МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

КОБА ВАЛЕРІЙ БОРИСОВИЧ

УДК 343.98: 343.131

ДИСЕРТАЦІЯ

ТЕОРЕТИЧНІ ТА ПРАКСЕОЛОГІЧНІ ЗАСАДИ МЕТОДИКИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ

12.00.09 – кримінальний процес та криміналістика; судова експертиза;
оперативно-розшукова діяльність
(081 – «Право»)

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

_____**В. Б. Коба**

Науковий керівник –
Чаплинський Костянтин Олександрович,
доктор юридичних наук, професор

Дніпро – 2024

АНОТАЦІЯ

Коба В. Б. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції. – *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. – Дніпропетровський державний університет внутрішніх справ, Дніпро, 2024.

У дисертації на монографічному рівні опрацьовано теоретичні й праксеологічні засади методики розслідування шахрайства у сфері е-комерції. Здійснено криміналістичний аналіз функціонування сфери е-комерції та визначено фактори, які зумовлюють вчинення шахрайських дій.

Здійснено аналіз юридичних джерел з питань функціонування сфери е-комерції та з'ясовано, що рівень комерційних угод у дистанційному форматі дедалі збільшується. Наголошено на істотній розбіжності у трактуванні низки термінів, які характеризують правовідносини у комерційній сфері, зокрема: «електронна комерція», «електронний бізнес», «електронна торгівля» та ін.

Акцентовано, що популярність комерційної діяльності у віртуальному просторі створила підґрунтя для шахраїв, які діють навіть на транснаціональному рівні.

Наголошено, що спосіб вчинення шахрайства у сфері е-комерції має повноструктурний характер і включає дії із підготовки, безпосереднього вчинення та приховування протиправних дій.

Розкрито й систематизовано типові способи вчинення шахрайства у сфері е-комерції, приділено увагу способам їх приховування, зокрема: знищення інформації, що міститься на електронних носіях (79 %), використання разових номерів мобільних телефонів (81 %), уникнення зорового контакті із потерпілим (81 %), внесення неправдивої інформації в електронні бази даних (27 %), фальсифікація доказів (78 %).

Проведено аналіз наукових думок щодо проблем розслідування шахрайств, учинених із застосуванням комп'ютерних технологій. Зроблено висновок, що найбільш спірним елементом криміналістичної характеристики є обстановка вчинення шахрайства даної категорії, адже внаслідок здійснення електронних комерційних операцій виникає віртуальне середовище, в якому будь-які дії з інформацією вчиняються за допомогою цифрових сигналів і можуть виходити за рамки однієї держави, що ускладнює визначення просторово-часових характеристик.

Зазначено, що у вузькому сенсі місцем вчинення шахрайства у сфері е-комерції є локації розташування програмно-технічних засобів, що зазнали злочинного впливу, та точки їхнього доступу до певних мереж, а також місцезнаходження банкоматів, відділень банку, зон вільного підключення до мережі «Інтернет» із використанням технології «Wi-Fi». У географічному розумінні 92 % усіх «віртуальних комерційних угод» здійснюється у великих містах мегаполісах. При цьому, відсоток суб'єктів, які пропонують товари та послуги комерційного призначення, набагато більше, ніж відсоток осіб, які потребують таких товарів та послуг, що пояснюється дефіцитом таких об'єктів у невеликих містах. Наголошено, що обстановка обов'язково повинна розглядатися, з урахуванням умов, у яких діяв шахрай. Наводиться ряд суб'єктивних та об'єктивних чинників, які визначають можливість, умови та інші обставини вчинення шахрайства у сфері е-комерції.

Виокремлено віртуальні (електронні, цифрові) сліди, характерні для шахрайства у сфері е-комерції. Натомість, наголошено, що матеріальні та ідеальні сліди також відіграють важливу роль при виявленні шахрайства даної категорії. Здебільшого інформацію про зовнішність шахрая потерпілі можуть надати у випадку безпосередньої зустрічі до, або після здійснення комерційної електронної угоди, або якщо спілкування здійснювалося у форматі відеоконференції. Матеріальні сліди можуть міститися у роздрукованих документах, скриншотах переписки, квитанціях тощо, а також

можуть залишатися на комп’ютерній техніці, на магнітних носіях і оптичних дисках.

Особливу увагу приділено предмету шахрайського посягання у сфері е-комерції, з урахуванням умов воєнного стану.

Зазначається, що, в основному фізичні особи виступають потерпілими при здійсненні роздрібної купівлі-продажу товарів або послуг на онлайн-платформах, на інтернет-аукціонах, під час здійснення інтернет-банкінгу тощо. Юридичні особи стають потерпілими внаслідок здійснення господарських операцій між юридичними та фізичними особами; при здійсненні матеріально-технічного постачання з використанням засобів електронної комерції у виробничому циклі підприємства; при наданні логістичних послуг; при здійсненні брендингу та просування торгової марки компанії; при забезпеченні фінансовими установами трансакцій між суб’єктами; при наданні іншим підприємцям власно-створеного онлайн-майданчику для створення магазинів і торгівлі своїм товаром (маркетплейси).

Здійснено опис характеристики осіб, які вчиняють шахрайства у сфері е-комерції. Акцентовано на великому відсотку вчинення шахрайств у сфері інтернет-комерції у складі організованої групи.

Виокремлено й висвітлено кореляційні зв’язки між елементами криміналістичної характеристик шахрайства у сфері е-комерції.

Наголошено на проблемних питаннях, що виникають під час організації та планування розслідування шахрайства у сфері е-комерції. Зазначено, що найсуттєвішою проблемою на початку кримінального провадження є визначення кримінально-правової кваліфікації, адже одні й ті самі дані про протиправне діяння можуть мати різну кримінально-правову кваліфікацію.

Зважаючи на виключний правовий характер цієї проблеми та не однакове застосування судами норм матеріального права під час розгляду справ зазначеної категорії, автор пропонує узагальнити судову практику та сформувати єдину правову позицію.

Розглянуто приводи та підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції, виокремлено джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт вчинення протиправних дій у кіберпросторі. Висвітлено заходи, спрямовані на документування таких шахрайств.

Виокремлено типові слідчі ситуації, що складаються на певному етапі розслідування шахрайства у сфері е-комерції, та визначено відповідні тактичні завдання, які необхідно вирішити у кожній такій ситуації.

Висвітлено особливості взаємодії слідчих з іншими правоохоронними органами, а також установами, підприємствами та організаціями, громадськими формуваннями.

Висвітлено проблемні питання та організаційно-тактичні особливості проведення слідчих (розшукових) та інших найбільш поширених процесуальних дій у провадженнях щодо шахрайства у сфері е-комерції. На основі узагальнення судово-слідчої практики з'ясовано, що найбільш проблемною слідчою (розшуковою) дією у досліджуваній категорії проваджень є обшук. Задля закріплення доказів, отриманих у ході проведення обшуку, важливим є визначення підстав для правомірного втручання в особисте життя особи та порушення недоторканості приватної власності тощо. Висвітлено організаційно-підготовчі заходи, що сприятимуть отриманню успішних результатів обшуку (визначення підстав для проведення обшуку; створення умов для дотримання процесуальних вимог та визнання допустимими доказів, отриманих у ході обшуку; створення сприятливих тактичних умов проведення обшуку; визначення правильної юридичної адреси об'єкта обшуку; визначення чіткого переліку об'єктів пошуку).

З'ясовано, що об'єктами вилучення можуть бути: реєстраційні документи, що посвідчують законність діяльності суб'єкта комерційної діяльності; фотографії, відеозаписи, на яких міститься інформація, що має значення для справи (факт знайомства певних осіб між собою, факт

перебування особи у певному місці тощо); документи, що відображають особливості комерційної діяльності осіб, які мають відношення до шахрайських дій; документи, які містять відомості про можливих покупців; електронні та паперові договори про комерційні угоди; документи, що посвідчують особу (їхні копії, підроблені документи на ім'я інших осіб); сім картки; квитанції про проведення банківських операцій; мобільні телефони, де міститься адресна книга (прізвища й адреси покупців, дані про організатора злочину); записні книжки, рукописні тексти на папері, у журналах; комп'ютерна техніка (ноутбуки, планшети, системні блоки), де може міститися інформація про протиправну діяльність шахрая; електронні носії інформації; документи, що підтверджують відкриття розрахункових рахунків у банківській установі; договори з іншими організаціями, підприємствами та приватними підприємцями, які беруть участь у комерційних операціях; печатки та штампи як справжні, так і підроблені, кліше підписів та ін.

