії є те, що США не лише відповідають за захист власних інтересів, а й прагнуть бути лідером у забезпеченні кібербезпеки на міжнародному рівні, оскільки багато сучасних кібератак мають глобальний характер і не обмежуються територією однієї країни.

Ця стратегія має значний вплив на регулювання інтернет-бізнесу і встановлення правил боротьби з кіберзлочинністю, зокрема фішингом, шкідливим програмним забезпеченням та іншими видами кібератак. США, фактично, виступають як основний центр розвитку міжнародної політики в галузі кібербезпеки [130, с. 45].

Згідно з дослідженням досвіду США щодо запобігання шахрайству в сфері електронної комерції, ряд вчених в Україні вже виділяють кілька ключових завдань, які мають бути реалізовані для ефективної боротьби з електронним комерційним шахрайством. Зокрема, це:

1. Створення Єдиної інформаційної системи профілактики шахрайства. Це передбачає об'єднання різноманітних інформаційних ресурсів, платформ і баз даних, що містять відомості про шахраїв, їх схеми та методи роботи. Така система дозволить забезпечити швидкий доступ до інформації для всіх учасників ринку та правоохоронних органів, а також значно підвищить ефективність боротьби з шахрайством.

2. Запровадження політики належного корпоративного управління. Важливою є створення чітких внутрішніх стандартів для електронної

комерції, які включатимуть запобігання шахрайству, захист прав споживачів та забезпечення безпеки транзакцій. Це включає моніторинг та контроль за діяльністю онлайн-магазинів і платформ, щоб мінімізувати ризики шахрайських дій.

3. Впровадження дієвих законодавчих ініціатив. Окремо потрібно створювати закони, які регулюють комерційну рекламу та просування товарів і послуг, щоб запобігти використанню шахрайських методів для заманювання клієнтів. Крім того, важливе питання кримінальної відповідальності за правопорушення, пов'язані з порушенням кібербезпеки, включаючи крадіжку даних, злом мереж і знищення приватної інформації.

4. Реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство. Потрібно оновити кримінальне законодавство, щоб забезпечити відповідальність за нові типи злочинів, пов'язаних з електронною комерцією, і адаптувати його до викликів цифрового середовища.

5. Використання новітніх електронних систем і досягнень штучного інтелекту. Впровадження інтелектуальних систем для моніторингу транзакцій і виявлення підозрілих операцій на основі алгоритмів машинного навчання стане важливим інструментом для боротьби з шахрайством в електронній комерції.

6. Популяризація електронної комерції через онлайн та офлайн магазини. Для збільшення довіри до електронної комерції і її розвитку важливо популяризувати онлайн-шопінг серед населення, а також створювати відповідні інструменти для захисту споживачів.

7. Посилення міжнародного співробітництва і залучення громадськості. Важливо налагоджувати співпрацю між державами для боротьби з міжнародним електронним шахрайством. Також варто активно залучати громадські організації до інформаційно-просвітницької роботи з попередження шахрайства в інтернеті.

Ці завдання відображають потребу в комплексному підході до протидії електронному шахрайству, що включає не тільки юридичні і технічні рішення, а й активну участь держави, бізнесу та громадян у забезпеченні безпеки в цифровому середовищі [79, с. 222].

Серед європейських держав Великобританія та Франція займають лідируючі позиції за масштабами фінансового шахрайства. Вони стикаються з найбільшими збитками через шахрайство внаслідок розвитку технологій, зокрема, в Інтернеті та електронній комерції. Обидві країни впроваджують різноманітні ініціативи, включаючи підвищення рівня обізнаності серед громадян, посилення контролю за фінансовими транзакціями, а також співпрацю з міжнародними правоохоронними органами для боротьби з кібершахрайством та фінансовими злочинами в межах ЄС та глобально [42]. Досвід Великобританії, Франції та інших європейських держав, які успішно справляються з кібершахрайством, зокрема в сфері е-комерції, може бути дуже корисним для впровадження подібних заходів у країнах, які лише починають серйозно розглядати проблему інтернет-шахрайств.

Створення спеціалізованих органів для боротьби з кіберзлочинністю є важливим кроком у забезпеченні національної безпеки в цифрову епоху. Такі органи виконують низку важливих функцій, серед яких формування національної політики щодо кібербезпеки, реалізація практичних заходів із захисту від кіберзагроз, розслідування кіберзлочинів і співпраця з міжнародними організаціями.

Зазначені органи відіграють ключову роль у національних системах кібербезпеки:

Фінляндія: Комітет з питань безпеки країни відповідає за координацію та розвиток політики в області кібербезпеки, зокрема захист національних інтересів у кіберпросторі, а також підтримує інтеграцію технологічних інновацій з метою забезпечення кібербезпеки на рівні держави.

Великобританія: Центр захисту національної інфраструктури Великобританії, разом з Управлінням кібербезпеки та інформаційного

забезпечення, відповідає за запобігання загрозам для критично важливих секторів економіки, включаючи енергетику, фінанси та телекомунікації. Вони забезпечують ефективне реагування на кіберінциденти та захист національної інфраструктури.

Чехія: Управління національної безпеки активно займається формуванням політики в сфері кіберзахисту і сприяє розвитку національної стратегії кібербезпеки. Вони також мають на меті забезпечення стійкості до кіберзагроз для державних установ та приватного сектору.

Польща: Міністерство адміністрації та впровадження цифрових технологій відповідає за розробку та впровадження національної стратегії з кібербезпеки, сприяючи забезпеченню захисту інформаційних систем і цифрових інфраструктур, а також підтримуючи розвиток новітніх технологій для боротьби з кіберзлочинністю.

Франція: Національна служба безпеки інформаційних технологій у Франції є головним органом для забезпечення кібербезпеки в державі. Вона займається захистом інформаційної інфраструктури, а також координацією дій з іншими міжнародними та національними органами для боротьби з кіберзагрозами.

Австрія: Керівна група з кібербезпеки в Австрії фокусується на стратегічному плануванні і координації політики в області кібербезпеки, сприяючи розвитку законодавства, яке дозволяє швидко реагувати на нові кіберзагрози.

Роль цих органів можна оцінити як критично важливу для розробки ефективної національної стратегії захисту від кіберзлочинності, яка включає:

Формування та реалізацію політики кібербезпеки на рівні держави.

Забезпечення співпраці між державними і приватними структурами, що дозволяє створювати єдину систему захисту від кіберзагроз.

Розробку та вдосконалення законодавства щодо боротьби з кіберзлочинністю, яке враховує сучасні виклики.

Реалізацію міжнародного співробітництва для боротьби з транснаціональними кіберзлочинами, таких як хакерські атаки та кібертероризм [131, с. 56].

Ми вважаємо, що створення подібних органів в Україні може значно посилити захист від кіберзлочинності, зокрема в рамках е-комерції, та допомогти інтегрувати національні заходи в міжнародні структури для боротьби з кіберзагрозами.

Аналіз міжнародного досвіду, зокрема в контексті Європейського Союзу, свідчить про важливість раннього виявлення та 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 і забезпеченню захисту інформаційних ресурсів.

Ключові органи та інструменти кіберзахисту в ЄС:

1. Стратегія кібербезпеки Європейського Союзу. Стратегія надає особливу увагу виявленню та блокуванню кібератак, а також локалізації їх наслідків. Важливо, що стратегію застосовують не лише до державних або військових об'єктів, але й до цивільних об'єктів усіх форм власності, що підвищує рівень захисту критичної інфраструктури в Європі.

2. Європейська агенція мережевої та інформаційної безпеки (ENISA). ENISA відіграє важливу роль у забезпеченні кіберзахисту через розробку та просування кращих практик для виявлення кібератак та реагування на них. Агентство також надає підтримку країнам ЄС у розвитку національних стратегій кібербезпеки.

3. CERT-EU (Computer Emergency Response Team). CERT-EU є основним інструментом для оперативного виявлення кіберзагроз в рамках ЄС. Використовуючи спеціалізовані технологічні системи датчиків, які встановлюються на серверах і абонентських лініях, CERT-EU здатний швидко виявляти атаки та негайно реагувати на них. У разі виявлення кіберзлочинів, інформація передається для подальшого розслідування.

4. Європейський центр з розслідування кіберзлочинів (EC3). Якщо CERT-EU виявляє кібератаки з ознаками злочинної діяльності, інформація передається до Європейського центру з розслідування кіберзлочинів (EC3), що займається глибшим аналізом інцидентів та взаємодією з іншими правоохоронними органами для розслідування кіберзлочинів.

5. Європейська агенція оборони (EDA) та Європейська служба зовнішніх справ (EEAS). У разі серйозних кіберінцидентів, що можуть мати геополітичні наслідки, Європейська агенція оборони та Європейська служба зовнішніх справ можуть бути залучені до організації кібероперацій або дипломатичних заходів, спрямованих на вирішення проблеми кібербезпеки на рівні ЄС.

Досвід ЄС демонструє важливість інтегрованої та скоординованої системи для виявлення і реагування на кіберзагрози. Україна може розглянути можливість створення подібних органів і технологій для оперативного реагування на кіберінциденти, а також активної міжнародної співпраці для боротьби з кіберзлочинністю, зокрема в контексті електронної комерції та критичних інфраструктур [196, с. 388].

На нашу думку, ключовими елементами системи кіберзахисту в ЄС є:

- інтеграція технологій та координація між органами. Взаємодія між різними агентствами, такими як ENISA, CERT-EU, EC3, дозволяє швидко реагувати на інциденти і ефективно розслідувати кіберзлочини;
- оперативне реагування. Виявлення і 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 кіберзлочинності на глобальному рівні.

Поширення криптовалют, таких як біткоїн та Monero, є одним із основних викликів для боротьби з кіберзлочинністю в Європейському Союзі. Анонімність криптовалют дозволяє зловмисникам використовувати їх для

фінансування незаконної діяльності, включаючи кіберзлочинність, таку як придбання інструментів для хакерських атак або оплата за нелегальні послуги в онлайн-просторі.

Біткоїн і інші криптовалюти, орієнтовані на анонімність (як Monero), забезпечують кіберзлочинцям високий рівень конфіденційності, що ускладнює їх відстеження і контроль. Ці валюти використовуються для різних нелегальних транзакцій, що ускладнює боротьбу з кіберзлочинністю в Інтернеті.

Окрім цього, криптовалюти дозволяють злочинцям обходити традиційні фінансові системи і правові механізми, що значно ускладнює процеси відстеження і конфіскації незаконно отриманих коштів.

Кроки ЄС для вирішення цієї проблеми:

- партнерства з криптовалютними біржами. Це дозволяє забезпечити прозорість і контроль за транзакціями, а також розробити ефективні механізми для виявлення підозрілих операцій.

- щорічна конференція з віртуальних валют. Це дозволяє обговорювати останні тенденції та обмінюватися досвідом з іншими державами і міжнародними організаціями.

- Законопроект MiCA (Markets in Crypto Assets). Важливим кроком на шляху до вирішення цієї проблеми є прийняття законодавства, яке регулює криптовалюти. Законопроект MiCA, прийнятий Європейським Союзом, визначає чіткі правила для всіх постачальників послуг криптоактивів, зокрема вимоги щодо захисту споживачів, вимоги до прозорості та відповідальності за транзакції. Законопроект також зобов'язує криптобіржі та інші учасники ринку дотримуватись норм, що дозволяють запобігати використанню криптовалют для фінансування незаконної діяльності.

- підтримка країн ЄС. Законопроект MiCA отримав широку підтримку серед країн-членів ЄС, зокрема Франції, що підкреслює важливість узгоджених дій на європейському рівні для ефективного регулювання і боротьби з ризиками, пов'язаними з криптовалютами [36, с. 113].

З огляду на все більшу роль криптовалют у сучасній кіберзлочинності, на нашу думку, важливим є впровадження комплексних заходів, що включають як регулювання криптовалют, так і співпрацю з міжнародними партнерами. ЄС, як показує його досвід, активно розробляє політику, спрямовану на зниження ризиків, пов'язаних з анонімними транзакціями, забезпечуючи водночас прозорість і контроль за фінансовими операціями в цифровому просторі.

Франція орієнтується на посилення кіберзахисту як ключовий аспект своєї національної безпеки. У країні активно розробляються і впроваджуються стратегії, спрямовані на протидію кіберзлочинності та забезпечення безпеки інформаційних систем, робиться акцент на комплексному підході до кіберзахисту, поєднуючи технічні рішення, боротьбу з кіберзлочинністю та стратегічне управління для забезпечення безпеки інформаційних систем. Важливим кроком у цьому напрямку є розвиток національних та міжнародних ініціатив, що дозволяють знижувати рівень кіберзагроз та забезпечувати кібербезпеку на всіх рівнях. [131, с. 56].

Німеччина демонструє високу зацікавленість у забезпеченні стабільності бізнесу та національної безпеки, що видно з її підходів до контролю за економічно важливими об'єктами та захисту від зовнішніх і внутрішніх загроз.

Наприклад, Уряд Німеччини створив спеціалізовані органи для забезпечення стабільності та безпеки в економічному секторі. Це включає в себе органи, що займаються контролем за об'єктами критичної інфраструктури, особливо в таких галузях, як енергетика, комунікації та фінансовий сектор. Завдання цих служб полягає у забезпеченні безпеки національних інтересів, зокрема, захисту від шкідливих іноземних впливів, кіберзагроз і економічного шпигунства.

У відповідь на потенційні загрози з боку іноземних спецслужб, Німеччина створила контррозвідувальні підрозділи, які працюють у тісній взаємодії з приватними охоронними та детективними агентствами. Ці

підрозділи виконують важливу роль у захисті бізнесу, керівництва компаній та працівників, а також забезпечують захист клієнтів від економічних та інтелектуальних загроз. Вони зосереджуються на зборі інформації про можливі правопорушення, що можуть вплинути на компанії та національну безпеку.

Німеччина активно співпрацює з приватними охоронними компаніями, які інколи виконують функції, що можуть бути еквівалентними оперативно-розшуковій діяльності. Це включає в себе збір оперативно-важливої інформації про злочини, які були скоєні чи готуються на рівні компаній або держави в цілому. Такі заходи дозволяють оперативно реагувати на потенційні загрози, однак в Україні це зазвичай є забороненим, оскільки відповідні функції мають виконувати лише правоохоронні органи.

В Німеччині існує культура громадянської відповідальності, що включає поінформованість населення про можливі правопорушення. Громадяни, які надають інформацію про злочини, можуть отримати винагороду, розмір якої може сягати значних сум, інколи більше ніж сто тисяч євро. Це заохочує населення активно співпрацювати з правоохоронними органами та надавати важливу інформацію для запобігання злочинам і кіберзагрозам.

Загалом, Німеччина застосовує комплексний підхід до забезпечення економічної безпеки, комбінуючи роботу державних спецслужб з приватними агентствами для ефективного моніторингу і захисту від внутрішніх та зовнішніх загроз. Така модель включає в себе не лише технічні та правові заходи, але й активну участь громадян у забезпеченні національної безпеки, що є важливим елементом стабільності та розвитку економічних відносин [133, с. 38].

Транснаціональна злочинність, зокрема у Європейському Союзі, набуває нових форм і взаємодій, що включають тісні зв'язки з корпоративним сектором. Транснаціональна злочинність, зокрема у сфері кіберзлочинності, має значний вплив на бізнес-сектор в країнах ЄС. Злочинні угруповання

активно використовують сучасні технології для досягнення своїх цілей, включаючи крадіжку інтелектуальної власності, відмивання грошей і маніпулювання персональними даними користувачів. Це створює серйозні ризики для стабільності та безпеки цифрових економік, і вимагає розробки нових стратегій для протидії таким загрозам [32, с. 300].

Залучення зовнішніх форензік-експертів для розслідування випадків шахрайства є усталеною практикою в міжнародних організаціях, оскільки ці фахівці мають необхідні навички та інструменти для ефективного аналізу складних ситуацій, виявлення шахрайських схем і розробки стратегій їхнього попередження та ліквідації наслідків.

В Україні ж ситуація виглядає інакше. За даними досліджень, лише 3% організацій в Україні використовували зовнішніх експертів для аналізу випадків шахрайства за останні два роки. Це значно нижчий показник, ніж у світі, де 20% респондентів мали такий досвід. Більшість українських компаній зосереджуються лише на реакції на вже скоєні шахрайства, замість того щоб вживати профілактичні заходи для їх запобігання.

Такий підхід створює ризики для організацій, оскільки вони не мають змоги вчасно виявляти та блокувати потенційні шахрайські схеми до того, як вони призведуть до серйозних фінансових або репутаційних збитків. Проблема ще більше загострюється через відсутність спеціалізованих інструментів або інвестування в кібербезпеку та технології, які допомагають виявляти шахрайські дії на ранніх етапах [43].

Ми вважаємо, що для зміни ситуації в Україні необхідно:

- розвивати культуру профілактики шахрайства, забезпечуючи постійну підготовку та навчання співробітників організацій.

- Інвестувати у спеціалізовані технології для виявлення шахрайства, такі як програми для моніторингу транзакцій, аналізу поведінки користувачів та використання машинного навчання для виявлення аномалій.

- Залучати зовнішніх експертів для проведення аудитів і розслідувань, що дозволить виявити можливі слабкі місця в захисті і покращити системи безпеки.