Висвітлюються організаційно-тактичні особливості обшуку, тимчасового доступу до речей та документів.

Приділено увагу огляду електронної інформації, що розміщена у відкритому доступі в мережі Інтернет, а також такої, що знаходиться на фізичних носіях інформації і у хмарних сервісах зберігання електронної інформації. Висвітлюються особливості програмного фотографування зображення з екрану монітору з подальшим його описанням у протоколі огляду, та особливості створення дублікату web-сайту за допомогою спеціальних програм, інші правила оформлення копій web-сторінок як електронних доказів.

Висвітлено організаційно-тактичні особливості проведення допиту та одночасного допиту різної категорії осіб, враховуючи специфіку розслідування шахрайства у сфері е-комерції. Визначено спектр тактичних прийомів, які найчастіше використовуються під час допиту у провадженнях досліджуваної категорії.

Проведено аналіз наукових думок з приводу визначення терміну «спеціальні знання». Акцентовано на дискусійності питань, пов'язаних із класифікацією форм спеціальних знань, серед яких автор виділяє процесуальні та непроцесуальні форми.

Наголошено на ролі спеціаліста при проведенні окремих процесуальних та слідчих (розшукових) дій, зокрема: обшуку, тимчасовому доступу до речей та документів, у ході яких ведеться пошук та вилучається інформація, яка міститься у комп'ютерах, на електронних носіях інформації, у хмарних сховищах тощо, а також у пам'яті мобільних телефонів. Описується роль спеціаліста при необхідності подолання системи логічного захисту інформації та входження до комп'ютерних систем, а також при огляді носіїв комп'ютерної інформації, комп'ютерної техніки та інших вилучених об'єктів.

Не менш важливою є участь спеціаліста під час проведення допиту, особливо, якщо показання надає особа, яка є компетентною у певній галузі економіки, комерційної, банківської діяльності, а також знається на комп'ютерних технологіях.

Висвітлено можливості консультаційно-довідкової допомоги спеціалістів різних галузей знань при розслідуванні шахрайства у сфері е-комерції, наводиться перелік осіб, які можуть надати таку допомогу.

Наголошено на ролі судових експертиз при розслідуванні шахрайств у сфері е-комерції та сформульовано їх перелік. Висвітлюються особливості підготовки та проведення таких експертиз: технічної експертизи документів; почеркознавчої; портретної; судової телекомунікаційної; трасологічної; комп'ютерно-технічної експертизи; експертизи відеозвукозапису та ін.

Визначено теоретичні засади побудови й використання тактичних операцій у розслідуванні кримінальних правопорушень. Наголошено, що тактичні операції є дієвим засобом оптимізації діяльності слідчого, які використовуються для вирішення комплексу тактичних завдань.

Визначено перелік типових тактичних операцій і висвітлено

особливості їх застосування, з урахуванням специфіки розслідування шахрайств у сфері е-комерції. Виокремлено організаційні заходи до їх проведення, а також визначено комплекс дій, що входять до їх змісту.

Висвітлено тактичні заходи, що сприяють виявленню ознак, які свідчать про злочинну діяльність організованого угрупування у сфері е-комерції.

Виокремлено тактичні помилки, яких припускаються слідчі при проведенні тактичних операцій.

Наголошено на суперечності між законодавчим та відомчим рівнями регулювання діяльності слідчих у сфері запобігання кримінальним правопорушенням, що потребує внесення в чинний КПК України положень, які б висвітлювали процедуру здійснення профілактичних заходів. Автор переконаний, що профілактична діяльність слідчого повинна бути необхідною складовою досудового розслідування кримінальних правопорушень, у тому числі й шахрайств у сфері е-комерції.

Виокремлено ряд причин та умов, що сприяють учиненню шахрайств у сфері е-комерції, серед яких: наявність законодавчих колізій щодо здійснення комерційних електронних операцій; неоднозначність судової практики щодо шахрайств, учинених у кіберпросторі; транснаціональний характер шахрайських дій у сфері е-комерції та їх розпливчастість у часі та просторі; хакерські атаки на банки, що зумовлюють труднощі з обслуговуванням клієнтів і здійсненням банківських операцій; хакерські атаки на сайти, через які здійснюються комерційні операції; сприяння вчиненню шахрайств у сфері е-комерції з боку працівників банку, інтернет-провайдерів, операторів мобільного зв’язку.

Запропоновано спеціальні заходи криміналістичної профілактики. Наголошено, що окремої уваги заслуговує використання можливостей інформаційних ресурсів самих правоохоронних органів, насамперед Національної поліції України, в якій створена та тривалий час функціонує система відділів комунікації, які співпрацюють з регіональними та

всеукраїнськими ЗМІ, мають власні сайти, сторінки у соціальних мережах, виробляють власний аудіовізуальний контент, а також проявляють високу активність в інших засобах масової комунікації, в т.ч. в соціальних мережах та електронних засобах масової інформації.

Як окрема складова концепції профілактики вчинення онлайн-шахрайств зазначено діяльність правоохоронців щодо моніторингу соціальних мереж та ЗМІ.

Наголошено, що кібершахрайство є глобальною міжконтинентальною проблемою, а розвиток світової електронної комерції зумовлює збільшення кількості шахрайств у даній сфері також у світовому масштабі. Проаналізовано досвід США та окремих європейських держав (Німеччини, Великої Британії, Франції) з питань протидії та боротьби з шахрайствами у сфері е-комерції.

Підтримується думка провідних світових вчених щодо створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції, яка б поєднувала різноманітні інформаційні ресурси та бази даних про шахраїв у всьому світі.

Наголошено на необхідності постійної міжнародної співпраці у боротьбі з шахрайством у сфері е-комерції, що ґрунтується на національних законодавчих та підзаконних актах, а також міжнародних угодах, обов’язковість яких підтверджено Верховною Радою України.

Висвітлені питання щодо надання міжнародної правової допомоги компетентними органами інших держав з питань виконання окремих процесуальних дій, видачі осіб, які вчинили шахрайства у сфері е-комерції, тимчасової передачі таких осіб, перейняття кримінального переслідування.

Ключові слова: *шахрайство, е-комерція, електронна комерція, електронний бізнес, Інтернет, банківські операції, електронні перекази, методика, криміналістична профілактика, слідчі (розшукові) дії, кіберзлочини.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Коба В.Б.Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право*. 2020. № 2 (68). С. 303–307.

2. Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

3. Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

4. Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

5. Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

6. Коба В.Б. Е-комерція – як об’єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Коба В.Б. Значення тактичних завдань для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

8. Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

9. Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі :матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування :матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

SUMMARY

Koba V. B. Theoretical and praxeological foundations of fraud investigation methods in the field of e-commerce. – *The manuscript.*

The thesis is for candidate's degree of law on specialty 12.00.09 – Criminal Procedure and Criminalistics; Forensic Examination; Operational-Search Activity. – Dnipropetrovskyi State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Dnipro, 2024.

The thesis elaborates the theoretical and praxeological principles of the fraud investigation method in the field of e-commerce at the monographic level. A forensic analysis of the functioning of the e-commerce sphere was carried out and the factors that lead to the commission of fraudulent actions were determined.

An analysis of legal sources on the functioning of the e-commerce sphere was carried out and it was found that the level of commercial transactions in a

remote format is increasing. The significant difference in the interpretation of a number of terms that characterize legal relations in the commercial sphere is emphasized, in particular: «electronic commerce», «electronic business», «electronic trade», etc.

It is emphasized that the popularity of commercial activities in the virtual space has created a basis for fraudsters who operate even at the transnational level.