- Розвивати законодавчу та нормативну базу, що регулює боротьбу з шахрайством, включаючи посилення відповідальності за шахрайські дії в Інтернеті.

Ці заходи допоможуть знизити ризики шахрайства та підвищити ефективність боротьби з ним в Україні, наближаючи країну до міжнародних стандартів.

Головною відмінністю між практиками протидії шахрайствам через Інтернет в Україні та в країнах Європейського Союзу і США є акцент на превентивних заходах та освітній роботі з населенням, а не лише на розслідуванні вже скоєних злочинів.

У країнах ЄС та США значно більша увага приділяється запобіганню шахрайству. Натомість в Україні, хоча і відбувається певне зростання у цій сфері, більшість зусиль зосереджено на реактивних заходах — тобто, вже після того, як шахрайство було вчинено. Існує необхідність у розвитку превентивних механізмів, більш активному використанні технологій і створенні системи безпеки, орієнтованої на виявлення та запобігання шахрайським діям до того, як вони стануть серйозною проблемою.

Таким чином, для підвищення ефективності боротьби з інтернет-шахрайством в Україні важливо не лише покращити методи розслідування вже скоєних злочинів, а й значно посилити профілактику, інформаційну освіту громадян та співпрацю з міжнародними партнерами [87, с. 210].

Як зазначають Н. А. Лугіна і А. М. Лучук, ефективне розслідування кримінальних правопорушень, пов’язаних з віртуальним простором, вимагає не лише гармонізації законодавства, а й розробки міжнародних механізмів співпраці. Для досягнення ефективності в боротьбі з кіберзлочинністю важливо забезпечити гармонізацію законодавства, посилити міжнародну

співпрацю, а також розробити сучасні інструменти для дослідження та розслідування правопорушень у віртуальному просторі [105, с. 239].

К. С. Качашвілі підкреслює важливість міжнародної співпраці для боротьби з інтернет-шахрайством. Дійсно, через глобальну природу кіберзлочинності та її безперервну еволюцію, розв'язання цієї проблеми на рівні окремих держав є майже неможливим. Тому важливою умовою для ефективної боротьби з кіберзлочинністю є:

- Міжнародні норми та стандарти. Як вказує Качашвілі, необхідність прийняття міжнародних норм і стандартів для боротьби з інтернет-шахрайством є критично важливою. Це дозволяє створити єдині правові підходи до вирішення проблеми в межах міжнародної спільноти. Важливим кроком у цьому напрямку є вже згадана Будапештська конвенція Ради Європи, яка надає основи для боротьби з кіберзлочинністю і регулювання кібербезпеки на міжнародному рівні.

- Гармонізація національних законодавств. Внесення змін до національних законодавств відповідно до міжнародних стандартів є необхідним для того, щоб країни могли ефективно співпрацювати між собою в боротьбі з інтернет-шахрайством. Гармонізація національних законодавств забезпечує єдиний підхід до покарання кіберзлочинців та забезпечує можливість їх екстрадиції, а також вирішення питань з міжнародним правопорушенням.

- Розробка комплексної програми боротьби. Пропозиція щодо розробки комплексної програми на міжнародному рівні, яка б включала всі можливі форми та методи боротьби з інтернет-шахрайством, є дуже важливою. Така програма може бути створена в рамках міжнародних організацій, зокрема, ООН, з включенням правових, технічних і організаційних аспектів боротьби з кіберзлочинністю. Це повинно включати як законодавчі ініціативи, так і стратегії навчання, профілактики та обміну інформацією.

- Система постійного моніторингу. Важливою умовою для ефективності цієї боротьби є система постійного моніторингу інтернет-

простору на міжнародному та національному рівнях. Це дозволяє виявляти шахрайські схеми на ранніх стадіях та оперативно реагувати на нові загрози. Такий моніторинг включає в себе використання новітніх технологій, аналіз поведінки користувачів, а також обмін інформацією між різними державами та міжнародними організаціями.

- Паралельні заходи правоохоронних органів. Для досягнення ефективних результатів необхідно, щоб правоохоронні органи всіх держав паралельно здійснювали заходи по припиненню та попередженню шахрайства. Це включає у себе і активну роботу з виявлення та затримання кіберзлочинців, і проведення заходів з обізнаності серед громадян, а також створення технічних засобів захисту для бізнесу та індивідуальних користувачів.

Для успішної боротьби з інтернет-шахрайством необхідна координація зусиль на міжнародному рівні між державами, міжнародними організаціями та бізнесом, а також наявність чітких механізмів для виявлення та реагування на кіберзлочини [61, с. 131].

Важливість поглиблення практичного міжнародного співробітництва в боротьбі з кіберзлочинністю, зокрема з кібершахрайством, через оперативний обмін інформацією. Враховуючи глобальний характер цієї проблеми, ефективна боротьба з кіберзлочинністю вимагає тісної співпраці між державами, правоохоронними органами та міжнародними організаціями.

Важливими аспектами, які потрібно враховувати для підвищення ефективності боротьби з кіберзлочинністю на міжнародному рівні:

1. Оперативний обмін інформацією. Для цього потрібні ефективні механізми комунікації та швидкої передачі даних про кіберзлочини, зокрема про многоепізодні кібершахрайства. Такі обміни інформацією дозволяють оперативно виявляти кримінально протиправні схеми, що переховуються на міжнародному рівні, а також відслідковувати розвиток нових загроз.

2. Угоди про видачу кібершахраїв. Для боротьби з кіберзлочинністю необхідно укладати угоди про видачу кібершахраїв, що дозволяють країнам,

де вчинені злочини, екстрадувати осіб, підозрюваних у кіберзлочинах, до країн, де їх можуть судити згідно з національним законодавством. Такі угоди допомагають забезпечити відповідальність зловмисників, які можуть ховатися за кордоном.

3. Взаємна правова допомога та консультації. Важливим аспектом є також надання взаємної правової допомоги і консультацій із роз'ясненнями щодо норм та кваліфікуючих ознак кримінальних правопорушень за національним законодавством. Це допомагає правоохоронним органам різних країн правильно кваліфікувати злочини і проводити розслідування, навіть якщо злочинці діють через кордони.

4. Імплементація та гармонізація міжнародного законодавства. Необхідно активно імплементувати та гармонізувати міжнародне законодавство з національними законами. У цьому контексті важливо, щоб країни мали спільні стандарти, які дозволяють ефективно реагувати на кіберзлочини. Це включає в себе стандарти щодо захисту інформації, криміналізації кіберзлочинів, а також забезпечення швидкого та ефективного правосуддя для жертв кіберзлочинів.

5. Активізація обміну інформацією між оперативними підрозділами. Як зауважує С. В. Шапочка, особливо важливим є обмін інформацією між оперативними підрозділами різних країн про багатоепізодні кібершахрайства. Це дозволяє правоохоронцям отримувати важливу інформацію про кіберзлочини, що вже сталися, і про ті, які готуються. Завдяки цьому можна запобігти можливим злочинам і зупиняти кіберзлочинців до того, як вони завдадуть шкоди.

6. Роль України в гармонізації законодавства. Для України важливим кроком є імплементація міжнародних стандартів та гармонізація законодавства в галузі інформаційної безпеки та боротьби з кіберзлочинністю. Це включає в себе і прийняття нових законів, які забезпечують ефективний захист від кіберзлочинців, і співпрацю з

міжнародними організаціями, такими як Інтерпол, Європейський Союз, ООН та інші [189, с. 189].

Таким чином, ефективне розслідування кіберзлочинів потребує розробки комплексних механізмів міжнародного співробітництва, що включають оперативний обмін інформацією, правову допомогу, угоди про видачу злочинців та гармонізацію законодавства. Тільки за умов тісної співпраці між державами та міжнародними організаціями можна досягти значного прогресу в боротьбі з кібершахрайством і забезпеченні безпеки в інформаційному просторі.

Слід підкреслети важливість Конвенції про кіберзлочинність, яка є основною міжнародною угодою, що регулює співпрацю країн у боротьбі з кіберзлочинністю, включаючи кібершахрайства у сфері е-комерції. Зокрема, Конвенція була розроблена Радою Європи і підписана понад 50 країнами, серед яких і США. Вона створює юридичну основу для міжнародної співпраці в галузі кібербезпеки та боротьби з кіберзлочинністю, дозволяючи країнам узгоджувати свої зусилля на глобальному рівні. ратифікація та виконання Конвенції ЄС є важливим кроком для України в напрямку гармонізації національного законодавства з міжнародними стандартами в сфері кібербезпеки та міжнародної співпраці у боротьбі з кіберзлочинністю. Це дозволить зменшити ризики кіберзлочинів, зокрема шахрайства в онлайн-середовищі, і створить основи для більш ефективної протидії таким загрозам на міжнародному рівні [168, с. 170].

Універсальні міжнародно-правові документи, що сприяють боротьбі з кіберзлочинністю, є вкрай важливою для розуміння міжнародної правової бази цієї проблеми. Важливі документи, які допомагають вирішувати питання кібербезпеки та кіберзлочинності на глобальному рівні, включають:

1. Довідник ООН із запобігання і контролю злочинності, пов’язаної з комп’ютерами (1995 рік). Цей документ надає рекомендації та стратегії для країн щодо запобігання та боротьби з комп’ютерною злочинністю, надаючи основу для розробки національних законодавств у цій сфері.

2. Конвенція ООН проти транснаціональної організованої злочинності (2000 рік). Ця Конвенція також охоплює злочини, пов’язані з кіберпростором, і встановлює основи для міжнародної співпраці у боротьбі з транснаціональними кіберзлочинами, такими як кібертероризм, шахрайство, фальсифікація даних тощо [76].

3. «Мінімальний список» правопорушень у сфері кіберзлочинності (1990 рік), прийнятий Європейським комітетом з проблем злочинності Ради Європи.

4. Інтерпол і міжнародна кримінальна поліція. Інтерпол зі своїм кодифікатором міжнародної кримінальної поліції, який був інтегрований у автоматизовану систему пошуку з 1991 року, відіграє важливу роль у координації діяльності правоохоронних органів різних країн. Це дозволяє обмінюватися інформацією про міжнародні кіберзлочини, зокрема, через Національні центральні бюро Інтерполу в більшості країн, у тому числі й в Україні. Важливою частиною цього процесу є своєчасне виявлення кіберзлочинців і оперативне реагування на кібератаки чи інші види кіберзлочинів.

Різні міжнародні документи створюють основу для гармонізації національних законодавств щодо кіберзлочинності та сприяють ефективному міжнародному співробітництву між державами.

Зміни в класифікації кіберзлочинів, а також створення таких систем як Інтерпол для обміну інформацією між країнами, дозволяють значно покращити координацію та ефективність боротьби з кіберзлочинністю.

Необхідність міжнародної гармонізації законодавства, особливо в галузі боротьби з кіберзлочинністю, є важливою складовою забезпечення глобальної кібербезпеки.

Ці заходи дозволяють не лише ефективно реагувати на кіберзлочини, але й запобігати їм на міжнародному рівні, що вимагає постійної співпраці та інтеграції нових технологічних рішень у правову систему [155, с. 388].

Україна активно бере участь у міжнародному співробітництві в рамках європейських та міжнародних проектів, зокрема щодо боротьби з кіберзлочинністю. Це співробітництво включає численні програми, ініціативи та партнерства з ключовими організаціями, що забезпечують платформу для обміну інформацією та кращими практиками в галузі кібербезпеки. Одним з таких проектів є CyberCrime@EAP, що є частиною Програми Східного партнерства Європейського Союзу. Цей проект спрямований на підтримку країн Східного партнерства, включаючи Україну, у боротьбі з кіберзлочинністю, допомагаючи розвивати національні механізми реагування на кіберзагрози та підвищуючи рівень кіберзахисту.

Міжнародне співробітництво України в сфері розслідування кіберзлочинів є важливим елементом євроінтеграції та сприяє розвитку ефективних механізмів боротьби з кіберзагрозами через обмін досвідом, вдосконалення законодавства та активну участь у міжнародних ініціативах і програмах [192, с. 129].

Включення положення про транскордонну передачу інформації до Закону України «Про основні засади кібернетичної безпеки України» є важливим кроком для посилення міжнародного співробітництва в боротьбі з кіберзлочинністю. Це дозволяє Україні активно взаємодіяти з іншими країнами, обмінюючись інформацією щодо кіберзагроз та кіберзлочинів, що є важливою складовою ефективного реагування на транскордонні кіберзлочини. Такий підхід дає змогу Україні бути більш інтегрованою в глобальну мережу боротьби з кіберзлочинністю, полегшує доступ до важливої інформації та сприяє швидкому реагуванню на кіберзагрози, що можуть мати міжнародний характер. Це також підвищує ефективність співпраці між правоохоронними органами різних країн у контексті сучасних кіберзагроз [192, с. 129].

Згідно із Законом України №1906-V від 29.06.2004 року «Про міжнародні договори України», міжнародні договори, які набрали чинності і на обов'язковість яких надано згоду Верховною Радою України, є частиною

національного законодавства. Це означає, що вони мають пріоритет над внутрішнім законодавством України у разі суперечностей між національними актами та міжнародними зобов'язаннями країни. Це положення дозволяє Україні дотримуватись своїх міжнародних зобов'язань у сфері боротьби з кіберзлочинністю та іншими правопорушеннями, що стосуються глобальних питань безпеки, а також забезпечує ефективну інтеграцію національного законодавства з міжнародними нормами і стандартами [145].

Згідно з думкою В. О. Тімашова та Д. Ш. Діденка, основною проблемою, яка виникає в міжнародній боротьбі з кіберзлочинністю, є те, що деякі з найбільш поширених кіберзлочинів, зокрема ті, які здійснюються з країн, де відсутні міжнародні угоди чи домовленості, є значною перешкодою для ефективної протидії. Як приклад, автори зазначають Північну Корею, де кіберзлочинці, ймовірно, можуть діяти без належного міжнародного контролю або співпраці з іншими державами. Це ускладнює виявлення і затримання зловмисників, оскільки відсутність міжнародних договорів або угод з цими країнами обмежує можливості для правового співробітництва.

У випадку з Сполученими Штатами Америки, ситуація виглядає дещо іншою. США можуть відслідковувати та діяти проти відомих північнокорейських хакерів, застосовуючи принцип юрисдикції за наслідками. Тобто, навіть якщо злочин скоєний на території іншої держави (наприклад, у Північній Кореї), Сполучені Штати можуть вважати, що злочин має значні наслідки на їхній території, і тому мають право на кримінальну юрисдикцію над даними діями. Це виправдовує можливість США застосовувати свої правові інструменти для боротьби з кіберзлочинністю, навіть у випадку, коли країна-джерело атак не має міжнародних угод з США.

Таким чином, хоча міжнародне співробітництво у боротьбі з кіберзлочинністю є надзвичайно важливим, країни, зокрема ті, що мають потужні кіберзлочинні угруповання, можуть використовувати відсутність

угод або законодавчих механізмів як перепону для ефективного реагування. [168, с. 171].

Інтереси України в міжнародному співробітництві в боротьбі з транснаціональною злочинністю, зокрема кіберзлочинністю, представляють Департамент Інтерполу та Європолу Національної поліції України. Ці органи координують і організовують діяльність, спрямовану на реалізацію державної політики України щодо боротьби зі злочинністю, що має транснаціональні ознаки. Це співробітництво дозволяє Україні бути частиною глобальних ініціатив з протидії міжнародним злочинам, зокрема в контексті кіберзлочинності, що має все більш глобальний характер [44].

Участь України в двосторонніх договорах про взаємну правову допомогу з кримінальних питань є важливим елементом системи міжнародного співробітництва у боротьбі з кібершахрайством. Враховуючи характер сучасної кіберзлочинності, коли правопорушники можуть перебувати на території кількох держав, такі угоди стають критично важливими для ефективного розслідування та припинення злочинної діяльності. Такий механізм сприяє ефективнішому вирішенню проблеми кібершахрайства, зокрема в тих випадках, коли злочинці діють у межах кількох юрисдикцій, використовуючи анонімність і можливості, які надає Інтернет для приховування своєї особи та місця знаходження [125, с. 94-97].

Міжнародне співробітництво у кримінальних справах, зокрема в боротьбі з кібершахрайством, потребує ефективної координації між державами-учасницями міжнародних договорів. У цьому контексті, важливими є такі аспекти, як надання міжнародної правової допомоги, взаємний обмін інформацією та виконання процесуальних дій, пов'язаних з розслідуванням і покаранням за кримінальні правопорушення.

Для розслідування кіберзлочинів, що мають транснаціональний характер, важливою є взаємодія уповноважених органів різних країн. У межах цієї співпраці можуть бути вжиті такі заходи:

1. Вручення документів – наприклад, передача запитів, повісток чи інших судових документів між країнами.

2. Виконання процесуальних дій – це може включати допит свідків, потерпілих, експертів, а також проведення обшуків, вилучення речей чи документів, арешт майна або конфіскацію.

3. Видача осіб, які вчинили злочини, тимчасова передача осіб для слідства чи судового розгляду, а також передача засуджених осіб для відбування покарання.

4. Перехід кримінального переслідування — якщо інша країна має юрисдикцію для продовження розслідування чи здійснення покарання.

Ключовою умовою для цього співробітництва є взаємність – тобто країни, що співпрацюють, повинні надавати одна одній рівноцінну допомогу у разі потреби, коли виникає необхідність здійснити певні дії чи отримати правову допомогу в кримінальному процесі.

Згідно з Кримінальним процесуальним кодексом України, питання надання міжнародної правової допомоги вирішуються уповноваженими органами України – такими як Офіс Генерального прокурора, Міністерство юстиції України, та Національне антикорупційне бюро України. Уповноважений орган має право вирішувати, чи надавати дозвіл на виконання запиту про міжнародну допомогу.

У разі відсутності міжнародних договорів, міжнародне співробітництво здійснюється на засадах взаємності, де одна держава гарантує, що у разі виникнення подібної потреби в майбутньому, вона розгляне запит іншої країни, надавши допомогу в межах закону.

Таким чином, ефективність боротьби з кібершахрайством на міжнародному рівні залежить від координації між національними правоохоронними органами та правильного застосування міжнародних правових норм для забезпечення безпеки в кіберпросторі [124].

У процесі розслідування кримінальних правопорушень у сфері е-комерції, зокрема шахрайств, часто виникає необхідність у міжнародній

правовій допомозі, оскільки ці злочини часто мають транснаціональний характер. Як показує судово-слідча практика, в 29% випадків для виконання окремих процесуальних дій, таких як видача осіб, тимчасова передача, чи перехід кримінального переслідування, правоохоронним органам необхідно звертатися до компетентних органів іншої держави.

При поданні клопотання про міжнародну правову допомогу у таких випадках, важливо чітко сформулювати запит, включаючи такі ключові аспекти:

- Компетентний орган іноземної держави та установи, допомога яких потрібна – чітко зазначається, які конкретно органи в іншій державі повинні виконати запитувану допомогу (наприклад, правоохоронні органи, суди, прокуратури).

- Кваліфікація та короткий виклад обставин справи – вказується, що саме є підставою для звернення (наприклад, конкретне шахрайство в е-комерції), і які кримінальні правопорушення стали причиною запиту.

- Докладна інформація про підозрюваних осіб – важливо вказати всі відомості про осіб, які підозрюються у вчиненні кримінального правопорушення, і які можуть переховуватися на території іншої держави, а також їхню ймовірну місцеперебування.

- Докладна інформація про свідків та потерпілих – запит має включати інформацію про осіб, які проживають в іншій державі і з якими необхідно провести процесуальні дії (наприклад, допит свідків чи потерпілих).

- Зміст доручення – детально описується, яку конкретно допомогу необхідно отримати: чи це допит, чи вручення документа, чи інші процесуальні дії (наприклад, обшук, вилучення майна тощо).

Усі ці моменти мають бути точно та ретельно вказані в клопотанні для забезпечення ефективного виконання запиту та координації між державами у розслідуванні транснаціональних кримінальних правопорушень у сфері кіберзлочинності [67].

Питання правового регулювання операцій з цифровою валютою є надзвичайно важливим в умовах швидкого розвитку технологій та глобалізації фінансових ринків. Незважаючи на те, що цифрові валюти, такі як біткоїн чи ефір, швидко здобувають популярність, правове поле для їх регулювання все ще знаходиться на етапі становлення. Це обумовлено не лише новизною явища, а й швидкою зміною технологій та способів їх використання, що ускладнює створення уніфікованого пакету нормативних актів.

Однак, навіть у відсутності чітко визначених правових норм для цифрових валют, можна стверджувати, що ці операції не знаходяться в правовому «вакуумі». Багато юрисдикцій вже розробили або знаходяться на шляху до впровадження законодавчих ініціатив щодо обігу електронних грошей та цифрових валют. Наприклад, деякі країни створюють спеціальні законодавчі рамки для криптовалютних операцій, визначають статус таких валют як активів, а також встановлюють правила для їх обігу, оподаткування та боротьби з потенційними ризиками.

Особливо важливим є питання безпеки фінансових операцій з цифровими валютами, оскільки вони часто використовуються для незаконних цілей, таких як відмивання грошей або фінансування кіберзлочинності. Через анонімність і децентралізовану природу деяких криптовалют, вони можуть бути використані для обходу традиційних механізмів контролю фінансових операцій, що підвищує ризик їхнього використання в злочинних цілях.

З цією метою на міжнародному рівні з'являються ініціативи, спрямовані на вдосконалення законодавства для боротьби з кіберзлочинами та відмиванням грошей, пов'язаними з цифровими валютами. Окремі країни вже активно працюють над впровадженням систем, які дозволяють моніторити операції з криптовалютами, а також визначають вимоги до криптовалютних бірж і інших фінансових інститутів, що працюють з

цифровими валютами, для забезпечення прозорості та запобігання злочинним діям.

У цьому контексті необхідно враховувати, що цифрові валюти та технології блокчейн мають великий потенціал для розвитку фінансових ринків та забезпечення більш ефективних і безпечних транзакцій. Однак, для забезпечення стабільності та безпеки фінансових систем необхідно ефективно поєднувати інноваційні підходи з належним правовим регулюванням, що зменшить ризики незаконного використання цих технологій і підвищить рівень довіри до цифрових валют.

Електронна торгівля, хоча й не має уніфікованого визначення на міжнародному рівні, широко розглядається як форма бізнес-угоди між фізичними та юридичними особами, що використовують електронні комунікаційні технології для здійснення угод, що традиційно відбуваються через фізичний обмін товарами або послугами. З розвитком Інтернету та глобалізацією цифрових технологій, електронна торгівля стала важливою складовою міжнародної економіки. Зокрема, обсяги електронної торгівлі досягли 5% від загальних продажів на глобальному рівні у 2014 році, і цей показник продовжує зростати.

Основним документом, що визначає стандарти для електронної торгівлі, є Типовий закон про електронну торгівлю, ухвалений Комісією ООН з права міжнародної торгівлі (UNCITRAL) у 1996 році. Хоча цей акт не є міжнародним договором у класичному розумінні, його застосовують багато країн для розробки власного національного законодавства у сфері електронної комерції. Закон сприяє створенню гармонізованої правової бази для електронної торгівлі та встановлює основні правила і принципи, які допомагають регулювати взаємодію у цифровій економіці.

Секретаріат UNCITRAL веде реєстр країн, які імплементували цей закон, і на сьогоднішній день його застосування охоплює 54 держави. Це підтверджує важливість цієї правової ініціативи як міжнародного стандарту,

що активно впливає на розвиток електронної торгівлі в глобальному масштабі.

Водночас, розширення електронної торгівлі підвищує потребу в удосконаленні міжнародних правових механізмів для забезпечення безпеки фінансових операцій, захисту прав споживачів, а також запобігання шахрайству, відмиванню грошей та іншим злочинам, які можуть бути здійснені в рамках електронної комерції. Тому міжнародне співробітництво в цій сфері, включаючи розробку спільних стандартів та угод, є важливим аспектом для подальшого розвитку цифрової економіки.

Типовий закон UNCITRAL про електронну торгівлю відіграє важливу роль у визначенні принципів та стандартів, що регулюють електронні операції, включаючи використання цифрових валют. Одним з ключових принципів, визначених цим законодавчим актом, є принцип технологічного нейтралітету (або медіанейтральності). Це означає, що сама технологія, яка використовується для проведення операцій з цифровою валютою, не може бути заборонена лише через можливість її зловживання. Технологія може використовуватися як для законних, так і для незаконних цілей, і тому вона не визнається незаконною сама по собі. Згідно з цією концепцією, відповідальність за незаконне використання технології покладається на кінцевих користувачів, а не на саму технологію. Це підкреслює важливість контролю за використанням цифрових валют та їх застосуванням в межах законодавства.

Захист прав споживачів є ще одним важливим аспектом у контексті регулювання електронної торгівлі, особливо коли мова йде про операції з цифровими валютами. Важливо, щоб клієнти, які використовують цифрові валюти для здійснення покупок або інвестицій, були захищені від шахрайства та ризикових угод. Законодавство має забезпечувати споживачів високим рівнем захисту, надаючи їм право отримувати товари та послуги відповідної якості. У цьому контексті важливим є визначення норм, які

сприяють захисту прав споживачів, а також встановлення чітких правил для обробки та вирішення спорів, пов'язаних з електронними угодами.

Наприклад, Директива ЄС про електронну торгівлю встановлює високі стандарти захисту прав споживачів у цифровому середовищі. Вона вимагає, щоб бізнеси, що здійснюють електронні угоди, надавали чітку інформацію про умови надання послуг, захищали права споживачів від неналежних практик та забезпечували ефективні механізми для вирішення спорів. Це включає захист від непередбачуваних ризиків, які можуть виникнути при здійсненні операцій із цифровими валютами або іншим контентом в електронній торгівлі.

У зв'язку з потенційними ризиками, що виникають через використання цифрових валют у злочинній діяльності, такі норми також включають заходи, спрямовані на забезпечення прозорості операцій, запобігання відмиванню грошей і боротьбу з фінансуванням тероризму [111]. Регулювання, що стосується цифрових валют, повинно забезпечувати ефективну взаємодію між національними органами та міжнародними правовими інститутами, щоб мінімізувати ризики зловживань у цій сфері.

Однією з важливих проблем у використанні криптовалют є незворотність операцій, особливо у випадку з біткоїнами. Це особливість, яку варто враховувати в контексті захисту прав споживачів, оскільки після завершення транзакції неможливо повернути кошти, навіть якщо угода була здійснена помилково або під впливом шахрайства. Це створює певні ризики для користувачів, які можуть стати жертвами обману або непередбачених ситуацій, і вимагає спеціальних механізмів захисту та регулювання на рівні правових норм.

Активне зближення сфер протидії кіберзлочинності та захисту даних дійсно сприяло тому, що організації, які займаються захистом прав споживачів, стали важливими партнерами у виявленні та запобіганні кіберзлочинам. Такі організації надають цінну інформацію про інциденти, пов'язані з кіберзлочинністю, і можуть допомогти визначити патерни

шахрайства в системах цифрових валют. Вони можуть також діяти як проміжні ланки між користувачами і правоохоронними органами для надання інформації про випадки порушень прав споживачів у цифрових операціях.

Тим не менше, більшість нормативно-правових актів щодо електронних платежів були розроблені для традиційних фінансових інструментів і базуються на фіатних валютах, що обробляються через фінансові установи. Однак цифрові валюти, такі як біткоїн, не прив'язані до традиційних фінансових систем і не потребують участі банків чи інших фінансових посередників для проведення транзакцій. Це створює ситуацію, коли звичні регуляційні механізми, які застосовуються до електронних платежів, не зовсім підходять для цифрових валют, оскільки ці валюти функціонують поза традиційними фінансовими мережами.

Проте, при конвертації цифрових валют у фіатні гроші і навпаки, застосовуються певні регуляції, особливо коли мова йде про фінансові установи, що працюють з криптовалютами. Проблема полягає в тому, що цифрові валюти, будучи децентралізованими (у випадку з біткоїном), не підпадають під контроль традиційних фінансових регуляторів, і механізми, які зазвичай застосовуються до фінансових установ, не є достатніми для захисту прав споживачів у цій сфері.

Тому важливою є розробка нових регуляцій, які враховуватимуть особливості транзакцій з цифровими валютами. Це включає в себе вивчення можливості адаптації існуючих нормативів до специфіки цифрових валют, а також створення нових правил для забезпечення захисту споживачів, особливо у випадках шахрайства або незворотних операцій.

Відмивання грошей – це процес, через який злочинці намагаються приховати або легалізувати кошти, здобуті від незаконної діяльності, створюючи видимість їх законного походження. Це включає в себе серії фінансових операцій, що мають на меті «замаскувати» джерело доходів,

зробити їх важкими для відстеження правоохоронними органами та демонструвати їх як законно отримані.

Сьогодні боротьба з відмиванням грошей забезпечується за допомогою низки міжнародних стандартів і інструментів, які значно покращили ефективність запобігання та боротьби з цією злочинною діяльністю. Важливими міжнародними документами, що визначають боротьбу з відмиванням грошей, є:

1. Конвенція ООН про боротьбу з незаконним обігом наркотичних засобів і психотропних речовин (1988). Цей документ став першим міжнародним правовим актом, що включав визначення відмивання доходів, здобутих через злочини, пов'язані з наркотиками. Вона встановлює обов'язки для держав боротися з незаконними фінансовими операціями, пов'язаними з наркотиками, і застосовувати відповідні кримінальні санкції [74].

2. Конвенція ООН проти транснаціональної організованої злочинності (2000). Даний документ розширює поняття відмивання грошей, охоплюючи не лише наркотики, але й інші форми організованої злочинності, такі як торгівля людьми, зброєю та іншими незаконними товарами. Він передбачає вимоги до держав щодо запобігання використанню фінансових систем для відмивання коштів, здобутих злочинним шляхом [76].

3. Конвенція ООН проти корупції (2003). Вона розвиває вимоги до боротьби з відмиванням коштів у контексті корупційних злочинів. Встановлюється, що держави повинні вжити заходів для виявлення та конфіскації активів, які отримано в результаті корупційних дій, а також для розслідування випадків відмивання доходів від корупції [75].

4. Міжнародна конвенція ООН про боротьбу з фінансуванням тероризму. Цей документ передбачає більш детальний підхід до боротьби з відмиванням грошей, пов'язаних з тероризмом. Окремі положення цієї конвенції визначають спеціальні механізми для відслідковування, ідентифікації та арешту коштів, здобутих через терористичну діяльність, а

також забезпечують зусилля держав для припинення фінансування тероризму через незаконні фінансові потоки.

Загалом, ці міжнародні угоди та конвенції забезпечують основу для розробки національних правових норм, спрямованих на боротьбу з відмиванням грошей і забезпечення міжнародної співпраці у цій сфері. Кожна з цих конвенцій надає конкретні механізми та вимоги до країн-учасниць, допомагаючи створити єдиний фронт у боротьбі з відмиванням грошей та іншими фінансовими злочинами на глобальному рівні.

FATF (Financial Action Task Force, Міжурядова група з фінансових заходів боротьби з відмиванням грошей та фінансуванням тероризму) є одним з основних міжнародних органів, що розробляє стандарти і сприяє впровадженню правових, нормативних і оперативних заходів у боротьбі з відмиванням грошей, фінансуванням тероризму та іншими загрозами цілісності міжнародної фінансової системи. Зазначені стандарти допомагають державам-учасницям розробляти ефективні механізми запобігання фінансовим злочинам, включаючи протидію відмиванню грошей і незаконному фінансуванню тероризму.

Рекомендації FATF – це зведення обов'язкових вимог, які мають бути виконані країнами, що є членами цієї організації. Ці рекомендації є основними стандартами для формування національних законодавств та практик щодо боротьби з фінансовими злочинами. Контроль за їх дотриманням здійснюється через регулярні моніторингові процедури, включаючи перевірки і оцінки ефективності виконання зобов'язань, що стосуються відмивання грошей і фінансування тероризму.

Особливу увагу FATF приділяє питанням, пов'язаним із цифровими валютами, оскільки децентралізована природа цих валют створює значні ризики для використання їх як інструментів для координації кримінальних фінансових потоків. Враховуючи, що цифрові валюти не мають центрального контролюючого органу, ризик їх використання в незаконних фінансових

операціях, таких як відмивання грошей або фінансування тероризму, є досить високим.

Проте, важливо зазначити, що проблеми з використанням цифрових валют для злочинної діяльності виникають не лише через саму технологію (зокрема через підвищену конфіденційність транзакцій, складність відслідковування і наявність криптографічного захисту), а й через відсутність належного регулювання та контролю за операціями з такими валютами з боку компетентних органів. Без належних заходів з регулювання операцій з цифровими валютами важко запобігти їх використанню для злочинних цілей, оскільки відсутність централізованого контролю створює умови для використання криптовалют в анонімних транзакціях, що ускладнює ідентифікацію учасників і походження коштів.

Тому однією з важливих задач є розробка регуляцій, які б дозволяли ефективно контролювати транзакції з цифровими валютами, зокрема через залучення фінансових установ, які займаються обміном криптовалют на фіатні гроші, до виконання обов'язків щодо верифікації клієнтів, перевірки джерел коштів і звітування про підозрілі транзакції.

Цифрові валюти можуть бути використані як засіб для учинення різних кримінальних правопорушень, а не тільки для відмивання грошей. Вони відкривають можливості для злочинців через свою анонімність і децентралізовану природу, що може ускладнити відслідковування та ідентифікацію учасників фінансових операцій.

Зважаючи на ці можливості, важливим аспектом є необхідність розвитку правового регулювання використання цифрових валют. Це включає як розробку чітких нормативних актів щодо використання криптовалют, так і впровадження ефективних механізмів контролю, таких як обов'язкові процедури ідентифікації учасників транзакцій (KYC - Know Your Customer), що дозволяють зменшити ризики використання цифрових валют у кримінальних цілях.

Окрім того, важливо, щоб країни, які не мають чіткої нормативно-правової бази щодо цифрових валют, почали приймати закони та правила, що забезпечують їх легальність, а також визначали кримінальні наслідки за їх незаконне використання, обіг або володіння.