It was emphasized that the method of committing fraud in the field of e-commerce has a full structural nature and includes actions of preparation, direct commission and concealment of illegal actions.

The typical methods of committing fraud in the field of e-commerce were revealed and systematized, attention was paid to the methods of their concealment, in particular: destruction of information contained on electronic media (79 %), use of disposable mobile phone numbers (81 %), avoiding eye contact with the victim (81%), entering false information into electronic databases (27 %), falsification of evidence (78 %) and others.

An analysis of scientific opinions on the problems of investigating fraud committed with the use of computer technologies was carried out. It was concluded that the most controversial element of forensic characteristics is the situation of committing fraud of this category, because as a result of conducting electronic commercial transactions, a virtual environment arises in which any actions with information are carried out with the help of digital signals and can go beyond the boundaries of one state, which makes it difficult to determine spatio-temporal characteristics.

It is noted that, in a narrow sense, the place where fraud is committed in the field of e-commerce is the location of software and technical means that have been criminally influenced and their access points to certain networks, as well as the location of ATMs, bank branches, zones of free connection to the Internet using Wi-Fi technology.

In a geographical sense, 92 % of all «virtual commercial transactions» are carried out in large cities and megacities. At the same time, the percentage of

entities that offer commercial goods and services is much higher than the percentage of people who need such goods and services, which is explained by the shortage of such facilities in small cities. It was emphasized that the situation must be considered, taking into account the conditions in which the fraudster acted. There are a number of subjective and objective factors that determine the possibility, conditions and other circumstances of committing fraud in the field of e-commerce.

The virtual (electronic, digital) traces characteristic of fraud in the field of e-commerce are singled out. Instead, it is emphasized that material and ideal traces also play an important role in detecting fraud in this category. In most cases, victims can provide information about the fraudster's appearance in the case of a direct meeting before or after the execution of a commercial electronic agreement, or if the communication was carried out in the format of a video conference. Material traces can be contained in printed documents, screenshots of correspondence, receipts, etc., and can also remain on computer equipment, on magnetic media and optical discs.

Special attention is paid to the subject of fraudulent encroachment in the field of e-commerce, taking into account the conditions of martial law.

It is noted that mostly natural persons act as victims during the retail sale of goods or services on online platforms, online auctions, during online banking, etc. Legal entities become victims as a result of economic transactions between legal entities and individuals; when carrying out material and technical supply using electronic commerce tools in the enterprise's production cycle; when providing logistics services; in the implementation of branding and promotion of the company's trademark; when providing transactions between entities by financial institutions; when providing other entrepreneurs with a self-created online site for creating stores and trading their goods (marketplaces), etc.

The description of the characteristics of persons who commit fraud in the field of e-commerce was carried out. Emphasis is placed on a large percentage of fraud in the field of e-commerce as part of an organized group.

The correlations between the elements of the forensic characteristics of fraud in the field of e-commerce are highlighted and highlighted.

Problematic issues arising during the organization and planning of e-commerce fraud investigations are emphasized. It is noted that the most significant problem at the beginning of criminal proceedings is the determination of criminal-legal qualifications, because the same data on an illegal act can have different criminal-legal qualifications.

Considering the exclusive legal nature of this problem and the non-uniform application of the norms of substantive law by the courts when considering cases of the specified category, the author proposes to generalize the judicial practice and form a unified legal position.

Reasons and grounds for opening criminal proceedings regarding fraud in the field of e-commerce are considered, sources are singled out, which make it possible to obtain official information that confirms or refutes information about the fact of committing illegal actions in cyberspace. Measures aimed at documenting such frauds are highlighted.

Typical investigative situations that arise at a certain stage of fraud investigation in the field of e-commerce are highlighted, and corresponding tactical tasks that must be solved in each such situation are identified.

The peculiarities of the interaction of investigators with other law enforcement agencies, as well as institutions, enterprises and organizations, public formations are highlighted.

Problematic issues and organizational and tactical features of conducting investigative (search) and other most common procedural actions in proceedings related to fraud in the field of e-commerce are highlighted. Based on the generalization of judicial and investigative practice, it was found that the most problematic investigative (search) action in the studied category of proceedings is a search. In order to consolidate the evidence obtained during the search, it is important to determine the grounds for legitimate interference in a person's personal life and violation of the integrity of private property.

The organizational and preparatory measures that will contribute to obtaining successful results of the search are highlighted (determining the grounds for conducting the search; creating conditions for compliance with procedural requirements and recognizing evidence obtained during the search as admissible; creating favorable tactical conditions for conducting the search; determining the correct legal address of the object of the search); definition of a clear list of search objects).

It was found that the objects of seizure can be: registration documents certifying the legality of the activity of the subject of commercial activity; photographs, video recordings, which contain information relevant to the case (the fact that certain persons know each other, the fact that a person is in a certain place, etc.); documents reflecting the specifics of the commercial activities of persons involved in fraudulent activities; documents that contain information about possible buyers; electronic and paper contracts on commercial agreements; identity documents (their copies, forged documents in the name of other persons); seven cards; receipts for bank transactions; mobile phones containing the address book (names and addresses of buyers, information about the organizer of the crime); notebooks, handwritten texts on paper, in magazines, etc.; computer equipment (laptops, tablets, system units) that may contain information about the fraudster's illegal activities; electronic media; documents confirming the opening of current accounts in a banking institution; contracts with other organizations, enterprises and private entrepreneurs participating in commercial transactions; seals and stamps both real and fake, signature clichés.

Organizational and tactical features of search, temporary access to things and documents are highlighted.

Attention is paid to the review of electronic information that is publicly available on the Internet, as well as that located on physical media and in cloud services for storing electronic information. Features of software photographing the image from the monitor screen with its subsequent description in the inspection

protocol, and features of creating a duplicate website using special programs, other rules for making copies of web pages as electronic evidence are highlighted.

The organizational and tactical features of interrogation and simultaneous interrogation of different categories of persons are highlighted, taking into account the specifics of the investigation of fraud in the field of e-commerce. The range of tactical techniques that are most often used during interrogation in proceedings of the studied category is determined.

An analysis of scientific opinions on the definition of the term «special knowledge» was carried out. Emphasis is placed on the debatability of issues related to the classification of forms of special knowledge, among which the author singles out procedural and non-procedural forms.

The role of a specialist in carrying out certain procedural and investigative (search) actions is emphasized, in particular: search, temporary access to things and documents, during which a search is conducted and information contained in computers, on electronic data carriers, in cloud storage is searched and extracted etc., as well as in the memory of mobile phones. The role of a specialist is described when it is necessary to overcome the logical information protection system and enter computer systems, as well as when examining computer information carriers, computer equipment and other seized objects.

No less important is the participation of a specialist during the interrogation, especially if the testimony is given by a person who is competent in a certain field of economy, commerce, banking, and also knows computer technologies.

The possibilities of consulting and reference assistance of specialists in various fields of knowledge in the investigation of fraud in the field of e-commerce are highlighted, and a list of persons who can provide such assistance is given.

The role of forensic examinations in the investigation of fraud in the field of e-commerce is emphasized and their list is formulated. Features of preparing and conducting such examinations are highlighted: technical examination of documents; handwriting; portrait; judicial telecommunications; traceological; computer and technical expertise; examinations of video and audio recordings, etc.

The theoretical principles of the construction and use of tactical operations in the investigation of criminal offenses are determined. It is emphasized that tactical operations are an effective means of optimizing the activity of the investigator, which is used to solve a complex of tactical tasks.

The list of typical tactical operations is defined and the features of their application are highlighted, taking into account the specifics of the investigation of fraud in the field of e-commerce. Organizational measures for their implementation have been singled out, as well as a set of actions included in their content has been determined.Tactical measures that contribute to the detection of signs that testify to the criminal activity of an organized group in the field of e-commerce are highlighted.