Цифрові валюти можуть бути використані не лише в межах традиційних кримінальних правопорушень, таких як шахрайство чи крадіжка, але й для фінансування серйозніших правопорушень, зокрема тероризму та міжнародних злочинів. Ці аспекти використовування цифрових валют в злочинній діяльності висвітлюють важливість розвитку глобальних і національних механізмів для контролю за їх обігом. Відсутність регулювання або недосконале законодавство можуть призвести до того, що криптовалюти залишаються важким інструментом для кримінальних цілей. Тому багато міжнародних організацій, таких як FATF, активно працюють над встановленням стандартів і рекомендацій для боротьби з такими загрозами, щоб мінімізувати ризики використання криптовалют у злочинних схемах.

Цифрові валюти, з огляду на їх електронну природу та використання в Інтернеті, справді можуть стати частиною кіберзлочинності, яка є одним з найбільш динамічно зростаючих напрямків кримінальної діяльності. Кіберзлочинність охоплює широкий спектр порушень, що стосуються не лише злочинів проти комп’ютерних систем і даних, а й тих, що стосуються використання цих систем для вчинення традиційних злочинів, таких як шахрайство, підробка документів, або поширення заборонених матеріалів.

Кіберзлочинність в контексті цифрових валют включає, зокрема:

- комп’ютерне шахрайство (наприклад, зловмисники можуть використовувати цифрові валюти для шахрайських операцій, таких як «фішинг», маніпуляції з курсами криптовалют чи створення фальшивих бірж). Такий тип злочину може також включати використання криптовалют для незаконних операцій на онлайн-платформах або в обміні на інші валютні одиниці через неперевірені канали;

- кіберзлочини, пов’язані з контентом. Використання цифрових валют у кіберзлочинності може включати обіг заборонених товарів чи послуг, таких як нелегальна зброя, наркотики чи дитяча порнографія. Криптовалюти можуть використовуватися як метод оплати для цих товарів і послуг у «темному вебі», де анонімність і відсутність контролю з боку фінансових установ значно ускладнюють розслідування таких злочинів;

- міжнародне співробітництво в боротьбі з кіберзлочинністю. Оскільки кіберзлочинність не обмежується кордонами держав, для боротьби з таким явищем необхідно активне міжнародне співробітництво. В рамках цього співробітництва було розроблено кілька міжнародних угод і конвенцій, що спрямовані на боротьбу з кіберзлочинністю та захист інформаційної безпеки. Важливими з них є:

1) Конвенція Ради Європи про кіберзлочинність (так звана Будапештська конвенція), яка є першим міжнародним юридичним інструментом, що забезпечує гармонізацію законодавства країн-учасниць в сфері боротьби з кіберзлочинами.

2) Угода ШОС та Ліги арабських держав з питань міжнародної інформаційної безпеки, що сприяють створенню співпраці між державами для запобігання кіберзлочинам, пов’язаним з інформаційними технологіями та цифровими валютами.

Правова динаміка кіберзлочинності та боротьби з нею в останні роки характеризується змінами в національних і міжнародних правових нормах, що визначають методи боротьби з кіберзлочинністю. Імплементація міжнародних актів в національні законодавства дозволяє країнам удосконалювати процедури розслідування кіберзлочинів, у тому числі й таких, що пов’язані з використанням цифрових валют. Однак, з огляду на швидкий розвиток технологій і нові форми злочинної діяльності, боротьба з кіберзлочинністю потребує постійного вдосконалення правових норм та механізмів, а також активного міжнародного співробітництва для ефективної протидії цьому явищу.

У сучасному контексті цифрові валюти часто стають інструментом для вчинення кіберзлочинів. Крадіжка цифрової валюти може бути кваліфікована як основний злочин, якщо, наприклад, хакерське проникнення в систему призводить до незаконного привласнення біткоїнів чи інших криптовалют. Водночас, це може бути частиною складнішого злочинного ланцюга, де кіберзлочин є вторинним і лише допомагає реалізувати основне правопорушення (наприклад, крадіжка коштів або відмивання грошей). Це підкреслює складність і багаторівневість сучасних кіберзлочинів.

З точки зору правової кваліфікації, слід також відзначити, що несанкціонований доступ до комп'ютерних систем і даних може бути задіяний у багатьох інших злочинах, які пов’язані з цифровими валютами. Наприклад, незаконне втручання у цифрові гаманці користувачів або доступ до приватних ключів може призвести до крадіжки криптовалют. Такий тип злочину має яскраво виражений вторинний характер, тобто є засобом для реалізації основного кримінального правопорушення, зокрема, відмивання грошей через криптовалюти.

Кіберзлочини можуть бути не тільки підставою для вчинення злочинів з використанням цифрових валют, а й самостійними правопорушеннями. Наприклад, комп’ютерне шахрайство, де криптовалюти використовуються як засіб обману, може бути основним кримінальним парвпорушенням. Це особливо актуально для випадків, коли користувачі стають жертвами схем обману, таких як фальшиві ICO (первинні пропозиції монет), фішинг або інші шахрайські методи, які використовують криптовалюти.

Ще один важливий аспект – це злочини, пов’язані з контентом, де цифрові валюти використовуються для обміну забороненими товарами або послугами. Наприклад, криптовалюти можуть служити інструментом для придбання матеріалів з дитячою порнографією, наркотиків або іншого незаконного контенту через темні мережі, де анонімність криптовалют є додатковим фактором для здійснення таких правопорушень. У таких

випадках криптовалюти можуть бути як частиною основного злочину, так і допоміжним елементом у схемах відмивання грошей.

Крім того, транснаціональний характер кіберзлочинності ускладнює процеси розслідування, оскільки ці злочини часто охоплюють кілька юрисдикцій, що ставить під загрозу ефективність національних правоохоронних органів. Додатковим викликом є складність збору і аналізу електронних доказів, оскільки сліди таких злочинів часто є складними для відстеження і потребують спеціалізованих технічних знань і інструментів для розслідування. Тому своєчасне інформування компетентних органів є критично важливим для ефективної боротьби з кіберзлочинністю, пов’язаною з цифровими валютами.

Загалом, боротьба з кіберзлочинністю, що використовує цифрові валюти, вимагає комплексного підходу, включаючи міжнародне співробітництво, правову гармонізацію, а також активне залучення новітніх технологій для ефективного збору і аналізу доказів у цифровому середовищі.

Правове регулювання цифрових валют у багатьох країнах, зокрема в США, відзначається поступовим розвитку та адаптацією до нових технологічних реалій. Відмінність між міжнародними підходами і національними стратегіями часто полягає в тому, як конкретні країни вирішують питання звітності, реєстрації, оподаткування та боротьби з можливими зловживаннями в контексті використання віртуальних валют. Водночас, для забезпечення стабільності і безпеки фінансових операцій з криптовалютами країни, як і США, розробляють спеціалізовані нормативно-правові акти.

Різні країни вивчають можливості регулювання цифрових валют у контексті зростання операцій і технологічних досягнень. На міжнародному рівні вивчаються різні підходи до правового статусу криптовалют, покращення контролю за їх використанням, а також боротьби з відмиванням грошей та іншими фінансовими злочинами. Зокрема, інституції як FATF (Фінансова акція по боротьбі з відмиванням грошей) сприяють створенню

міжнародних стандартів для забезпечення належного контролю над фінансовими транзакціями з використанням цифрових валют, зокрема для попередження терористичного фінансування та інших злочинних діяльностей.

Таким чином, питання регулювання цифрових валют знаходиться на перехресті інтересів національних урядів, міжнародних організацій та фінансових установ, і має великий потенціал для подальшого розвитку правової бази, що відповідає вимогам технологічного прогресу та забезпечує безпеку фінансових операцій в епоху цифрової економіки.

Велика Британія та Китай обрали різні підходи до регулювання ринку цифрових валют, враховуючи власні економічні, правові та соціальні особливості.

У Великій Британії підхід до криптовалют базується на балансі між підтримкою інновацій та забезпеченням регуляторного контролю. Це особливо видно у Податковому та митному бюлетені 09/14, який містить ключові положення щодо оподаткування операцій із цифровими валютами.

Китай обрав більш обмежувальний підхід до регулювання криптовалют, зосередившись на обмеженні їх використання в офіційній фінансовій системі.

Порівняння підходів:

Велика Британія прагне інтегрувати криптовалюти у правове поле через механізми оподаткування та контролю, залишаючи простір для інновацій.

Китай зосереджується на обмеженні використання криптовалют, побоюючись їхнього впливу на стабільність фінансової системи та потенційних ризиків, пов'язаних із відмиванням грошей.

Обидва підходи відображають стратегію забезпечення безпеки фінансових систем і водночас реагування на швидкий розвиток ринку цифрових валют.

Підходи Канади та Сингапуру до регулювання цифрових валют вирізняються зваженим балансом між підтримкою інновацій та забезпеченням контролю, хоча їхні акценти і пріоритети різняться.

Уряд Канади визнав криптовалюти, включно з біткоїнами, інструментом, що може стати частиною фінансової екосистеми в майбутньому, але наразі вони не є законним платіжним засобом [41, с. 23].

Сингапур підходить до регулювання криптовалют із прагматизмом, допускаючи їх використання як платіжного засобу, але встановлюючи чіткі правила для забезпечення прозорості.

Канада зосереджується на поетапному регулюванні, враховуючи ризики та залишаючи простір для адаптації в майбутньому. Сингапур активно впроваджує криптовалюти у фінансову систему, встановлюючи жорсткі вимоги до прозорості операцій.

Обидві держави демонструють прагматичний підхід, орієнтований на підтримку розвитку технологій, зберігаючи при цьому контроль над ризиками.

3.3. Міжнародне співробітництво у справах про шахрайство, вчинене з використанням цифрових технологій

У сучасному світі стрімкий розвиток цифрових технологій не лише відкриває нові можливості, а й породжує нові виклики, зокрема кіберзлочинність. Цей феномен є наслідком глобалізації інформаційних процесів і став серйозною загрозою для безпеки держав, економічної стабільності та приватного життя громадян.

Кіберзлочини, такі як незаконний доступ до даних, шахрайство, порушення конфіденційності, а також атаки на критичну інфраструктуру, стали повсякденним явищем. Їхній вплив посилюється через: доступність методів соціальної інженерії; транснаціональний характер; еволюцію технологій [170].

Незважаючи на наявність різних інструментів, боротьба з кіберзлочинністю стикається з певними труднощами такими як: різниця в національному і міжнародному законодавстві; недостатній обмін інформацією; технічна складність доказів [77].

Ми вважаємо за доцільне запропонувати шляхи вирішення вище зазначених проблем, а саме:

- посилення міжнародної співпраці. Розширення участі країн у Будапештській конвенції та залучення ООН до створення нових ініціатив;
- уніфікація стандартів. Встановлення глобальних стандартів для розслідування кіберзлочинів і обміну даними;
- навчання фахівців. Підготовка кіберекспертів, здатних працювати з цифровими доказами та технологіями розслідування;
- інформування громадян. Проведення інформаційних кампаній для підвищення обізнаності про методи соціальної інженерії та захист особистих даних.

Сучасний розвиток інформаційного суспільства породжує нові виклики, пов’язані із захистом електронних інформаційних ресурсів та протидією кіберзлочинності. Незважаючи на значний вклад вітчизняних і закордонних науковців, таких як М.О. Будаков, В.М. Бутузов, М.М. Галамба, Я.Ю. Кондратьєв, А. Роберт і Т. Блентан, у дослідженні цієї сфери, існує потреба в подальшому вдосконаленні законодавчої бази та механізмів протидії кіберзлочинам. Однак необхідність подальшого наукового пошуку у сфері протидії кіберзлочинності та кібершахрайству обумовлена низкою проблем, які потребують вирішення. З огляду на динамічний розвиток інформаційних технологій, запровадження сучасних підходів до регламентації та співпраці у сфері боротьби з кіберзлочинністю є ключовим завданням для України. Це дозволить не лише забезпечити ефективний захист інформаційних ресурсів, але й підвищити довіру міжнародної спільноти до здатності України дотримуватися стандартів у галузі кібербезпеки.

Конвенція про кіберзлочинність, ухвалена Радою Європи 23 листопада 2001 року та ратифікована Україною 1 липня 2004 року, є важливим кроком у боротьбі з кіберзлочинністю на міжнародному рівні. Цей документ заклав основи для формування уніфікованих підходів до розслідування та запобігання правопорушенням, вчиненим з використанням комп'ютерних технологій. На міжнародній арені Конвенція є орієнтиром для країн, які прагнуть інтегрувати свої законодавчі та адміністративні системи до єдиного підходу в боротьбі з кіберзлочинністю. Під час одинадцятого і дванадцятого Конгресів ООН із запобігання злочинності та кримінального правосуддя була висловлена серйозна стурбованість щодо глобального поширення кіберзлочинності [78]. Прирівняння кіберзлочинності до таких загроз, як тероризм, підкреслює стратегічну важливість цього питання для глобальної безпеки. Такий підхід відображає необхідність координації зусиль на міжнародному рівні, оскільки кіберзлочини часто виходять за межі однієї юрисдикції та вимагають глобальної відповіді.

Конвенція про кіберзлочинність є важливим інструментом для боротьби з правопорушеннями у цифровому просторі, а її імплементація та розвиток міжнародного співробітництва залишаються пріоритетними завданнями для країн-учасниць. Інтенсивна взаємодія у цій сфері може стати ефективною відповіддю на виклики, що ставить перед суспільством цифрова епоха [23, с. 107-112].

У сфері боротьби з кіберзлочинністю існує низка універсальних міжнародних документів, що визначають принципи, стандарти та механізми співпраці [180].

До основних міжнародних актів належать: Довідник ООН із запобігання і контролю злочинності, пов'язаної з комп'ютерами (1995); Конвенція ООН проти транснаціональної організованої злочинності (2000); «Мінімальний список» комп'ютерних злочинів (1990); Конвенція Ради Європи про кіберзлочинність (2001).

У 1991 році Інтерпол інтегрував кодифікатор кіберзлочинів у свою автоматизовану систему пошуку, що дозволяє правоохоронним органам багатьох країн, зокрема України, оперативно обмінюватися інформацією про кіберзлочинців та їх дії.

До документів Європейського Союзу в цій сфері належать:

- Директива ЄС щодо протидії кібератакам на інформаційні системи (2013);
- Директива Єврокомісії щодо боротьби з шахрайством і фінансовими злочинами в Інтернеті (2017);
- Стратегія кібербезпеки ЄС.

Міжнародна співпраця є ключовим фактором ефективної боротьби з кіберзлочинністю, оскільки такі кримінальні правопорушення часто мають транснаціональний характер. Документи, ухвалені на рівні ООН, Ради Європи, ЄС та Інтерполу, закладають правову та організаційну основу для протидії сучасним викликам у цифровому середовищі [196; 181].

Деякі держави досягли значного прогресу у створенні регіональних механізмів співпраці для боротьби з кіберзлочинністю. Основою такої кооперації є гармонізація правових норм, взаємне визнання законодавчих актів і розвиток правових механізмів для забезпечення швидкого реагування на загрози у сфері кібербезпеки. Ефективна кооперація між державами, що спирається на гармонізовані норми матеріального права та регіональні правові механізми, є основою для подолання кіберзлочинності. Використання директив, таких як Directive 2011/93/EU та Directive 2016/1148, допомагає країнам забезпечувати єдиний рівень захисту від кіберзагроз та покращувати правову базу для співпраці в межах транснаціональних розслідувань [65].

Боротьба з кіберзлочинністю вимагає тіснішої взаємодії між державами та гармонізації не лише кримінально-правових норм, але й процесуальних інструментів. Це дозволяє оперативно реагувати на динамічні загрози, пов'язані з протиправною діяльністю в кіберпросторі.

Для ефективної боротьби з кіберзлочинністю важливо уніфікувати:

- механізми збору електронних доказів, включаючи їх прийнятність у суді;
- інструменти екстрадиції для швидкого переслідування осіб, які вчинили кримінальні правопорушення у кіберпросторі;
- процедури спільних розслідувань з участю правоохоронних органів різних держав.

Ефективна боротьба з кіберзлочинністю можлива лише за умови інтегрованого міжнародного партнерства. Використання інструментів, таких як регіональні модельні закони та глобальні ініціативи, дозволяє державам адаптувати своє законодавство до сучасних викликів. Крім того, важливим аспектом є впровадження нових форм співпраці, що враховують специфіку кіберзлочинів та швидкість розвитку інформаційних технологій.

З 1990-х років міжнародна спільнота почала активно розробляти та приймати правові акти, спрямовані на боротьбу з кіберзлочинністю. ООН та інші організації відіграють ключову роль у формуванні глобальної політики у цій сфері. Діяльність ООН демонструє важливість координації зусиль міжнародної спільноти для вирішення проблем, пов'язаних із комп'ютерними злочинами. Завдяки прийняттю концептуальних і правових документів, зокрема резолюцій ГА ООН та ЕКОСОР, були започатковані основи для ефективної боротьби з кіберзлочинністю та захисту персональних даних на глобальному рівні [47, с. 2].

Резолюція Генеральної Асамблеї ООН A/RES/58/199, ухвалена в 2003 році, підкреслює необхідність захисту інформаційних інфраструктур, що є основою для функціонування сучасного суспільства. Вона визначає низку компонентів для забезпечення їх охорони, зокрема:

1. Присутність мереж для негайного реагування.
2. Збільшення поінформованості відповідальних осіб.
3. Забезпечення належних законів і процесуальних норм.
4. Розвиток комунікаційних концепцій і контроль їх діяльності.

5. Міжнародне співробітництво в боротьбі з кібератаками.

Резолюція A/RES/58/199 є важливим документом, що окреслює стратегічні підходи до захисту критичних інформаційних інфраструктур. Вона акцентує увагу на необхідності підвищення обізнаності, прийнятті законодавчих ініціатив, розвитку міжнародного співробітництва та ефективних заходів реагування для забезпечення безпеки в кіберпросторі. [161, с. 5].

У рамках глобальних зусиль щодо розвитку інформаційно-комунікаційних технологій (ІКТ) та забезпечення кібербезпеки, ООН разом з Комісією Африканського Союзу працює над створенням конвенції про кібербезпеку для Африки в рамках програми «Нове партнерство на користь розвитку Африки» (НЕПАД). Ця ініціатива має на меті посилення правових основ для розслідування кіберзлочинності та забезпечення ефективнішого захисту інформаційних ресурсів на континенті.

Однак міжнародне співробітництво в сфері боротьби з кіберзлочинністю та забезпечення кібербезпеки стикається з низкою серйозних проблем: розбіжності у сфері співпраці; відсутність чітких зобов'язань щодо термінів відповіді; проблеми доступу до екстериторіальних даних; неофіційні мережі правоохоронних органів; відмінності в гарантіях співпраці.

Розв'язання цих проблем вимагає подальшого розвитку міжнародної правової співпраці, гармонізації законодавчих норм і стандартів, а також створення ефективних механізмів реагування на кіберзагрози. Успішне виконання цих завдань потребує міжнародної взаємодії, зокрема в рамках таких ініціатив, як програма НЕПАД і Конвенція про кіберзлочинність, що дозволяють створити правові засади для боротьби з кіберзлочинністю на глобальному рівні [120, с. 5].

Проєкт «Загального договору з питань кібербезпеки та кіберзлочинності», запропонований професором Штайном Шольбергом та Соланж Гернуті-Елі, є важливою ініціативою у сфері міжнародного

регулювання кіберзлочинності та інформаційного тероризму. Цей проект був розроблений в рамках групи експертів високого рівня з питань кібербезпеки, заснованої в 2007 році, з метою створення загального міжнародного правового документа для боротьби з кіберзлочинністю в рамках ООН. Цей проект спрямований на створення чітких міжнародних стандартів для боротьби з кіберзлочинністю та тероризмом в кіберпросторі, визначаючи, зокрема, порядок міжнародної правової допомоги в розслідуванні таких злочинів та кримінальної відповідальності за їх вчинення. Враховуючи масштаби та глобальний характер кіберзагроз, цей договір може стати важливим етапом у розробці міжнародного правового регулювання кібербезпеки [33, с. 315].

Концепція «Універсальності Інтернету», розроблена в рамках ЮНЕСКО, стала важливим кроком у визначенні принципів, що мають сприяти розвитку Інтернету як інструменту досягнення сталого розвитку та підтримки прав людини в цифрову епоху. Ця концепція була розроблена з огляду на перспективи розвитку Інтернету до 2021 року та має на меті забезпечити рівні можливості для всіх користувачів.

Основні принципи концепції, відомі як R.O.A.M., є основою для формування ефективної та справедливої цифрової екосистеми. Ці принципи мають важливе значення для розвитку політик щодо Інтернету, що сприяють досягненню цілей сталого розвитку ООН, і допомагають забезпечити справедливе використання технологій для покращення життя людей в усьому світі [64, с. 82].

Концепція Конвенції ООН про забезпечення міжнародної інформаційної безпеки є важливим кроком у розвитку міжнародного правового регулювання питань, пов'язаних із захистом інформаційного простору на глобальному рівні. Однією з основних цілей цієї Конвенції є забезпечення стабільності в інформаційному середовищі і боротьба з кіберзлочинністю та іншими загрозами, що можуть порушити міжнародний мир і безпеку.

У статті 4 Конвенції визначено основні загрози, що становлять небезпеку для міжнародної безпеки в інформаційному просторі.

Серед базових загроз можна виділити:

- використання інформаційних технологій та засобів для здійснення ворожих дій та актів агресії – це включає використання кіберзброї або інших технологій для нападів на держави або міжнародні структури;

- цілеспрямований деструктивний вплив на критично важливі структури іншої держави – йдеться про спроби вивести з ладу критичні інфраструктури, такі як енергетичні мережі, фінансові системи чи системи національної безпеки;

- транскордонне поширення інформації, що суперечить міжнародному праву та національним законодавствам – розповсюдження шкідливої або неправдивої інформації, що може викликати міжнародну напругу або порушення суверенітету держав.

Крім базових, Конвенція також визначає додаткові загрози, що включають, зокрема, порушення правил кібербезпеки, кібершахрайство і крадіжки особистих даних.

Для підвищення ефективності міжнародної правової допомоги у боротьбі з кіберзлочинністю, важливими є нововведення у сфері електронних доказів. Одним із таких нововведень є включення модуля з електронних доказів в перероблену програму складання прохань про надання взаємної правової допомоги Управління ООН з наркотиків та злочинності (УНП ООН). Це дозволяє значно спростити і пришвидшити процеси збору, обміну та використання електронних доказів у кримінальних провадженнях, зокрема тих, що стосуються транснаціональних кіберзлочинів.

Водночас, правоохоронні органи повинні враховувати зростаючі потреби у новаторських методах співпраці, оскільки кіберзлочинність часто має транснаціональний характер і вимагає координації між різними країнами. Це включає вдосконалення процесів транснаціональних розслідувань, розробку спільних стандартів для збору електронних доказів і їх визнання в

різних юрисдикціях, а також створення механізмів, що дозволяють країнам ефективно співпрацювати під час розслідувань складних кіберзлочинів [108, с. 109]. Участь міжнародних організацій у координації транснаціональних розслідувань кіберзлочинів має важливе значення для забезпечення ефективного реагування на глобальні загрози в кіберпросторі. Такі організації, як Глобальний інноваційний комплекс Інтерполу та Європейський центр по боротьбі з кіберзлочинністю (ЕЦК), виконують ключову роль у наданні координації, ресурсів та експертної допомоги державам для боротьби з кіберзлочинністю.

Інтерпол є важливою платформою для міжнародного співробітництва у боротьбі з кіберзлочинністю, забезпечуючи обмін інформацією між правоохоронними органами країн-членів. Глобальний інноваційний комплекс Інтерполу допомагає країнам швидко реагувати на нові кіберзагрози та розвивати інноваційні стратегії для боротьби з ними. Це включає як технічну підтримку, так і надання навчальних матеріалів та координацію міжнародних операцій. Інтерпол також сприяє інтеграції кіберпідрозділів національних поліційних сил у глобальні мережі обміну даними та розслідувань.

ЕЦК Європолу відіграє ключову роль у координації європейських зусиль у боротьбі з кіберзлочинністю. Центр займається підтримкою країн ЄС у розслідуваннях кіберзлочинів, сприяє розвитку інформаційних систем для обміну даними між правоохоронними органами, а також надає аналітичну та технічну допомогу. Крім того, ЕЦК активно співпрацює з іншими міжнародними організаціями та приватними компаніями для покращення реакції на кібератаки та кіберзлочинність.

Інші міжнародні ініціативи, такі як Глобальна конференція з кіберпростору, створюють платформу для держав, приватних секторів та міжнародних організацій для обміну досвідом і кращими практиками у сфері кібербезпеки та боротьби з кіберзлочинністю. Це важливий захід, який дозволяє розробляти інноваційні заходи реагування на сучасні виклики, що постають перед міжнародною спільнотою в кіберпросторі. Конференція

забезпечує можливість розгляду питань міжнародної співпраці, розробки нових стандартів безпеки та реагування на кіберзагрози в глобальному контексті.

Координація таких структур, як Інтерпол, Європол, а також участь у міжнародних ініціативах дозволяє державам ефективно протидіяти кіберзлочинності через гармонізацію зусиль, створення спільних платформ для обміну інформацією та забезпечення кращого реагування на нові загрози в кіберпросторі [171, с. 15-16]. Всесвітня організація інтелектуальної власності (ВОІВ) відіграє важливу роль у забезпеченні охорони інтелектуальної власності в контексті швидкого розвитку технологій і Інтернету. Один з основних аспектів її діяльності стосується виконання міжнародних угод, що забезпечують захист авторських прав у кіберпросторі, зокрема через Інтернет-договори 1996 року – Договір про авторське право та Договір про виконання та фонограми. На сьогодні ВОІВ продовжує працювати над удосконаленням міжнародних норм в сфері інтелектуальної власності для Інтернету. Проте забезпечення гармонізації правових норм у різних юрисдикціях залишається складним завданням, оскільки не всі країни одночасно впроваджують відповідні зміни в своє національне законодавство. Крім того, нові технології, такі як штучний інтелект та блокчейн, можуть вимагати подальших змін у міжнародному правовому регулюванні інтелектуальної власності.

Таким чином, хоча ВОІВ і зробила певні кроки в забезпеченні охорони авторських прав в Інтернеті, багато питань, зокрема щодо захисту контенту в реальному часі, залишаються відкритими [64, с. 82-83].

Генеральна Асамблея ООН відіграє ключову роль у розробці міжнародних ініціатив, спрямованих на боротьбу з кіберзлочинністю, і є важливим консультативним органом, що координує співпрацю між державами-членами ООН. Через свою універсальність та масштаб діяльності, Асамблея займається розглядом питань, що стосуються глобальної безпеки в інформаційному просторі, і є платформою для визначення основних

напрямків міжнародного співробітництва в цій сфері. Завдяки своїй універсальності та координаційній ролі Генеральна Асамблея ООН здатна об'єднувати країни для вирішення глобальних проблем кібербезпеки, визначати принципи та рамки міжнародної співпраці у протидії кіберзлочинності, а також створювати основи для формування ефективних правових і організаційних механізмів у цій сфері [161, с. 77-80]. Практика Китаю в створенні «національного Інтернету», яку часто називають «Великий Китайський Фаєрвол», дійсно є цікавим прикладом, що може вплинути на інші країни та міжнародні об'єднання. Китайський підхід передбачає ретельний контроль над доступом до Інтернету, блокування зовнішніх вебсайтів, обмеження доступу до певних міжнародних ресурсів і фільтрацію інформації, що є частиною ширшої стратегії контролю над інформаційним простором. Технології та політика, що ведуть до ізоляції Інтернету в окремих країнах, можуть мати глибокі наслідки для міжнародних відносин, економіки та безпеки. Україні варто серйозно розглядати такі можливості та активно брати участь у міжнародних дискусіях щодо майбутнього глобального Інтернету, щоб уникнути потенційної ізоляції, одночасно забезпечуючи національну безпеку та збереження доступу до глобальних ресурсів [163]. ЮНОДК (Управління Організації Об'єднаних Націй з наркотиків і злочинності) дійсно є важливим майданчиком для міжнародної співпраці у боротьбі з кіберзлочинністю та іншими формами транснаціональних злочинів. З огляду на свою роль у визначенні стандартів у галузі попередження злочинності та кримінального правосуддя, ЮНОДК активно працює над створенням глобальних партнерських зв'язків для вирішення питань безпеки в Інтернеті та кіберпросторі. ЮНОДК грає ключову роль у зміцненні міжнародної співпраці у боротьбі з кіберзлочинністю, надаючи технічну допомогу і мобілізуючи ресурси, включаючи приватний сектор, для вирішення актуальних проблем. Підтримка країн, що розвиваються, є важливим елементом цієї стратегії,

оскільки без глобальної співпраці та зміцнення потенціалу на національному рівні боротьба з кіберзлочинністю не буде ефективною [171, с. 18].

Міжнародний союз електрозв'язку (МСЕ) є важливою спеціалізованою установою в рамках ООН, що активно працює над розвитком глобальних стандартів у сфері електрозв'язку та кібербезпеки. Його роль у боротьбі з кіберзлочинністю та кібершахрайством, зокрема, полягає у стандартизації процедур, обміні досвідом та впровадженні нових ініціатив на міжнародному рівні. Однією з ключових його ініціатив є організація Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства (ВСІС), яка створює платформу для обговорення ключових питань кібербезпеки та сприяє обміну кращими практиками між країнами.

Для ефективної протидії кіберзлочинності та кіберзагрозам в Україні та інших країнах, необхідно впроваджувати певні зміни в національне законодавство, зокрема:

1. Механізм оперативного обмеження (блокування) інформаційних ресурсів. Закріплення в законодавстві процедур блокування доступу до ресурсів, що є джерелами кіберзагроз або порушують законодавство, дасть змогу оперативно реагувати на інциденти.

2. Особливі умови для обшуку і арешту електронних доказів. Важливим є впровадження спеціальних умов для проведення обшуків у кіберпросторі та арешту електронних доказів, зокрема копіювання інформації та її збереження до початку розслідування.

3. Імплементація вимог щодо збереження даних. Встановлення обов'язку для операторів телекомунікацій та провайдерів зберігати дані щодо користувачів і забезпечувати їх цілісність. Це дозволить швидко і ефективно реагувати на правопорушення, пов'язані з інформаційними технологіями.

Роль міжнародних організацій у формуванні стандартів кібербезпеки та забезпеченні ефективної міжнародної співпраці в боротьбі з кіберзлочинністю важко переоцінити, адже лише через спільні зусилля

можна створити надійну систему захисту від кіберзагроз на глобальному рівні [155].

Інтернет-шахрайство стало серйозною проблемою для користувачів в Україні, і ця ситуація постійно погіршується. Останні дані свідчать, що 45% українців, які купують в Інтернеті, стикалися зі спробами шахрайства під час онлайн-шопінгу. Це значне збільшення порівняно з 2020 роком, коли цей показник становив 22%. Проте, незважаючи на зростання кіберзлочинів, українці все ще неохоче звертаються до поліції у випадках онлайн-шахрайства.

Ці результати демонструють необхідність покращення обізнаності громадян про онлайн-шахрайства та вжиття додаткових заходів для захисту користувачів в Інтернеті. В Україні, як і в інших країнах Європи, залишається проблема недостатньої уваги до цієї теми, зокрема щодо звернення до поліції, і важливим кроком буде розвиток освітніх програм для підвищення цифрової грамотності та безпеки в мережі.

Згідно з даними Всесвітнього економічного форуму, кіберзагрози стали одним із основних ризиків для світової економіки, що підкреслює серйозність ситуації з кібербезпекою. На жаль, низький рівень довіри до правоохоронних органів та небагато звернень до поліції в Україні та ЄС створюють сприятливі умови для шахраїв, що, в свою чергу, збільшує кількість атак. Зважаючи на зростаючі кіберзагрози, важливо продовжувати освітні ініціативи та підвищувати рівень цифрової грамотності в Україні. Успішний досвід країн, таких як Польща, може слугувати орієнтиром для розвитку програм, які сприяють безпеці користувачів та ефективному захисту від шахраїв [57].

Кібершахрайство є новим, але схожим на звичайне шахрайство видом правопорушення. Таким чином, хоча за своєю суттю кібершахрайство є схожим на традиційне шахрайство, його методи, інструменти і масштаби значно відрізняються, що вимагає нових підходів до боротьби з цим видом кримінальних правопорушень [14, с. 41; 38, с. 59–61, 198].

Аналіз причин та умов, що зумовлюють поширення кібершахрайства у воєнний час, є важливим для розробки ефективних заходів протидії цим кримінальним правопорушенням.

Причини поширення кібершахрайства:

1. Соціально-економічні проблеми: бідність та безробіття; втрата стабільності.

2. Психологічний стан: психічне перевантаження; втрати близьких осіб;

3. Фактори, що приваблюють злочинців: анонімність в Інтернеті; доступність кримінальних правопорушень; складність їх виявлення.

4. Обтяжена робота правоохоронних органів:

- у період війни правоохоронні органи часто зосереджені на фізичних загрозах та порушеннях, що пов'язані з бойовими діями, що залишає менш часу і ресурсів для боротьби з кіберзлочинністю.

- зібрання інформації про кіберзлочини у такий час може бути ускладнене через низький рівень координації та обмежену взаємодію між органами різних країн та організацій.

В умовах війни боротьба з кіберзлочинністю потребує комплексного підходу, поєднуючи ефективне реагування правоохоронців, співпрацю на міжнародному рівні та освіту громадян про потенційні загрози в Інтернеті.

В умовах війни, коли правоохоронні органи зосереджені на вирішенні низки нагальних питань, таких як перевірка документів, патрулювання, встановлення блокпостів і контроль за гуманітарною допомогою, виникає високий ризик, що шахраї скористаються цією ситуацією.

Шахраї використовують ситуацію, коли правоохоронні органи перебувають під значним навантаженням через і обставини, і займаються кримінальною діяльністю, зокрема через Інтернет [195]. Вони можуть залишатися безкарними через труднощі в боротьбі з кіберзлочинністю та забороненою онлайн-торгівлею. Для ефективної протидії цьому необхідно посилити контроль, підвищити обізнаність громадян та забезпечити більше співпраці між правоохоронцями та онлайн-платформами.