Tactical mistakes that investigators make when conducting tactical operations are singled out.A set of objective and subjective factors characterizing the level of resistance to the investigation of fraud in the field of e-commerce is singled out, and ways to overcome such manifestations are proposed. On the basis of the analysis of judicial and investigative practice regarding the investigation of fraud in the field of e-commerce, the most effective security measures for participants under pressure were identified, in particular: presentation for identification in the format of a video conference (8 %), presentation for recognition outside of visual observation (21 %), change of questionnaire data (8 %), personal protection and taking under protection (4 %).

Contradictions between the legislative and departmental levels of regulation of the activities of investigators in the field of prevention of criminal offenses are emphasized, which requires the inclusion of provisions in the current Code of Criminal Procedure of Ukraine that would highlight the procedure for implementing preventive measures. The author is convinced that preventive activities of the investigator should be a necessary component of the pretrial investigation of criminal offenses, including fraud in the field of e-commerce.

A number of reasons and conditions contributing to fraud in the field of e-commerce are singled out, including: the presence of legislative conflicts

regarding the implementation of commercial electronic transactions; the ambiguity of judicial practice regarding fraud committed in cyberspace; the transnational nature of fraudulent actions in the field of e-commerce and their vagueness in time and space; hacker attacks on banks causing difficulties with customer service and banking transactions; hacker attacks on sites through which commercial operations are carried out; facilitation of fraud in the field of e-commerce by bank employees, Internet providers, and mobile operators.

Special measures of forensic prevention are proposed. It was emphasized that special attention should be paid to the use of information resources of the law enforcement agencies themselves, first of all, the National Police of Ukraine, in which a system of communication departments was created and has been functioning for a long time, which cooperate with regional and all-Ukrainian mass media, have their own websites, pages in social networks, and produce their own audiovisual content , and are also highly active in other means of mass communication, including in social networks and electronic media.

As a separate component of the concept of prevention of online frauds, the activities of law enforcement officers regarding monitoring of social networks and mass media are indicated.It was emphasized that cyber fraud is a global intercontinental problem, and the development of global e-commerce leads to an increase in the number of frauds in this field, also on a global scale. The experience of the USA and certain European states (Germany, Great Britain, France, etc.) in countering and fighting fraud in the field of e-commerce was analyzed.

Special attention is paid to the problems of early detection and prompt response to cyber incidents and cyber attacks against electronic information resources. The opinion of the world's leading scientists on the creation of a Unified information system for the prevention of fraud in the field of electronic commerce, which would combine various information resources and databases about fraudsters around the world, is supported.

The need for constant international cooperation in the fight against fraud in the field of e-commerce, which is based on national legislative and by-laws, as

well as international agreements, the binding nature of which has been confirmed by the Verkhovna Rada of Ukraine, is emphasized.

Issues related to the provision of international legal assistance by the competent authorities of other states on the execution of certain procedural actions, the extradition of persons who have committed fraud in the field of e-commerce, the temporary transfer of such persons, and the taking over of criminal prosecution are highlighted.

Keywords:*fraud, e-commerce, electronic commerce, electronic business, pre-trial investigation, Internet, banking operations, electronic transfers, methodology, forensic prevention, investigative (search) actions, cybercrimes.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Коба В.Б.Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право*. 2020. № 2 (68). С. 303–307.

2. Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

3. Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

4. Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

5. Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

6. Коба В.Б. Е-комерція – як об’єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management)*. 2022. № 7 (51). С. 223–227 (Республіка Польща).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Коба В.Б. Значення тактичних завдань для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

8. Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

9. Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі :матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування :матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

ЗМІСТ

Перелік умовних скорочень……..…….....23

ВСТУП.……...24

РОЗДІЛ 1

НАУКОВІ ЗАСАДИ ПОБУДОВИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ…….…….35

1.1. Сфера е-комерції як об’єкт криміналістичного дослідження.……...35

1.2. Способи вчинення шахрайства у сфері е-комерції.…….…..46

1.3. Обстановка та слідова картина шахрайства. Предмет злочинного посягання……..……63

1.4. Характеристика особи злочинця та потерпілого……73

Висновки до 1 розділу……..81

РОЗДІЛ 2

ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ……...85

2.1. Криміналістичний аналіз первісної інформації та організація розслідування шахрайства.….....85

2.2. Організаційно-тактичні особливості проведення окремих процесуальних дій...……...99

2.3. Використання спеціальних знань як засіб тактичного забезпечення розслідування шахрайства у сфері е-комерції...…….115

Висновки до розділу 2……128

РОЗДІЛ 3

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ

Е-КОМЕРЦІЇ……1
31
3.1. Тактичні операції як засіб оптимізації розслідування шахрайства у сфері е-комерції…….……..……..131
3.2. Профілактична діяльність уповноважених осіб у провадженнях за фактами шахрайства у сфері е-комерції..……..152
3.3. Міжнародний досвід протидії шахрайствам у сфері е-комерції..……168
Висновки до 3 розділу……181

ВИСНОВКИ.…….……..…….....183

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.…….…….....193

ДОДАТКИ.…….…….....221

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДФСУ		Державна фіскальна служба України
ДКП		Департамент кіберполіції
ЄС		Європейський Союз
Е-комерція		Електронна комерція
Е-банкінг		Електронний банкінг
ЕОМ		Електронні обчислювальні машини
ЄРДР	–	Єдиний реєстр досудових розслідувань
ЗМІ		Засоби масової інформації
ЗСУ		Збройні Сили України
КК	–	Кримінальний кодекс
КПК	–	Кримінальний процесуальний кодекс
КТЕ		Комп’ютерно-технічна експертиза
МВС	–	Міністерство внутрішніх справ
НП		Національна поліція
ОМП		Огляд місця події
ОУ		Організоване угрупування
ОРЗ		Оперативно-розшукові заходи
СОГ	–	Слідчо-оперативна група
СІЗО	–	Слідчий ізолятор
СУ		Слідче управління
СРД	–	Слідчі (розшукові) дії
НСРД	–	Негласні слідчі (розшукові) дії
ЦК		Цивільний Кодекс
УВП		Установа виконання покарань

ВСТУП

Обґрунтування теми дослідження. Сучасна світова діджиталізація суспільства сформувала зростання попиту на цифрові технології та споживання їх у різних секторах державного управління та суспільного життя. Значне місце у цифрових новаціях займає сфера комерційної діяльності, де переважна кількість угод здійснюється в електронному форматі. Торгівельні, фінансові й виробничо-сервісні операції докорінно змінюють свій технологічний прояв, а ведення електронного бізнесу досить стрімко набуває обертів як серед приватних осіб, так і провідних компаній, які задіяні у реалізації глобальних комерційних проєктів. Особливо значний попит на комерційні операції у цифровому форматі виник в умовах запровадження соціальної дистанції (2020-2021 рр.) у межах боротьби з гострою респіраторною хворобою COVID-19. Внаслідок повномасштабного збройного вторгнення рф на територію України (2022-2023 рр.) суттєво було порушено логістику, спостерігався обмежений доступ до здійснення комерційних операцій в офлайн-режимі, що змусило більшість осіб, задіяних у е-бізнесі, перейти на цифровий формат спілкування. Враховуючи швидкоплинність цифрових процесів, неврегульованість низки питань стосовно здійснення е-бізнесу та відсутність достатнього контролю з боку контролюючих органів зумовили збільшення шахрайських дій у сфері е-комерції.

Так, за даними Департаменту інформаційно-аналітичної підтримки Національної поліції у 2018 р. до ЄРДР внесено 1598 фактів шахрайств, учинених з використанням високих інформаційних технологій, у той час як повідомлення про підозру було вручено у 1006 випадках; 2019 р. – 796, повідомлення про підозру – у 513 провадженнях; 2020 р. – 1355, повідомлення про підозру – у 1004 провадженнях; 2021 р. – 1928, повідомлення про підозру – у 1524 провадженнях; 2022 р. – 6591, повідомлення про підозру – у 1253 провадженнях. Лише за І квартал 2023 р.