У воєнний час шахрайство набуває нових форм і схем, використовуючи вразливість людей та ситуацію нестабільності. Ось деякі з найбільш поширених шахрайських схем, що можуть бути актуальними під час війни:

1. Пропозиції з оренди неіснуючого чи вже зайнятого житла.

2. Фейкові перевезення та квитки для в'їзду в місто.

3. Недійсні талони на паливо.

4. Маніпуляції з продажу затребуваних товарів.

5. Надання недостовірної інформації про родичів та полонених військових.

6. Різного роду збори у соціальних мережах на допомогу військовим та постраждалим особам.

У цьому контексті боротьба з кіберзлочинністю в умовах війни вимагає комплексного підходу, включаючи законодавчі зміни, посилення контролю за Інтернетом і регулярне інформування громадян про можливі шахрайські схеми.

Схема шахрайства, яка передбачає пропозицію отримання грошової допомоги від держави, міжнародних організацій чи благодійних фондів, є однією з найпоширеніших у часи кризи, особливо під час воєнних дій або інших надзвичайних ситуацій. З огляду на зростаючі технологічні можливості та вплив кризових ситуацій, кіберзлочинці продовжують адаптувати свої методи до нових реалій, тому важливо постійно підвищувати свою кіберобізнаність і обережність при взаємодії з цифровими платформами [95, с. 522].

З метою ефективнішого реагування на зростаючий рівень кіберзлочинності, Верховна Рада України внесла низку важливих змін до кримінального та кримінального процесуального законодавства, аби удосконалити підстави та механізми притягнення до кримінальної відповідальності кіберзлочинців. Зокрема, ці зміни були спрямовані на підвищення ефективності боротьби з кіберзлочинністю, а саме в умовах воєнного стану.

В умовах воєнного стану кіберзлочини можуть мати серйозні наслідки для безпеки держави. Атаки на критичну інфраструктуру, зокрема енергетичні, транспортні або комунікаційні системи, можуть мати катастрофічні наслідки. Тому ці зміни в законодавстві покликані не тільки підвищити ефективність боротьби з кіберзлочинністю, а й забезпечити надійний захист країни від потенційних загроз з боку кіберзлочинців, особливо в період кризи.

Загалом, ці законодавчі ініціативи є важливим кроком до побудови більш безпечного кіберпростору для українських громадян і підприємств в умовах надзвичайної ситуації [138; 147].

Дійсно, посилення кримінальної відповідальності, розширення повноважень правоохоронних органів і додаткові механізми криміналізації окремих діянь без сумніву є важливими кроками у боротьбі з кіберзлочинністю. Однак, проблема полягає в тому, що більшість кримінологічних досліджень з цього питання здебільшого фокусуються лише на статистичних даних про злочинність, що фіксуються у відповідних реєстрах правоохоронних органів, і не охоплюють глибший аналіз причин, що спричиняють цей вид злочинності.

Щоб ефективніше боротися з кіберзлочинністю, необхідно не лише вивчати юридичні аспекти та кримінальні покарання, а й звертати увагу на широкий спектр факторів, що сприяють її поширенню.

Для ефективної боротьби з кіберзлочинністю необхідно не лише покращити кримінально-правову відповідальність та розширити повноваження правоохоронних органів, а й глибше досліджувати соціальні, економічні, політичні, демографічні та організаційні фактори, що сприяють поширенню кіберзлочинів. Це дозволить розробляти комплексні стратегії, спрямовані не тільки на каральну функцію, але й на профілактику злочинності та підвищення загальної кіберграмотності населення.

У 2021 році в Україні спостерігалося зростання збитків від незаконних дій із платіжними картками, хоча їх рівень все ще залишається відносно

низьким, за даними Національного банку. Кіберполіція досягла значного прогресу у боротьбі з інтернет-шахрайством, скерувавши до суду понад 2000 кримінальних проваджень, у яких були викриті 422 зловмисники. Водночас у роботі залишаються ще понад 6600 проваджень.

У більшості випадків використовувались такі механізми вчинення інтернет шахрайства – надсилання у меседжері повідомлення з проханням проголосувати за знайому людину та інші прохання, створення спеціальних сайтів з метою виведення коштів, активне використання соціальних мереж для розповсюдження недостовірної інформації, надсилання повідомлень про нібито виграш великої суми тощо.

За даними правоохоронних органів, зловмисники виманили у громадян понад 193 млн грн. І серед цих справ три чверті – це кримінальні правопорушення, вчинені з використанням цифрових технологій [148]. Цей фактор є тривожним і спонукає до розробки методів підвищення ефективності цифрової грамотності населення громадян.

Що стосується курівлі-продажу товарів за допомогою платіжних карток, то на практиці розробляються заходи щодо мінімізації шахрайства у цій сфері. Так, наразі банки удосконалили захист платіжних карток. Це дозволяє зменшити кількість таких правопорушень у торговельній мережі.

Водночас, зростання обсягів шахрайства в Інтернеті підкреслює необхідність підвищення обізнаності користувачів про правила безпечного використання платіжних карток онлайн. Зокрема, важливо не розголошувати персональні дані та уважно ставитися до підозрілих повідомлень чи сайтів. З цією метою Національний банк постійно роз’яснює правила безпечного повадження з платіжними картками.

У 2021 році в Україні спостерігалося зменшення середньої суми шахрайських операцій у торговельній мережі та загалом на одну незаконну операцію. Це свідчить про ефективність впровадження сучасних технологій захисту платіжних систем та зростання обізнаності користувачів про загрози шахрайства.

Однак у 2022 році ситуація змінилася. Середня сума шахрайської операції зросла на 35% і склала 2 206 гривень. Це зростання пов'язане з активізацією шахраїв у кіберпросторі, особливо через використання методів соціальної інженерії. Зокрема, 86% шахрайських операцій відбувалися через Інтернет, а 53% загальної суми збитків припадали на шахрайство, пов'язане з соціальною інженерією [148].

Таким чином, хоча в 2021 році спостерігалося зменшення середньої суми шахрайських операцій, у 2022 році відбулося зростання цього показника, що підкреслює необхідність постійного вдосконалення заходів безпеки та підвищення обізнаності користувачів.

У 2021 році в Україні спостерігалося зростання рівня шахрайства в Інтернеті. На кожен мільйон гривень видаткових операцій із платіжними картками, здійснених онлайн, обсяг збитків збільшився з 61 гривні (у 2020 році) до 114 гривень (у 2021 році). Це свідчить про зростання ризиків, пов'язаних із онлайн-операціями.

Водночас, загальний показник відносних збитків від шахрайства в Україні залишався нижчим порівняно з країнами Європейського Союзу. У 2021 році він становив 0,0065% (65 гривень на мільйон гривень), тоді як у країнах ЄС, за даними Європейського центрального банку, у 2019 році цей показник складав 0,036% (360 євро на мільйон євро) [148].

Зростання шахрайства в Інтернеті в Україні пов'язане з активізацією кіберзлочинців, які використовують методи соціальної інженерії, фішингові посилання та інші шахрайські схеми. Більшість шахрайських випадків сталося під час купівлі чи продажу товарів в Інтернеті – 52,7%. Інші поширені методи включають фішингові посилання (18,6%), злам акаунтів у соцмережах (12%) та виманювання інформації телефоном (10,2%).

Національний банк України у своєму листі від 4 липня 2018 року (№57-0009/36366) надав рекомендації щодо запобігання та протидії шахрайству в банківській системі. Основні акценти цього документа спрямовані на

підвищення рівня безпеки банківських операцій, захист даних клієнтів та посилення протидії шахрайським схемам [149].

З 14 лютого 2022 року стартувала інформаційна кампанія Національного банку України з платіжної безпеки під назвою #ШахрайГудбай. Вона є продовженням успішної кампанії 2020 року і має на меті підвищення рівня обізнаності громадян щодо кібергігієни та формування культури безпечної поведінки в цифровому просторі, зокрема у сфері безготівкових розрахунків.

Кампанія #ШахрайГудбай акцентує увагу на ключових аспектах захисту персональних даних та фінансів, сприяючи підвищенню фінансової та цифрової грамотності серед українців [148].

Сайт кампанії #ШахрайГудбай пропонує широкий спектр порад і рекомендацій щодо платіжної безпеки, що допомагають користувачам уникати шахрайства [148].

Дотримання цих рекомендацій мінімізує ризик шахрайства в онлайн-просторі та підвищує захист ваших фінансів під час здійснення безготівкових розрахунків. Кампанія акцентує увагу на цифровій грамотності та обізнаності громадян як основних чинниках запобігання кіберзлочинам.

У 2017 році Публічне акціонерне товариство «Приватбанк» затвердило положення про запобігання шахрайству, метою якого є реалізація ефективних заходів боротьби з шахрайськими діями та зловживаннями в банківській установі. Це положення також включає механізм отримання зворотного зв'язку для оцінки ефективності впроваджених заходів та їх подальшого вдосконалення.

Метою цієї системи є:

- Запобігання шахрайству та зловживанням, що можуть завдати шкоди банку і його клієнтам.
- Оцінка ефективності реалізованих заходів для подальшого вдосконалення політики безпеки.

- Підвищення загальної обізнаності співробітників про ризики шахрайства та необхідність постійного контролю.

Ця система дозволяє банку ефективно реагувати на змінні шахрайські технології та зміцнювати довіру клієнтів через забезпечення високого рівня захисту від фінансових кримінальних правопорушень [142].

У рамках боротьби з шахрайством, «Приватбанк» запустив послугу «Страхування від шахрайства», яка доступна для всіх користувачів банку. Ця послуга пропонує фінансовий захист від шахрайських операцій, забезпечуючи компенсацію у разі несанкціонованих транзакцій з картки. Ця послуга надає клієнтам фінансову безпеку та захист від шахрайських дій, забезпечуючи відшкодування за потерпілі від несанкціонованих операцій суми [48].

Отже, боротьба з кібершахрайством в Україні реалізується через три основні напрямки діяльності:

- Попередження кіберзлочинів.

Це комплекс заходів, спрямованих на запобігання шахрайствам та злочинам у кіберпросторі. Сюди входять як загальнодержавні заходи (економічні, ідеологічні, правові та виховні), так і спеціалізовані організаційні, технічні та програмні заходи, а також використання криптографії для захисту інформації.

- Організація боротьби з кіберзлочинністю та правоохоронна діяльність.

Включає створення ефективних механізмів виявлення, запобігання та розкриття кіберзлочинів. Для цього активно працюють правоохоронні органи, зокрема Кіберполіція України, яка здійснює розслідування та забезпечує координацію з іншими державними та приватними організаціями.

- Кримінальна відповідальність.

Включає застосування правових заходів для покарання осіб, які вчинили кіберзлочини. Це стосується як покарання безпосередньо через

кримінальні санкції, так і встановлення чітких юридичних норм для боротьби з кіберзлочинністю.

Крім того, в Україні існує велика кількість платформ, що сприяють інформуванню громадян про існуючі шахрайські схеми та способи, як не стати їх жертвою. Одним із таких ресурсів є оновлена вебсторінка #ШахрайГудбай, яку організували Національний банк України разом із партнерами для підвищення обізнаності громадян щодо платіжного шахрайства та кібербезпеки в цілому [38].

Кампанії на кшталт #ШахрайГудбай надають користувачам детальну інформацію про правила безпеки в онлайн-просторі та допомагають сформувати культуру обережної поведінки серед громадян.

Загалом, ефективне розслідування кіберзлочинності вимагає комплексного підходу, застосування спеціалізованих засобів, а також активної інформативної роботи серед населення.

Висновки до розділу 3

1. 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 факторів. По-перше, процес тимчасового доступу до документів та речей часто затягується. Цей захід є важливим, але повільним і залежить від численних додаткових кроків, таких як необхідність присутності представника організації, у володінні якої знаходяться потрібні документи чи матеріали (наприклад, банківських установ, операторів телекомунікаційних послуг). Це ускладнює процес і збільшує час, необхідний 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 у кримінальному процесуальному законодавстві. Так, у КПК України

відсутні чіткі вказівки щодо терміну, протягом 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.

2. 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; інвестувати у спеціалізовані технології для виявлення шахрайства, такі як програми для моніторингу транзакцій, аналізу поведінки користувачів та використання машинного навчання для виявлення аномалій; залучати зовнішніх експертів для проведення аудитів і розслідувань, що дозволить виявити можливі слабкі місця в захисті і покращити системи безпеки, розвивати законодавчу базу, що регулює протидію шахрайства, включаючи посилення відповідальності за шахрайські дії в Інтернеті.

3. 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 і обміну даними); навчання фахівців (підготовка кіберекспертів, здатних працювати з цифровими доказами та 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 ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абламський С. Є., Конюшенко Я. Ю. Стратегічне управління у сфері протидії злочинності в Україні. *Форум права*. 2023. № 1 (74). С. 122–131. DOI: https://doi.org/10.5281/zenodo.7699516.

2. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. К.: Атіка, 2007. 304 с.

3. Александров О. О., Дудоров В. А., Клименко В. А. та ін. Кримінальне право України. Особлива частина: підручник. За ред. М. І. Мельника, В. А. Клименка. 3-тє вид., переробл. та допов. Київ: Атіка, 2009. 744 с.

4. Ангеленюк А.-М. Ю. Використання електронних доказів у кримінальному процесуальному праві україни (проблемні питання). *Науковий вісник Ужгородського Національного Університету, 2023. Серія «Право»*. Випуск 79, частина 2. С. 214-218. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/289572/283146.

5. Ахтирська Н. М., Томас Ж. Ю. Актуальні питання розслідування злочинів проти власності: навч. посіб. К.: ВПЦ «Київський університет», 2018. 246 с.

6. Баулін Ю. В., Борисов В. І., Тютюгін В. І. та ін. Кримінальне право України: Особлива частина: підручник. За ред. В. В. Сташиса, В. Я. Тація. 4-те вид, переробл. і допов. Харків: Право, 2010. 608 с.

7. Башкатов О., Дружинін Г. та ін. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж. Донецьк : ДНДІСЕ, 2010. 179 с.

8. Бельський Ю. А. Кримінальна відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку : дис. ... канд. юрид. наук: 12.00.08. К., 2017. 253 с.;

9. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2008. 20 с.

10. Бодунова О. М. Запобігання кібершахрайству у фінансовому секторі // *Ірпінський юридичний часопис: науковий журнал (Серія : право).* – 2023. Вип. 3 (12). С. 194–200.

11. Бодунова О. М., Грицюк І. В. Особливості судової (кримінальної) термінології в Україні. *Юридичний науковий електронний журнал.* 2022. № 12. С. 89–94. URL : http://lsej.org.ua/12_2022/142.pdf.

12. Вакуленко О. В., Стрільців О. М., Тарасенко О. С. та ін. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. Київ: Нац. акад. внутр. справ, 2016. 56 с.

13. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. В. Т. Бусел. Київ, Ірпінь : ВТФ «Перун», 2005. 1728 с.

14. Веліканов С. В., Волобуєв А. Ф., Журавель В. А., та ін. Криміналістична профілактика економічних злочинів: науково-практичний посібник. Харків : «Харків юридичний», 2006. 236 с.

15. Веліканов С.В. Ситуаційний підхід як засіб підвищення ефективності організації розслідування злочинів. *Правові засади підвищення ефективності боротьби зі злочинністю в Україні* : матеріали міжнар. наук. конф., 15 трав. 2008 р. Х., 2008. С. 181–184.

16. Вирок по справі № 199/3015/17 від 20.05.2022. Жовтневий районний суд м. Дніпропетровська. URL: https://reyestr.court.gov.ua/Review/104513473.

17. Вирок по справі № 299/1169/13-к від 28.05.2013. Виноградівський районний суд Закарпатської області. URL: https://reyestr.court.gov.ua/Review/31501462.

18. Вирок по справі № 331/1761/14-к від 28.05.2014. Жовтневий районний суд м. Запоріжжя. URL: https://reyestr.court.gov.ua/Review/39274951.

19. Вирок по справі № 422/2128/14-к від 03.06.2014. Перевальський районний суд Луганської області. URL: https://reyestr.court.gov.ua/Review/39148923.

20. Вирок по справі № 442/3925/17 від 13.07.2018. Дрогобицький міськрайонний суд Львівської області. URL: https://reyestr.court.gov.ua/Review/75286407.

21. Вирок по справі № 523/7978/17 від 22.07.2018. Суворовський районний суд м. Одеси. URL:https://reyestr.court.gov.ua/Review/72548283.

22. Вирок по справі № 592/9048/14-к від 16.10.2018. Ковпаківський районний суд м. Суми. URL:https://reyestr.court.gov.ua/Review/77239091.

23. Вирок по справі № 712/9535/14-к від 21.10.2015. Соснівський районний суд м. Черкаси. URL: https://reyestr.court.gov.ua/Review/52533810.

24. Вирок по справі № 752/13250/13-к від 23.06.2014. Голосіївський районний суд міста Києва. URL: https://reyestr.court.gov.ua/Review/39609762.

25. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і Безпека*. 2011. № 4. С. 107-112.

26. Волобоєв А. Оцінка первинної інформації та коло обставин, що підлягають встановленню під час розкриття кібершахрайств. *Věda a perspektivy*. 2024. № 4 (35). С. 135-148.

27. Воробйова К. В. Криміналістична характеристика шахрайств, що вчиняються у сферах використання електронних технологій. *Від громадянського суспільства – до правової держави*: тези VIII Міжнар. наук. інтернет-конф. студентів та молодих вчених. Харків: Харк. нац. ун-т ім. В. Н. Каразіна, 2013. С. 96–99.

28. Воронов І. О. Феномен BOTNET – латентна мобілізація сегментів мережі Інтернет для вчинення злочинів у сфері високих інформаційних

технологій. Вісн. Луган. держ. ун-ту внутрішніх справ. Луганськ, 2010. № 3. С. 275–287.

29. Головкін С. В. Криміналістична характеристика шахрайства відносно власності особи та її використання на початковому етапі розслідування: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2008. 216 с.

30. Горлач В. М., Макар В. М. Побудова та адміністрування INTRANET-мереж. Ч. 1. Основи мережних технологій : Тексти лекцій. Львів, 1999. 45 с.

31. Господарський процесуальний кодекс України : Закон України від 06.11.1991 № 1798-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1798-12.

32. Гребенюк М., Черняк А. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємство, господарство і право*. № 3. 2019. С. 297-303.

33. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. 2014. № 4. С. 312-317.

34. Гутник А. В., Хитра А. Я. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні : монографія. Львів : ЛьвДУВС, 2022. 204 с.

35. Гуцу С.Ф. Правове регулювання мережі «Інтернет»: міжнародний і вітчизняний досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. Випуск 2 (38). С. 114–118.

36. Дерещук Т. М., Струтинська Т. З., Романченко В. В. Виклики на шляху ефективної протидії кіберзлочинності в Європейському Союзі. *Філософія та політологія в контексті сучасної культури.* 2022. Т. 14. № 2. С. 110-118.

37. Дзьобань О. П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. *STRATEGICPRIORITIES*. 2017. № 3 (44). С. 163–170.

38. Діброва Т. А., Пісенко Д. О., Сметаніна Н. В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С. 547-549. URL: http://lsej.org.ua/11_2022/132.pdf.

39. Довженко О.Ю. Класифікація кіберзлочинів у криміналістиці. *Протидія злочинності: проблеми практики та науково-методичне забезпечення*. 2019. №1. С. 19-22. URL: http://sulj.oduvs.od.ua/archive/2019/1/7.pdf

40. Домінова І.В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Науково-виробничий журнал «Бізнес-навігатор»*.2017. Випуск 4-2 (43). С. 92-98.

41. Досвід країн Європейського Союзу щодо виявлення та розслідування відмивання злочинних доходів із використанням цифрової валюти (криптовалюти): метод. рек. С. С. Чернявський, І. Кржечковськис, В. В. Тацієнко та ін. Київ : Нац. акад. внутр. справ, 2017. 86 с.

42. Дубина М. В., Садчикова І. В., Середюк І. О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України. Журнал «Бізнес Інформ». URL: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349 _359.pdf.

43. Економічні злочини та шахрайство: досвід українських організацій. Офіційний сайт видання «Економічна правда». URL: https://www.epravda.com.ua/columns/2020/12/17/669308/.

44. Єдиний портал органів системи МВС України. URL: https://mvs.gov.ua/ua/news/9190_Pracivniki_Departamentu_Interpolu_ta_vropolu_Nacpolicii_Ukraini_rozshukuyut_svidkiv_podii_v_Londoni.htm.

45. Єфімов М. М., Павлова Н. В., Чучко С. В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу «Інтернет»: теоретичні та праксеологічні засади : монографія. Одеса : Видавничий дім «Гельветика», 2022. 200 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/10224/1/Єфімов%20М.%20М.%2с

%20Павлова%20Н.%20В.%2с%20Чучко%20С.%20В._Методика%20розслідування%20шахрайств.pdf.

46. Єфімова О. І., Коваль С. М. Узагальнення судової практики розгляду слідчими суддями клопотань сторін кримінального провадження про тимчасовий доступ до речей та документів відповідно до статей 159–166 КПК України. Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/Uzag4.doc.

47. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. *Часопис Академії адвокатури України.* 2012. № 17. С. 1-6.

48. Захист від шахрайства. *Офіційний сайт ПриватБанку.* URL: https://privatbank.ua/strahovaniye/zakhyst-vid-shakhraystva

49. Зачек О. І., Захарова О. В., Навроцька В. В., Федчак І. А. Особливості розкриття та розслідування кіберзлочинів: метод. рек. Львів: Львів. держ. ун-т внутр. справ, 2010. 92 с.

50. Заяць К.Д. Методика розслідування шахрайств : дис. ... канд. юрид. наук : 12.00.09. Харківський нац. ун-т внутр. справ. Харків, 2020. 196 с.

51. Золотарьов С. О. Судова комп'ютерно-технічна експертиза та її роль у боротьбі з кіберзлочинами. *Протидія кіберзлочинності та торгівлі людьми*. Збірник матеріалів Міжнар. наук.-практ. конференції. Харків, 27 травня 2020 р. С. 95–96.

52. Інструкція з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні. Наказ МВС України від 07.07.2017 № 575. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/z0937-17#Text.

53. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України. Наказ

МВС України від 27.04.2020 № 357. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/ z0443-20#Text,

54. Казначеєва Д. В., Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник кримінологічної асоціації України*. 2021. № 2 (25). С. 149-157. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/882dbcb7-bd33-412f-8a0c-94491e535d4d/content.

55. Каланча І. Г., Столітній А. В. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності*. 2019. Вип. 146. С. 179–191.

56. Капцош В. Я. Стан та особливості розвитку інтернет-торгівлі товарами в міжнародному вимірі. *Науковий вісник Ужгородського національного університету.* 2017. № 13 (1). С. 115–119.

57. Карта кібершахрайств: як обманюють користувачів в Україні та ЄС. Офіційний сайт інтернет-видання «Новий погляд». URL: http://np.org.ua/2021/12/08/karta-kibershahrajstv-yak-obmanyuyut-korystuvachiv-v-ukrayini-ta-yes/

58. Карчевський М. В. Злочин у сфері використання інформаційних технологій: визначення поняття. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2013. № 4. С. 77–86.

59. Карчевський М. В., Дудоров О. О. Проблеми кримінально-правової кваліфікації злочинів проти власності, вчинюваних із використанням платіжних карток або їх реквізитів. *Кримінальне судочинство*. *Судова практика у кримінальних справах*. 2014. № 1. С. 97–123.

60. Карчевський М. В., Коваленко В. В., Комлєв В. Є. та ін. Протидія злочинам у сфері використання інформаційних технологій : інтегр. навч.-практ. посіб. За ред. М. В. Карчевського Харків : Право, 2019. 188 с.

61. Качашвілі К. С. Проблема інтернет-шахрайства в Україні та способи боротьби із ним. URL: http://dspace.puet.edu.ua/bitstream/123456789/9762/1/Качашвілі%20К.С..pdf.

62. Кирбят'єв О. О. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : дис. ... канд. юрид. наук: 12.00.08. Запоріжжя, 2015. 200 с.

63. Кириленко Н. Ю. Методика розслідування шахрайства у сфері побутових відносин: дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Одеса, 2013. 236 с.

64. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. *Актуальні проблеми міжнародних відносин.* 2015. Випуск 126 (частина ІІ). С. 77-90.

65. Кіберзлочинність: проблеми боротьби і прогнози. Антикібер Національне антикорупційне бюро. URL: http://anticyber.com.ua.

66. Кіпа О.О. Правопорушення в мережі «Інтернет». *Часопис Київського університету права*. 2010. № 4. С. 346–349.

67. Коба В.Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції. дис. ... докт. філос. права: спец. 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Дніпро, 2024. URL: https://dduvs.edu.ua/wp-content/uploads/files/Structure/science/rada/new_d0872702/2023/4/3/d3.pdf

68. Коваленко І. О. Розслідування шахрайства у сфері використання банківських електронних платежів : дис. ... доктор філософії. Дніпро, 2022. 236 с.

69. Кодекс адміністративного судочинства України : Закон України від 06.07.2005 № 2747-IV. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text.

70. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. № 8. С. 418–421.

71. Колесник В. Г. Проблемні питання збереження, фіксації та дослідження інформації в сучасних мобільних телефонах. *Протидія кіберзлочинності та торгівлі людьми*. Збірник матер. Міжнар. наук.-практ. конференції. Харків, 27 травня 2020 р. С. 102–105.

72. Коліса Я. Ю. Взаємодія служб у боротьбі з кіберзлочинністю. *Криміналістичний вісник.* 2015. № 1 (23). URL: http://elar.naiau.kiev.ua/bitstream/123456789/1868/1/%D0%9A%D0%BE%D0%BB%D1%96%D1%81%D0%B0%20%D0%AF.%20%D0%AE..pdf.

73. Комп`ютерно-технічна експертиза. Офіційний сайт Київського науково-дослідного інституту судових експертиз. URL: https://kndise.gov.ua/kompyuterno-tehnichna.

74. Конвенція ООН про боротьбу з незаконним обігом наркотичних засобів і психотропних речовин: *ратифіковано Постановою ВР № 1000-XII (1000-12) від 25.04.91*. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/1000-12.

75. Конвенція ООН проти корупції: *ратифіковано із заявами Законом № 251-V (251-16) від 18.10.2006*. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/995_c16#Text.

76. Конвенція ООН проти транснаціональної організованої злочинності: *ратифіковано Законом № 1433-IV (1433-15) від 04.02.2004*. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: *https://zakon.rada.gov.ua/laws/show/995_789#Text.*

77. Конвенція про кіберзлочинність: ратифіковано Законом 2824-IV (2824-15) від 07.09.2005. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

78. Конгреси ООН щодо запобігання злочинності та поводження з правопорушниками. Юридична енциклопедія: у 6 т. Ред. кол.: Ю. С. Шемшученко [та ін.]. К. : Українська енциклопедія ім. М. П. Бажана, 2001. Т. 3 : К. 792 с.

79. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського національного університету*. 2021. С. 220-224.

80. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. База даних «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

81. Користін О. Є., Бутузов В. М., Василевич В. В. та ін. Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб. Київ: Видавничий дім «Скіф», 2012. 728 с.;

82. Коршенко В. А. Методи судової телекомунікаційної експертизи. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. Вип. 3 (79). С. 224–230.

83. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2017. 20 с.

84. Коршенко В. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice*. 2017. Вип. 2. С. 197–199.

85. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки : дис. .... доктор філософії. Київ, 2021. 255 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/91e29df8-f347-4437-b46d-266bf4909664/content.

86. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків. нац. ун-т внутр. справ. Харків, 2016. 16 с.

87. Кривенко О. І. Міжнародний досвід протидії шахрайствам, що вчиняються через мережу Інтернет (на прикладі Європейського Союзу та Сполучених Штатів Америки). *Форум права*: електрон. наук. фахове вид.

2017. № 5. С. 208–212. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2017_5_32.pdf.

88. Крижевський А. В. Криміналістична характеристика шахрайств у сфері мобільного зв'язку: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2012. 20 с.

89. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

90. Кримінальний процес (у схемах і таблицях) / Criminal process (in diagrams and tables) : навчальний посібник / П. В. Цимбал, Л. В. Омельчук, О. В. Сіренко, Н. А. Лугіна [та ін.] / за заг. ред. В. В. Топчія ; Державний податковий університет. – Ірпінь, 2024. – 232 с.

91. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/ 4651-17#Text.

92. Криушенко Л. І. Особливості виявлення обставин, що підлягають з’ясуванню під час розслідування шахрайства в банківській сфері. *Науковий вісник Ужгородського національного університету*. 2016. Випуск 39, т. 2. URL: http://surl.li/qepzik.

93. Кулик Я. О. Проблеми призначення судової експертизи у кримінальному провадженні. *ΛΌГОΣ. ОНЛАЙН*. 2020. URL: https://www.ukrlogos.in.ua/10.11232-2663-4139.16.68.html.

94. Курман О. В. Методика розслідування шахрайства з фінансовими ресурсами. Дис... канд. юрид. наук: 12.00.09. Національна юридична академія України ім. Ярослава Мудрого. Х., 2002. 227 с.

95. Левківська Я. І. Вплив воєнного стану на трансформування та розвиток інтернет-шахрайства в Україні. URL: http://dspace.onua.edu.ua/handle/11300/19993.

96. Лефтеров Л. В. Запобігання підрозділами Національної поліції шахрайству, що вчиняється з використанням засобів електронних комунікацій: автореф. дис. ... канд. юрид. наук : 12.00.08. Одес. держ. ун-т внутр. справ. Одеса, 2019. 20 с.

97. 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.

98. 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.

99. Липкан І. І., Топчій В. В. Проблемні питання розслідування шахрайств, вчинених з використанням цифрових технологій. *Юридична наука*. 2020. № 3. Том 2. С. 189-194. URL: ???

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

101. 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.

102. 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. 167–170.

103. 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. 232–234.

104. 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. 122–124.

105. Лугіна Н. А., Лучук А. М. Оптимізація правового регулювання боротьби з кібершахрайством: зарубіжний досвід та його значущість в українській практиці. *Юридичний науковий електронний журнал*. № 1. 2021. С. 238-241.

106. Лук'янчиков Є.Д., Лук'янчиков Б.Є. Участь спеціаліста в розслідуванні комп`ютерних злочинів. *Актуальні питання розслідування кіберзлочинів.* Матеріали Міжнародної науково-практичної конференції. Харків. 2013. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/553/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf?sequence=1&isAllowed=y.

107. Майстренко М. М., Татарин І.І. Проблемні аспекти доказування шахрайств, вчинених у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2021. № 52. С. 85-89. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/4227/1/майстренко%202.pdf

108. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека*. 2015. № 2. С. 107-113.

109. Метелев О. П. Проблеми визначення допустимості і належності електронних (цифрових) доказів у кримінальному процесі. *Вісник кримінального судочинства.* 2019. № 3. С. 224–238.

110. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в*

Україні: правові та організаційні питання: матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовт. 2016 р.). Одеса: ОДУВС, 2016. С. 155–157.

111. Міжнародна конвенція ООН про боротьбу з фінансуванням тероризму: *ратифіковано із заявою Законом № 149-IV (*149-15*) від 12.09.2002*. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_518#Text.

112. Мізерак А.Б. Шахрайство при інтернет-торгівлі: схеми та аспекти запобігання. *Маркетинг і контролінг: сучасні виклики підприємництв*. Київ, 2017. С. 153–155.

113. Міхайліна Т. В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : автореф. дис. ... канд. юрид. наук : 12.00.08. К., 2011. 20 с.

114. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань*: матеріали міжвузівської наук.-практ. конф. (Донецьк, 22 груд. 2000 р.). Донецьк. ін-т внутр. справ, 2001. С. 81–85.

115. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2005. 20 с.

116. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах: автореф. дис... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Харків, 2007. 19 с.

117. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучасних умовах: монографія. За ред. проф. В. Ю. Шепітька. Харків: Право, 2010. 168 с.

118. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304–307.

119. Неділько Я. В. Розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій. дис. док-ра філос. 081 – Право. Київський національний університет імені Тараса Шевченка, Київ, 2021. 254 с

120. Орлов О. В., Онищенко Ю. М. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. *Теорія та практика державного управління*. 2013. Вип. 4 (43). С. 1-6.

121. Орлов С. О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : дис. ... канд. юрид. наук: 12.00.08. Х., 2004. 213 с.

122. Офіційний сайт Української міжбанківської асоціації платіжної системи ЄМА. URL: https://ema.com.ua/fraud-digest-25-07-2017/.

123. Охрімчук Т. В. Криміналістична характеристика шахрайства з фінансовими ресурсами та основні напрями розслідування: автореф. дис. ... канд. юрид. наук: спец. 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Київ, 2011. 16 с.

124. Павлик М. П. Розслідування злочинів у сфері надання послуг із працевлаштування за кордоном: дис. док-ра філос. 081 – Право. Національна академія внутрішніх справ, Київ, 2021. 254 с.

125. Павлова Н. В., Біденчук Т. М. Встановлення психологічного контакту під час допиту громадянина іншої держави за участю перекладача. *Jurnalul Juridic National: teorie si practica: Международный научно-практический правовой журнал*. 2019. № 2 (2). С. 94-97.

126. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: дис... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Харків, 2006. 215 с.

127. 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: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза». Київ, 2005. 18 с.

128. Патик А. А. Взаємодія слідчих та оперативно-розшукових підрозділів при розкритті та розслідуванні майнових злочинів: автореф. дис. ... канд. юрид. наук: 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». К., 2011. 17 с.

129. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. ... канд. юрид. наук : 12.00.09. Харків, 2007. 228 с.

130. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 45-46.

131. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений*. 2019. № 12/1. С. 55-59.

132. Письменна О. П., Баранова О. С., Шкринда О. М. Захист прав споживачів під час придбання продукції через мережу «Інтернет». *Електронне наукове видання «Порівняльно-аналітичне право»*. № 1. 2015. С. 59–62.

133. Пістунов І. М., Кочура Є. В. Безпека електронної комерції: навч. посібн. Нац. гірн. ун–т. Електрон. текст. дані. Д. : НГУ, 2014. 125 с.

134. Порядок ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події. Наказ МВС України від 08.02.2019 № 100. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/ z0223-19#Text

135. Постанова колегії суддів Першої судової палати ККС ВС від 28 січня 2021 року у справі № 182/523/16-к (провадження № 51-1103км20). URL: https://reyestr.court.gov.ua/Review/94553286.