обліковано 7749 таких шахрайств, повідомлення про підозру вручено лише у 1126 провадженнях. При цьому, питома вага розкритих шахрайств у сфері е-комерції, передбачених ч. 3 ст. 190 КК, з кожним роком знижується. Так, у 2021 р. рівень розкриття шахрайств складав 79 %, а вже з 2022 р. відсоток розкритих фактів істотно почав знижуватися і склав 19 % і лише за 3 місяці 2023 р. досяг критичної позначки – 14,5 %. Кількість шахрайств дедалі збільшується, а кількість шахраїв, притягнутих до відповідальності, залишається на низькому рівні. Окрім того, шахрайські дії у сфері е-комерції мають високий рівень латентності, внаслідок чого більшість фактів залишаються невикритими, особливо в частині протиправного заволодіння коштами громадян з використанням високих інформаційних технологій.

Низька ефективність процесу доказування у кримінальних провадженнях зумовлена такими чинниками: значний проміжок часу між шахрайськими діями та повідомленням про їх учинення; складність документування шахрайських дій; відсутність належної взаємодії між підрозділами Національної поліції, насамперед, працівників кіберполіції й слідчих; несвоєчасна реалізація НСРД та інших процесуальних заходів; низький рівень обізнаності слідчих щодо типових шахрайських схем та шляхів встановлення шахраїв за цифровою слідовою картиною; висока латентність шахрайств; поверхневе проведення СРД і низька ефективність застосовування НТЗ; відсутність належних заходів профілактики; низький рівень міжнародного співробітництва у кримінальному провадженні. Це свідчить про низку проблемних питань у сфері розслідування шахрайства.

Наукове підґрунтя дисертаційного дослідження у галузево-предметному плані становлять праці таких учених, як: В. П. Бахін, А. Ф. Волобуєв, В. Г. Дрозд, В. А. Журавель, А. В. Іщенко, Н. І. Клименко, В. О. Коновалова, В. С. Кузьмічов, Є. Д. Лук’янчиков, І. В. Пиріг, М. В. Салтевський, Р. Л. Степанюк, В. В. Тіщенко, К. О. Чаплинський, С. С. Чернявський, Ю. М. Чорноус, В. Ю. Шепітькота ін.

Проблемні питання кримінально-правової та кримінологічної

характеристик, кримінально-процесуального, криміналістичного та оперативно-розшукового забезпечення розслідування шахрайства висвітлювалися у наукових працях: С. В. Головкіна, І. А. Гукової, О. В. Добровӧ, Г. В. Захаровӧ, І. О. Коваленка, О. В. Курмана, В. Р. Мойсика, О. Л. Мусієнко, Н. В. Павловӧ, В. І. Пазиніч, Д. А. Птушкіна, О. А. Самойленко, Т. Л. Тропінӧ, С. В. Чучка та ін.

Серед сучасних наукових розробок, які мають спеціалізований теоретико-прикладний характер, а також є підґрунтям для формування концепційно-сутнісної моделі розслідування шахрайств у сфері е-комерції варто виокремити дослідження на рівні кандидатських дисертацій. Так, А. В. Рейнгольд у дисертації «Основи методики розслідування шахрайства в інтернет-комерції» (м. Дніпро, 2023 р.) визначив особливості регулювання правовідносин у віртуальному просторі, що впливають на рівень вчинення шахрайства у мережі Інтернет, окресливструктуру криміналістичної характеристики шахрайства, особливості організації розслідування і проведення деяких тактичних операцій. А. Е. Жилін у роботі «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів» (м. Дніпро, 2023 р.) розкрив криміналістичну характеристику шахрайства, охарактеризував окремі її елементи; окреслив тактику СРД та напрями взаємодії слідчих і працівників оперативних підрозділів; запропонував тактичні операції, спрямовані на збирання відомостей стосовно шахрайства та джерел криміналістично вагомої інформації.

Відзначаючи теоретичну значущість наведених праць, потрібно зазначити, що деякі питання так і залишилися недослідженими або потребують додаткового висвітлення через цифровізацію економічного простору, диджиталізацію світового суспільства, новітні зміни у законодавстві, наявність надзвичайних правових режимів, модернізацію способів шахрайства з використанням інтернет-технологій. Не дослідженими залишаються питання використання зарубіжного досвіду і міжнародного

співробітництва, забезпечення відшкодування шкоди, заподіяної кіберзлочином, профілактичної діяльності уповноважених осіб, перспективні напрями взаємодії правоохоронних органів та застосування комплексів тактичних операцій у кримінальному проваджені.

Наведені обставини у своїй сукупності визначили актуальність окресленої проблематики, її теоретичне й практичне значення, а також зумовили вибір напряму дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до положень Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації (розпорядження Кабінету Міністрів України від 17.11.2021 № 1467-р), Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії кібербезпеки України (Указ Президента України від 14.05.2021 № 447/2021), Національної економічної стратегії на період до 2030 року (постанова Кабінету Міністрів України від 03.03.2021 № 179),Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року (розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та Міністерства внутрішніх справ України (спільний наказ Офісу Генерального прокурора та МВС України від 22.11.2021 № 371/846), тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022-2026 роки (наказ МОН України від 03.02.2022 № 109), тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11.06.2020 № 454), Основних напрямів наукових досліджень Науково-дослідного інституту публічного права на 2020–2024 рр.

Мета і задачі дослідження. *Мета* дисертаційного дослідження полягає

у вирішенні конкретного наукового завдання з розробки концептуальних основ методики розслідування шахрайства у сфері е-комерції. Комплексність мети, її багатоплановість обумовили необхідність вирішення окремих *задач:*

– здійснити криміналістичний аналіз функціонування сфери е-комерції та визначити фактори, що зумовлюють учинення шахрайських дій;

– охарактеризувати криміналістично вагомі ознаки структурних елементів криміналістичної характеристики шахрайства у сфері е-комерції;

– визначити основні напрями організації розслідування шахрайства;

– конкретизувати організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій;

– розкрити форми використання спеціальних знань при розслідуванні шахрайства у сфері е-комерції;

– сформувати типові тактичні операції при розслідуванні шахрайства у сфері е-комерції та розробити оптимальний комплекс дій для їх проведення;

– виокремити заходи профілактичної діяльності уповноважених осіб щодо виявлення й усунення причин та умов учинення шахрайства у сфері е-комерції;

– узагальнити міжнародний досвід протидії шахрайствам у сфері е-комерції.

Об'єктом дослідження є кримінальні процесуальні відносини, що виникають у діяльності правоохоронних органів під час розслідування шахрайства у сфері е-комерції.

Предмет дослідження – *теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції.*

Методи дослідження. Відповідно до поставленої мети, через призму об'єкта і предмета дослідження застосовано низку загальнонаукових і спеціальних методів наукового пізнання. *Порівняльно-правовий метод* – для аналізу кримінальних і кримінально-процесуальних норм та нормативно-правових актів, що регулюють питання функціонування е-комерції (підрозділ 1.1, розділи 2–3). *Формально-логічний метод* – для

аналізу матеріалів кримінальних проваджень, наукових концепцій, що відтворюють особливості дослідження шахрайства (розділи 1–3). *Системно-структурний метод* – для з'ясування структури криміналістичної характеристики шахрайства, класифікації типових способів його вчинення, систематизації тактичних операцій, виокремлення віктимогенних груп потерпілих (розділ 1). *Функціональний метод* – для визначення перспективних напрямів застосування тактичних операцій (підрозділ 3.1), проведення СРД і НСРД (підрозділ 2.2), оптимізації організації розслідування шахрайства(підрозділ 2.1). *Системний метод* – для формування заходів профілактичної діяльності (підрозділ 3.2)**.** *Типологічний метод* **–** для формування «портрету» ймовірного злочинця і виділення віктимогенних груп потерпілих(підрозділ 1.4). *Статистичний метод* – для аналізу судово-слідчої практики, узагальнення статистичних даних, матеріалів кримінальних проваджень і опитування респондентів (розділи 1–3). *Соціологічний метод* – для проведення анкетування працівників органів прокуратури, слідчих, оперативних та експертних підрозділів МВС України (розділи 1–3). На основі *синтезу* сформульовано загальні висновки за темою дослідження (розділи 1–3).