136. Правила продажу товарів на замовлення та поза торговельними або офісними приміщеннями : затв. наказом Міністерства економіки України від 19.04.2007 № 103. *Офіційний вебпортал Верховної Ради України.* URL: http://zakon.rada.gov.ua/laws/show/z1181–07.

137. Про банки та банківську діяльність : Закон України № 2121-III від 7 грудня 2000 р. *Офіційний вебпортал Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text

138. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану від 24.02.2022 No 2149-IX. *Офіційний вебпортал Верховної Ради України.*URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

139. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам: Закон України від 15 березня 2022 року № 2137-IX / Верховна Рада України URL : https://zakon.rada.gov.ua/laws/show/2137-20#Text.

140. Про електронні комунікації: Закон України ві 16 грудня 2020 року № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#top.

141. Про електронну комерцію: Закон України від 3 вересня 2015 року № 675-VIII. URL: http://zakon2.rada.gov.ua/laws/ show/675–19.

142. Про запобігання шахрайству: Положення затв. рішенням Правління банку «ПриватБанк» від 28.09.2017 р. URL: https://static.privatbank.ua/files/politika-zapobigannya-shaxrajstva-ta-korupcii.pdf

143. Про застосування реєстраторів розрахункових операцій у сфері торгівлі, громадського харчування та послуг : Закон України від 6 липня 1995 року. No 265/95-ВР. / Верховна Рада України URL : https://zakon.rada.gov.ua/laws/main/index.

144. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Національної поліції України від 10 листопада 2015 року № 85 / Верховна Рада України URL :

https://cyberpolice.gov.ua/Legislation-and-other-normative-legal-acts-in-the-field-of-prevention-of-corruption/

145. Про міжнародні договори України: Закон України від 29 червня 2004 року № 1906-IV / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/1906-15.

146. Про платіжні послуги : Закон України від 30 червня 2021 року № 1591-IX. / Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/1591-20#n1249

147. Проект Закону про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів : від 01.09.2020 № 4004. Ініціатори С. А. Мінько, О. С. Бакумов, Г. О. Михайлюк та ін. // БД «Законодавство України» / ВР України. URL:https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69771.

148. Проєкт «#ШахрайГудбай». Офіційний сайт Національного банку України. URL: https://promo.bank.gov.ua/stopfraud/#section-35.

149. Рекомендації для зниження ризику шахрайських операцій» від 4 липня 2018 р. Лист Національного банку України. URL: https:// vk24.ua/regulations_and_jurisprudence/listi/oplata-praci/list-nacionalnogo-banku-ukraini-rekomendacii-dlya-znizhennya-riziku-shakhrayskikh- operaciy.

150. Рішення Вищого антикорупційного суду у справі від 13 липня 2022 року у справі № 991/366/22. Офіційний сайт Єдиного державного реєстру судових рішень. URL: https://reyestr.court.gov.ua/Review/105252483.

151. Розовський Б. Г. Крадіжка або шахрайство: за та проти (репліка під час дискусії*). Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2014. № 1. С. 109–115.

152. Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій. Київ: Вид. Поливода А. В., 2004. 144 с.

153. Романюк В. В., Абламський С. Є. Критерії допустимості цифрових (електронних) доказів у кримінальному процесі *Право і безпека. Law and Safety*. 2024. № 2 (93). С. 140-150.

154. Сабадаш В. П. Шахрайство в електронній комерції: реалії сьогодення. *Вісник Запорізького національного університету.* 2011. № 1. С. 216-220.

155. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету*. No 64. 2021. С. 386-391. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/238897/237481.

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

157. Самойлов О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* Вип.4. 2015. С. 408–411.

158. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: автореф. дис. ... канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Донецьк, 2014. 18 с.

159. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: дис. … канд. юрид. наук: 12.00.09. «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». Донецьк, 2014. 226 с.

160. Самойлов С. В. Шахрайства на Інтернет-аукціонах як один із способів скоєння шахрайств з використанням мереж Інтернет (криміналістична характеристика способу вчинення). *Форум права.* 2011. Вип. 4. С. 645–650.

161. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Актуальна юриспруденція. зб. матеріалів інтернет-конференції. Київ. 2018. С.77-80. URL: http://legalactivity.com.ua.

162. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності. *Міжнародні стандарти з кібербезпеки та їх застосування в Україні* : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). Харків, 2016. С. 59–61.

163. Спроби впровадження міжнародного контролю за діяльністю в Інтернеті під егідою ООН: нові можливості реалізації Україною інформаційного суверенітету: аналітична записка / Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1093/.

164. Стрільців О. М., Крижна В. В., Максименко О. В. та ін. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту: метод. рек. За заг. ред. Ю. Ю. Орлова. Київ: Нац. акад. внутр. справ, 2014. 80 с.

165. Стрільців О. М., Тарасенко О. С., Курилін І. Р. та ін. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет медійного контенту провайдерами програмних послуг та Інтернет-провайдерами: метод. рек. Київ: Нац. акад. внутр. справ, 2017. 44 с.

166. Тарасенко О. С., Гуцалюк М. В., Гавловський В. Д. та ін. Розслідування кримінальних правопорушень, вчинених у сфері захисту інтелектуальної власності з використанням мережі Інтернет: метод. рек. 2-ге вид., доповн. Київ: Міжвід. наук.-дослід. центр з проблем б-би з орг. злоч. при РНБО України; Нац. акад. внутр. справ, 2021. 74 с.

167. Тарасова О. В. Удосконалення законодавства щодо кримінальної відповідальності за шахрайство, учинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. *Актуальні проблеми держави і права.* 2014. Вип. 72. С. 481–488.

168. Тімашов В. О., Діденко Д. Ш. Міжнародний досвід протидії сучасній кіберзлочинності в мережі «Даркнет». *Південноукраїнський правничий часопис*. 2021. № 1. С. 167-171.

169. Ткаченко О., Ткаченко Т. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. № 1. С. 75–86.

170. Топчій В. В., Бодунова О. М. Система кримінальних правопорушень у сфері інформаційних технологій: міжнародно-правовий вимір. *Ірпінський юридичний часопис*. 2023. № 1(10). С. 187–195. URL: https://drive.google.com/file/d/1QYxkSzbanckeo8gw1YyKwjpoJLPXLx08/view.

171. Тринадцятий Конгрес Організацій Об'єднаних Націй по попередженню порушень і кримінальному правосуддю: довідковий документ. Доха, 12-19 квітня 2015 року. 114 с. URL: https://www.unodc.org.

172. Тютюн Т. М. Узагальнення проблемних питань, які виникають при розгляді клопотань про тимчасовий доступ до речей і документів // Київський апеляційний суд : офіц. сайт. URL: https://www.kas.gov.ua/wp-content/uploads/2015/07/12014-kr.pdf.

173. Усманов Р.А. Шахрайство з використанням електронно-обчислювальної техніки: аналіз судової практики. *Науковий вісник Львівського державного університету внутрішніх справ*. 2024. № 1. С. 153-163.

174. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: юридичні науки*. 2023. № 4. С. 97–105. DOI: https://doi.org/10.32782/galician_studies/law-2023-4-14.

175. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2(5). С. 162–175.

176. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України. Київ: Істина, 2004. 504 с.

177. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2013. № 5. С. 256–260. 2013.

178. Цивільний кодекс України : Закон України від 16 січня 2003 року № 435-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

179. Цивільний процесуальний кодекс України : Закон України від 18.03.2004 № 1618-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1618-15.

180. Циганюк Ю., Кучинська О. Система міжнародних стандартів прав людини у кримінальному процесі України. *Право України*. 2019. № 9. С. 50-64.

181. Чернявський С.С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ: Хай-ТекПрес, 2010. 624 с.

182. Чуйко С. В. Розслідування шахрайств при купівлі-продажу товарів через мережу Інтернет : дис. ... доктор філософії. Дніпро, 2021. 276 с.

183. Чупрікова І. Л. Допустимість доказів у світлі нового Кримінального процесуального кодексу : дис. … канд. юрид. наук : 12.00.09. Одеса, 2016. 191 с.

184. Чучко С. В. Щодо регулювання правовідносин у віртуальному просторі при купівлі-продажу товарів через мережу «Інтернет». *Вісник Національного технічного університету України «Київський Політехнічний Інститут». Політологія. Соціологія. Право.* 2020. № 1 (45). С. 78–82.

185. Чучко С.В. Визначення віртуального середовища вчинення шахрайства, пов’язаного із куплею-продажем товарів через мережу «Інтернет»: наукові дискусії. *Кримінальний процес та криміналістика: сучасний стан та перспективи* : матеріали Всеукраїнської науково-практичної конференції (26 лист. 2020 р., м. Харків). Харків : Харківський національний університет внутрішніх справ, 2020. С. 403–405.

186. Чучко С.В. Криміналістичний аналіз шахрайств, пов’язаних із куплею-продажем товарів через мережу «Інтернет». *Актуальні проблеми експертного забезпечення досудового розслідування* : матеріали

регіонального науково-практичного семінару (31 травня 2020 р., м. Дніпро). Дніпро : Дніпр. держ. ун-т внутр. справ, 2020. С. 351–353.

187. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі Інтернет. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 1. С. 145–149.

188. Шапочка С. В. Запобігання шахрайству, що вчиняється з використанням комп'ютерних мереж: дис. … канд. юрид. наук: 12.00.08. Донцьк. юрид. ін.-т. Кривий Ріг, 2018. 302 с.

189. Шапочка С. В. Інформаційна безпека та кібершахрайство : *Внутрішні та зовнішні загрози національній безпеці держави :* матеріали міжнар. наук.- практ. конф. (м. Київ, 2 квіт. 2013 р.); НАВС. Київ: ТОВ «Три К», 2013. С. 188-191.

190. Щербакова Г. Досудове розслідування злочинів, учинених із використанням платіжних інструментів. *Наукові записки Інституту законодавства Верховної Ради України*. Кримінальне права і кримінальний процес. 2017. Вип. 3. С. 41–46.

191. Юдкова К. В. Сфера правового регулювання віртуальної реальності. *Політологія. Соціологія. Право*. 2012. Випуск 2(14). С. 137–140.

192. Яцишин М. Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю: дис. ... канд. юрид. наук (12.00.11) 2019. *Національний авіаційний університет*. 220 с.

193. Ablamskyi S. Ye., Havryliuk L. V., Drozd V. G., Nenia O. V. Substantial Violation of Human Rights and Freedoms as a Prerequisite for Inadmissibility of Evidence. *Justicia*. 2021. Vol. 26, No. 39. Pp. 47–56. DOI: https://doi.org/10.17081/just.26.39.4819. 48.

194. Anderson Ross J. Security engineering: a guide to building dependable distributed systems (2 ed.). Indianapolis, IN: Wiley. 2008. p. 1040.

195. Bodunova O. Participation of mass media in detection of crimes in martial law in Ukraine (on the example of Irpin, Kyiv region) / O. Bodunova, T.

Yatsyk, N. Luhina // Ірпінський юридичний часопис: науковий журнал. 2023. № 2 (11). С. 76–89.

196. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. Brussels, 7.2.2013. Join (2013) URL: http:// www.enisa.europa.eu.

197. Hadnagy C. Social engineering: The art of human hacking. John Wiley & Sons. 2010. P. 310.

198. Nizovtsev Yuriy, Parfylo Oleg, Barabash Olha; Kyrenko, Sergij; Smetanina, Nataliia. Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control*. Volume 25, Issue 2, Pages 297–305. 21 April 2022. URL: https://www.emerald. com/insight/content/doi/10.1108/JMLC-02-2021-0015/full/html.

199. Susan H. Nycum. The Criminal Law Aspects of Computer Abuse: Applicability ofthe State Penal Laws to Computer Abuse (Menlo Park, California, Stanford Research Institute, 1976). Ulrich Sieber, Computerkriminalität und Strafrecht (Cologne, Karl Heymanns Verlag, 1977). URL: http://www.worldcat.org/title/criminal-law-aspects-of-computer-abuse-applicability-of-the-state-penal-laws-to-computerabuse/oclc/654145221/editions?referer=di&editionsView=true

200. Yefimov M., Pavlova N., Fedchenko V., Viktor Pletenets, Oleksandr Kryvopusk. Foreign experience in legal regulation of fraud investigation. *Journal of University of Zulia (Revista de la Universidad del Zulia)*. 2022. Number 38. P. 121–129.

Додаток А

Узагальнені дані

проведеного соціологічного опитування узагальнені дані проведеного соціологічного опитування 89 слідчих, 76 оперативних працівників, 65 прокурорів у 2017-2023 рр. у %

В анкетуванні взяло участь 230 респондентів.

1. Загальний стаж роботи:
а) до 2-х років – **19**
б) від 2-х до 5 років – **41,5**
в) від 5 до 10 років – **11,5**
г) понад 10 років – **28**

2. Чи варто замінювати у законодавстві термін «електронно-обчислювальна техніка» на «цифрові технології»?
а) так **– 41,5**
б) ні – **19**
в) ваш варіант – **11,5**

3. Чи доцільно виокремлювати кваліфікуючі ознаки кібершахрайства у законодавстві (ч. 4 ст. 190 КК України)?
а) так – **74**
б) ні – **26**

4. Чи вважаєте за доцільне розробити методичні рекомендації для слідчих і суддів щодо розслідування та кваліфікації кримінальних правопорушень, пов'язаних із шахрайством в інтернеті?
а) так – **81**
б) ні – **19**

5. Чи потрібно законодавчо закріплювати у кримінальному процесуальному законодавстві поняття «цифрові докази»?
а) так – **82**
б) ні – **18**

Продовження Додатку А

6. Чи потрібно передбачити у КПК України джерела цифрових доказів?

а) так – **85**

б) ні – **15**

7. Чи є ефективним механізм тимчасового доступу до речей і документів, зокрема в контексті кримінальних проваджень, пов'язаних з кібершахрайствами?

а) так – **34**

б) ні – **66**

8. Чи потрібно вдосконалити рівень європейської співпраці-розробка єдиного правового механізму взаємодії політико-правових систем окремих європейських держав?

а) так – **69**

б) ні – **31**

9. Чи виникають у вас проблеми під час доказування у справах про кібершахрайство?

а) так – **73,5**

б) ні – **26,5**

10. Як, на Вашу думку, покращити процес доказування кібершахрайства?

а) проведення спеціальних навчань щодо збирання цифрових доказів – **37**

б) внесення змін до законодавства – **21**

в) належне фінансування діяльності органів досудового розслідування – **13**

г) ваш варіант – **29**

11. Чи співпрацюєте Ви з іноземними колегами у сфері доказування кібершахрайств?

а) так – **62**

Продовження Додатку А

б) ні – **38**

12. Чи брали участь у розслідувань кібератак росії проти України?

а) так – **42**
б) ні – **58**

13. Чи співпрацюєте з експертами перед формуванням клопотання про призначення експертизи у справах про кібершахрайство?

а) так – **52**
б) ні – **48**

Додатку Б

«ЗАТВЕРДЖУЮ»
Проректор
з навчально-методичної роботи
Державного податкового університету
_____ Іван ШЕМЕЛИНЕЦЬ
«02» квітня 2024 року

АКТ
впровадження результатів дисертаційної роботи
Липкана Ігоря Івановича
на тему: «Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій»

Комісія у складі: завідувача навчально-методичного відділу, к.б.н. Качур І. В., заступника директора навчально-наукового інституту права з навчально-методичної роботи, к.ю.н., доцента Лугіної Н. А., гаранта освітньої програми «Правове регулювання публічних та приватних відносин», к.ю.н., доцента Гарбінської-Руденко А. В. склали цей акт про те, що опублікувані результати дисертаційного дослідження Липкана Ігоря Івановича на тему: «Особливості доказування у справах про шахрайство, вчинене з використанням цифрових технологій», подану на здобуття наукового ступеня кандидата юридичних наук зі спеціальності 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність», використовувалися у навчальному процесі при підготовці та проведенні лекційних і семінарських занять з навчальних дисциплін «Судові та правоохоронні органи», «Кримінальне процесуальне право України», «Криміналістика» для підготовки здобувачів вищої освіти першого (бакалаврського) рівня денної та заочної форм навчання галузі знань 08 Право спеціальності 081 «Право» за освітньою програмою «Правове регулювання публічних та приватних відносин» Державного податкового університету, а саме:

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. http://www.law.stateandregions.zp.ua/archive/1_2017/28.pdf

Продовження Додатка Б

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. 167–170.

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. 232–234.

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. 122–124.

Комісія підтверджує, що сформульовані за результатами дослідження Липкана Ігоря Івановича пропозиції, висновки, рекомендації використані при формуванні навчально-методичного забезпечення та проведенні навчальних занять.

Гарант освітньої програми
«Правове регулювання публічних та приватних відносин»,
к.ю.н., доцент **Альона ГАРБІНСЬКА-РУДЕНКО**

Заступник директора ННІ права
з навчально-методичної роботи,
к.ю.н., доцент **Наталія ЛУГІНА**

Завідувач навчально-методичного
відділу, к.б.н. **Ірина КАЧУР**

Додаток В

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.

Продовження Додатка В

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.