Емпіричну основу дослідження становлять згруповані відомості ДІАП Національної поліції за 2018-2023 рр., Єдиного звіту про вчинені кримінальні правопорушення Офісу Генерального прокурора України за період 2017-2023 рр., а також результати опрацювання слідчої і судової практики протягом 2015-2023 рр. Зокрема, досліджено матеріали 157 кримінальних проваджень за фактами шахрайств у сфері е-комерції (Вінницька, Волинська, Дніпропетровська, Донецька, Запорізька, Київська, Львівська, Миколаївська, Одеська, Полтавська, Сумська, Харківська, Черкаська та Чернівецька області, м. Київ) за 2016-2023 рр.; зведені результати анкетування 245 слідчих, 138 працівників органів прокуратури, 56 працівників кіберполіції, 198 працівників оперативних підрозділів, 76 працівників експертних установ МВС України. Під час дослідження використано власний досвід роботи у

підрозділах Національної поліції України.

Наукова новизна одержаних результатів полягає в тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням криміналістичної характеристики та організаційно-тактичних аспектів розслідування шахрайства у сфері е-комерції, в якому сформульовано низку наукових положень, висновків і практичних рекомендацій, що мають важливе теоретико-прикладне значення, зокрема:

вперше:

– здійснено криміналістичний аналіз функціонування сфери е-комерції, на підставі якого надано оцінку основним криміногенним факторам, що впливають на рівень та динаміку шахрайських посягань у цій сфері, у тому числі з боку ОГ;

– охарактеризовано міжнародний досвід протидії шахрайствам у сфері е-комерції та запропоновано напрями взаємодії правоохоронних органів з уповноваженими компетентними органами іноземних держав в межах міжнародного співробітництва, з дотриманням положень ратифікованих Україною міжнародно-правових актів і міждержавних угод або на засадах взаємності з питань надання правової допомоги у кримінальних провадженнях;

– здійснено системний аналіз (моніторинг інформації) щодо телефонних номерів, банківських рахунків і карток, які використовувалися злочинцями під час шахрайських дій, з метою встановлення фактів збігів таких номерів при вчиненні значної кількості шахрайств, за якими відкрито кримінальні провадження у різних регіонах країни;

– запропоновано структуру окремої методики, зокрема, до стандартної структури методики розслідування шахрайства у сфері е-комерції, яка складається з криміналістичної характеристики, організаційно-тактичних особливостей розслідування та використання спеціальних знань, додано окремі складові елементи: а) реалізація тактичних операцій; б) профілактична

діяльність уповноважених осіб з виявлення причин й умов, що сприяли шахрайству; в) взаємодія окремих підрозділів правоохоронних органів; г) міжнародне співробітництво у кримінальному провадженні;

– сформовано перелік тактичних завдань, що стоять перед правоохоронними органами під час розслідування шахрайства, та розроблено комплекс дій для їх вирішення в рамках проведення низки тактичних операцій;

– обґрунтовано необхідність запровадження функціонування єдиної автоматизованої системи, яка, у разі виникнення підозрілих дій, автоматично направляє запит до банківських установ, де встановлюється факт транзакції та відстежується подальший рух коштів до кінцевого рахунку/банківської картки, на яку були перераховані кошти, з одночасним блокуванням рахунків;

удосконалено:

– систему ознак механізму утворення слідів шахрайства через дослідження матеріальної й ідеальної їх складової, зокрема, обґрунтовано значення комп'ютерних (віртуальних) слідів з урахуванням сучасних інформаційних технологій та глобальної мережі Інтернет;

– перелік джерел інформації, які дозволяють підтвердити або спростувати факт учинення шахрайських дій у кіберпросторі;

– наукові підходи щодо систематизації типових способів учинення шахрайства та виокремлено такі, що найчастіше використовують члени організованих груп у процесі злочинної діяльності**;**

– теоретичні знання щодо предмету шахрайства у сфері е-комерції – інформація комерційного призначення, гроші (готівкова і безготівкова форма), товари, цінності, право на майно, цінні папери (корпоративні акції, облігації, векселі, у тому числі електронні);

– організаційно-тактичні особливості взаємодії слідчого з працівниками правоохоронних органів (кіберполіції, оперативно-технічних служб); комерційними представництвами, які здійснюють торгівельно-комерційні операції через електронні системи та комп'ютерні мережі; суб'єктами, які

забезпечують передачу і зберігання інформації з використанням інформаційно-комунікаційних систем; банківськими установами з питань проведення комерційних операцій за рахунками конкретної юридичної або фізичної особи;

– алгоритм щодо проведення СРД, які плануються для передачі за підслідністю до інших регіонів держави, зокрема, у фабулах обов'язково вказувати інформацію про обставини і спосіб шахрайства із зазначенням номеру телефону і банківської картки або рахунку, на який здійснювався переказ коштів;

– використання основних форм міжнародного співробітництва, що застосовуються у діяльності з розслідування шахрайства у сфері е-комерції;

дістали подальшого розвитку:

– теоретичні домінанти стосовно напрямів наукових досліджень з проблем протидії шахрайствам, враховуючи умови запровадженого воєнного стану**;**

– теоретичні положення щодо основних кримінально-процесуальних і криміналістичних категорій (профілактична діяльність, криміналістична характеристика, міжнародне співробітництво, тактичні операції, типові слідчі ситуації, спеціальні знання, СРД, НСРД, обставини, що підлягають доказуванню);

– система даних щодо обстановки вчинення шахрайства у сфері е-комерції з урахуванням просторово-часових, соціально-економічних, нормативно-правових та соціально-психологічних факторів;

– характеристика слідової картини шахрайства з формулюванням криміналістичного значення віртуальних (електронних, комп'ютерних) слідів;

– уявлення про структуру організованої групи, що вчиняє шахрайства у сфері електронної комерційної діяльності, та особливості її функціонування;

– організаційно-тактичні особливості проведення окремих процесуальних дій, спрямованих на вилучення інформації з матеріальних джерел (обшук, огляд комп'ютерної техніки та електронних документів,

тимчасовий доступ до речей і документів), ідеальних джерел (допит, одночасний допит) та НСРД;

– система тактичних помилок щодо кримінально-правової кваліфікації, допущених на початковому етапі розслідування шахрайства у сфері е-комерції;

– практичні рекомендації стосовно врегулювання профілактичної діяльності уповноважених осіб щодо обов'язку виявляти причини і умови вчинення шахрайства, що полягають у внесенні змін і доповнень до КПК України.

Практичне значення одержаних результатів полягає в тому, що викладені й аргументовані в дисертації теоретичні положення, висновки та практичні рекомендації впроваджені та використовуються у:

– *законотворчій діяльності* – для удосконалення законодавства у сфері запобігання шахрайствам сформульовано низку пропозицій щодо внесення змін і доповнень до чинного Кримінального процесуального кодексу України;

– *науковій діяльності* – для удосконалення методики розслідування окремих видів кримінальних правопорушень проти власності (акти впровадження Харківського національного університету внутрішніх справ від 17.03.2023 р., Національної академії внутрішніх справ від 14.04.2023 р., Дніпропетровського державного університету внутрішніх справ від 12.05.2023 р.);

– *освітньому процесі* – при викладанні навчальних дисциплін «Організація розслідування кримінальних правопорушень», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність», а також підготовці підручників і навчальних посібників (акти впровадження Дніпропетровського державного університету внутрішніх справ від 27.04.2023 р., ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 10.05.2023 р.);

– *правозастосовній діяльності* – для вдосконалення діяльності органів досудового розслідування, оперативних та експертних підрозділів

Національної поліції (акти впровадження Дніпропетровського НДЕКЦ МВС від 30.03.2023 р.).

Апробація результатів дисертації. Основні теоретичні положення й висновки дисертації оприлюднено на міжнародних науково-практичних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 2020 р.), «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 2021 р.), «Перспективні напрямки розвитку юридичної науки у 21-му сторіччі» (м. Київ, 2022 р.), «Актуальні проблеми взаємодії правової науки та практики її застосування» (м. Київ, 2022 р.).

Публікації. Основні положення та результати дисертації відображено у десяти наукових публікаціях, з яких п’ять статей – у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, одна – у закордонному юридичному виданні, чотири – у збірниках тез наукових доповідей, оприлюднених на міжнародних науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, трьох розділів, що містять десять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 262 сторінки, з яких 192 сторінки основного тексту. Список використаних джерел налічує 243 найменувань і займає 28 сторінок, 8 додатки викладено на 42 сторінках.

РОЗДІЛ 1
НАУКОВІ ЗАСАДИ ПОБУДОВИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ

1.1. Сфера е-комерції як об’єкт криміналістичного дослідження

Епоха динамічного розвитку інформаційно-комунікаційних технологій, однією з яких є Інтернет, призвела до виникнення віртуального простору – особливого електронного середовища взаємодії, в якому будь-які дії з інформацією вчиняються за допомогою цифрових сигналів. Такі значні перетворення спричинили суттєві зміни майже в усіх сферах, пов’язаних із інформаційним обміном, не залишивши осторонь і систему організації та здійснення комерційної діяльності [44; 75].

Натомість, порівняно з традиційною господарською діяльністю робота з використанням інформаційно-комунікаційних технологій має певну специфіку, тому для її виокремлення був запроваджений термін «електронна комерція» (англ. «e-commerce»), а також «електронна торгівля» [44]. Проте, аналіз наукових думок показав істотну розбіжність як раз у трактуванні вказаних термінів та їх змістовній складовій.

Досить абстрактно формують бачення е-комерції К. М. Краус, Н. М. Краус та О. В. Манжура, під якою розуміють будь-які форми ділових операцій, де сторони взаємодіють через електронні технології, а не в процесі фізичного обміну чи контакту [90, с. 20]. У свою чергу, В. Ю. Юдин вважає, що взагалі будь-яка ділова активність, яка використовує можливості глобальної інформаційної мережі для модифікації внутрішніх і зовнішніх зв’язків фірми з метою створення прибутку, охоплюється поняттям «електронна комерція» [232, с. 213].

Поширеним є також розуміння електронної комерції як укладення шляхом обміну електронними документами наступних угод: купівля-продаж, поставка, угода про розподіл продукції, агентські відносини, факторинг,

лізинг, проектування, консалтинг, інженерія, інвестиційні контракти, страхування, угоди про експлуатацію та концесії, банківські послуги, спільна діяльність та інші форми ділового співробітництва, транспортні послуги тощо [103]. Деякі вчені звужують електронну комерцію лише до торгівельних відносин через мережу Інтернет за допомогою комп'ютерів покупця та продавця. Інші пропонують розглядати електронну комерцію як торгову діяльність, яка має за основну мету отримання прибутку та ґрунтується на комплексній автоматизації комерційного циклу за рахунок використання засобів обчислювальної техніки [115]. Водночас, на переконання О. Л. Андронік та А. В. Вороніна, використання терміну «електронна торгівля» повністю відповідає поняттю «електронна комерція», враховуючи тільки покупку чи продаж товарів або послуг у мережі Інтернет, замінюючи і доповнюючи традиційні способи взаємодії покупців і продавців, переносячи їх в електронний простір [3, с. 120].

Натомість, є й нормативне визначення терміну «електронна комерція», під яким у Законі України «Про електронну комерцію» від 03.09.2015 № 675-VIII розуміються відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-комунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру» [151]. Разом з тим, окреме визначення у вказаному Законі надається й «електронній торгівлі», якою вважається господарська діяльність у сфері електронної купівлі-продажу, реалізації товарів дистанційним способом покупцю шляхом здійснення електронних правочинів із використанням інформаційно-телекомунікаційних систем [151].

З цього виходить, що законодавець розділяє поняття «електронна комерція» та «електронна торгівля» та покладає різну змістовну складову у їх наповнення.

Досліджуючи цю проблематику, О. В. Мельник пояснює розбіжність у визначеннях тим, що електронна комерція розглядається у декількох сенсах. В більш вузькому розумінні електронна комерція (e-coomerce) – це торгівля через Інтернет. В широкому розумінні це ведення бізнесу в глобальних мережах. Це сфера цифрової економіки, що включає всі фінансові та торгові трансакції, що проводяться за допомогою комп'ютерних мереж, та бізнес-процеси, пов'язані з проведенням цих трансакцій [114].

Разом з тим, е-комерція є найважливішою складовою е-бізнесу, і охоплює не тільки операції купівлі-продажу, як електронна торгівля, а й супровід процесів створення попиту на продукцію і послуги, автоматизацію адміністративних функцій, пов'язаних з онлайновими продажами і обробленням замовлень, а також із вдосконаленням обміну інформацією між партнерами [65, с. 6].

Зокрема, електронна комерція включає в себе такі функції та процеси: електронний обмін інформацією (ElectronicDataInterchange, EDI); електронний рух капіталу (ElectronicFundsTransfer, EFS); електронна торгівля (e-trade); електронні гроші (e-cash); електронний маркетинг (e-marketing); електронний банкінг (e-banking); електронне страхування грошей (e-insurance) [110].

Кожна з наведених функції має свої особливості. Під електронним обміном інформацією зазвичай розуміють процес будь-якої передачі даних шляхом електронної комунікації. Електронний рух капіталу розуміється, як спосіб електронних транзакції з одного банківського рахунку на інший. Електронна торгівля – це процес купівлі-продажу товару або послуг у мережі Інтернет. Електронні гроші – це безготівкові розрахунки між продавцями та покупцями, банками та клієнтами, які здійснюються за допомогою комп'ютерної мережі. Електронний маркетинг – це звичайне використання маркетингових стратегій прямого впливу, але в інтернет-мережі. Його перевагами вважаються доступність інформації щодо асортименту, зменшення витрат на проведення рекламної кампанії та легкість моніторингу

за отриманою інформацією щодо споживачів. Електронний банкінг – це операції певних банківських послуг, які проводяться через мережу Інтернет. Він дає можливість клієнтам банку мати доступ до їх рахунків, а також проводити певні фінансові операції. Електронне страхування грошей – це страхові послуги, які можна отримати через Інтернет [110].

При цьому, Я. С. Тертичний вважає, що не є доцільним звужувати природу «е-комерції» лише до здійснення трансакцій у торгівельній, фінансовій або рекламній сферах бізнесу із застосуванням інформаційно-комунікаційних технологій. Процес прискореної дифузії цифрових технологій швидко розширює можливості застосування ІКТ у будь-якій сфері торговельно-підприємницької діяльності, спрямованої на отримання прибутків. Таким чином, під електронною комерцією він пропонує розуміти будь-який вид торгівельно-підприємницької, торговельної, комерційно-посередницької діяльності, участі у торгівлі, продажу товарів, нерухомості, цінних паперів, наданні послуг з метою одержання прибутків, який здійснюється дистанційним способом із використанням інформаційно-телекомунікаційних систем [192, с. 279].

В контексті даної проблематики слід зауважити, що поряд з терміном «е-комерція» використовується ще й термін «інтернет-комерція».

При цьому, ряд вчених вважають, що термін «інтернет-комерція» є цілком синонімічним терміну «електронна комерція» [228; 160]. Натомість, слід погодитися із М. Ю. Карпенко, який пояснює, що поняття «е-комерція» трохи ширша, ніж «інтернет-комерція», оскільки до нього входять усі види комерційної діяльності, здійснюваної електронним шляхом. Інтернет-комерція – це комерція, обмежена використанням тільки комп’ютерної мережі Інтернет. До інтернет-комерції не входять: здійснення банківського обслуговування через системи «Клієнт-Банк», комерційна діяльність з використанням мереж VAN, мобільна комерція, системи управління ресурсами підприємства (MPR, ERP, CSRP). Е-комерція використовує ресурси Інтернету і може включати: 1) інтерактивний

маркетинг; 2) замовлення й оплату товарів через WorldWideWeb; 3) екстранет-доступ покупців і постачальників до баз даних товарів; 4) інтранет-доступ дистриб'юторів, продавців і служби підтримки − покупців до баз даних покупців; 5) залучення до процесу розробки продукту споживачів і бізнес-партнерів − за допомогою електронної пошти та дискусійних груп [65, с. 7].

Як наголошують Т. М. Тардаскіна, Є. М. Стрельчук та Ю. В. Терешко, предметом е-комерції може бути будь-яка форма проведення комерційних операцій в електронній формі, наприклад, торгівля, дистриб'юторські угоди, комерційне представництво й агентські відносини, факторинг, лізинг, будівництво промислових об'єктів, надання консультативних послуг, інжиніринг, купівля/продаж ліцензій, інвестування, фінансування, банківські послуги, страхування й інші форми промислової або підприємницької співпраці. Всі процеси, які складають зміст електронної угоди, наприклад, дослідження ринку, пошук комерційного партнера, платіжні операції, страхування ризиків і тому подібне також є предметом е-комерції [191, с. 27; 143].

Отже, в юридичній літературі єдине розуміння е-комерції відсутнє, і цілком зрозуміло, що цим поняттям охоплюється досить широке коло відносин.

Натомість, підтримуємо думку Ю. В. Білоусова та О. Ю. Черняк, які вважають, що для даних правовідносин доцільним є використання саме терміна «електронна комерція», а не «електронна торгівля», оскільки, обмежуючи таку діяльність виключно торгівлею, ми спонукатимемо до обмеження ринку робіт та послуг у цій сфері, що не відповідатиме вимогам норм європейського законодавства в цій сфері, зокрема, Директиві 2000/31/ЄС Європейського парламенту та Ради від 8 червня 2000 року про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку («Директива про електронну комерцію») [14, с. 190].

Тому, у своєму дослідженні пропонуємо використовувати термін «електронна комерція» (у скороченому вигляді – е-комерція).

В контексті даної проблематики слід сказати, що популярність комерційної діяльності у віртуальному просторі створила підґрунтя для шахраїв, які діють навіть на транснаціональному рівні.

Останнім часом, рівень кібершахрайства швидко зростає й в Україні. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Бразилією, Китаєм та меншою мірою – Індією. У цих країнах досить освічене молоде населення, високий рівень безробіття та обмежені можливості працевлаштування [240, с. 133].

Шахрайство у сфері е-комерції – один із видів корисливої злочинності, системоутворюючою ознакою якого виступає спільна корислива мотивація до незаконного збагачення та спрямованість злочинної поведінки на заволодіння матеріальними благами у різний спосіб або отримання іншої незаконної вигоди, характеризується значною поширеністю, багатомільйонними збитками, організованим характером, а також складністю його виявлення та запобігання [26, с. 17].

Кримінальні афери під маскою е-комерції розквітнули в Україні ще й тому, що законодавство не зобов'язує продавців в Інтернеті вказувати реальні реквізити компанії: назву юридичної особи, виписку з Єдиного державного реєстру підприємств та організацій, юридичну та фактичну адреси бізнес-структури. Це уможливлює безкарне розміщення фіктивних даних. Їх правдивість не перевіряють ні Держпродспожив. служба, ні інші профільні державні органи [231].

Вітчизняне законодавство недосконале, а ефективний контрольний орган щодо захисту споживачів у сфері е-комерції відсутній – як і окремий розділ щодо електронної комерції в законі «Про захист прав споживачів». Законодавство про електронну комерцію не містить дієвих інструментів захисту онлайн-покупців. Натомість у Євросоюзі захист прав споживачів у сфері е-торгівлі регулюється директивою 2000/31/ЄС «Про електронну

комерцію» та директивою 97/7/ЄС «Про захист прав споживачів у дистанційних контрактах». У нас досі нема, як у країнах ЄС, розгалуженої громадянської системи захисту споживачів і реєстру доброчесних продавців. Україна обрала європейську систему захисту споживачів е-комерції, у якій інструменти ефективно діють на рівні «третього сектору». Такі центри незалежні від держави, проте наділені правовими повноваженнями і доступні громадянам ЄС навіть у селах [231].

Крім того, шахрайства відносяться до кримінальних правопорушень, що найбільш чутливо реагують на будь-які зміни в суспільстві, а особливо на послаблення правоохоронних функцій в державі. Офіційні статистичні дані свідчать про реєстрацію досить невеликої частки досліджуваної категорії кримінальних правопорушень (приблизно 4-5% від загальної кількості), але це не відображає дійсної картини їх учинення. Шахрайство характеризується найбільшим рівнем латентності серед інших злочинів. Це обумовлено двома основними чинниками. По-перше, потерпілі не звертаються із заявами про вчинення злочину, не здогадуючись, що стали жертвою обману. По-друге, значна частина потерпілих намагаються відновити втрачені майнові права через вирішення спорів у судах, адже шахрайство маскується під оболонкою цивільних, адміністративних чи господарських правовідносин [56, с. 233].

З цього приводу ряд авторів зазначають, що проблема полягає у складності доведення факту вчинення обману в мережі Інтернет. Для того, щоб правильно зібрати докази та розібратися в ситуації, необхідно знати порядок здійснення правочинів в мережі Інтернет, види та порядок розрахунків тощо [46].

Від правильності кваліфікації онлайн-шахрайств на етапі внесення відомостей до ЄРДР залежить не тільки форма проведення досудового розслідування (дізнання або досудове слідство), можливість проведення НСРД чи відсутність законних підстав для їх проведення, але й проведення досудового розслідування уповноваженою особою та подальша оцінка, здобутих під час досудового розслідування доказів, як допустимих.

Окрім того, для здійснення криміналістичного аналізу сфери е-комерції слід знати коло суб'єктів, які задіяні у цьому секторі економіки, характер їх взаємодії та функціональне призначення, правовий статус кожного тощо.

У цьому розрізі фахівці у галузі комерційної діяльності наголошують, що, залежно від учасників взаємин, електронна комерція поділяється на сектори, зокрема:B2B – сектор взаємодії між юридичними особами і організаціями;B2C – сектор взаємодії між юридичними і фізичними особами;C2C – сектор взаємодії між фізичними особами;G2C – сектор взаємодії між державними організаціями і фізичними особами [191, с. 44].

Втім, сектор B2B ще називають «бізнес – бізнесу». Як зазначають Т. М. Тардаскіна, Є. М. Стрельчук, Ю. В. Терешко, цей сектор е-комерції охоплює переважну більшість комерційних операцій: 1) торгово-закупівельні майданчики; 2) електронні вітрини і каталоги; 3) електронні торгові ряди; 4) електронні магазини; 5) електронні біржі; 6) електронні аукціони; 7) галузеві торгові майданчики; 8) системи повного циклу супроводу постачальників (SCM); 9) системи управління розподілом; 10) системи повного циклу супроводу клієнтів (CRM); 11) аутсорсинг; 12) електронні платіжні системи; 13) віртуальні підприємства; 14) системи інтернет-трейдінгу; 15) інтернет-інкубатори; 16) інтернет-реклама; 17) системи мобільної комерції; 18) системи страхування і перестрахування. Разом з тим, B2C, тобто «бізнес – споживачам» охоплює: 1) торгові ряди; 2) електронні вітрини і каталоги; 3) електронні магазини; 4) електронні аукціони; 5) інтернет-трейдінг; 6) електронні платіжні системи; 7) інтернет-страхування; 8) системи телероботи; 8) інтернет-реклама; 9) спонсорські програми; 10) інтерактивне телебачення; 11) електронні ЗМІ; 12) туристичні послуги. Охоплює питання взаємодії фізичних осіб між собою сектор C2C, який ще в економіці називають «споживачі – споживачам», до якого входять: 1) дошки оголошень; 2) інтернет-аукціони тощо. G2C – «влада – споживачам» охоплює: 1) системи соціального обслуговування (виплати,

допомоги, пільги і т.п.); 2) системи комунального обслуговування; 3) юридичні та інформаційно-довідкові служби тощо [191, с. 45-46].

Кожного року рівень застосування електронної комерції в Україні поступово збільшується, і разом з тим збільшується кількість суб'єктів господарювання, які вже знаходяться в цій площині, проте недостатній регулятивний вплив з боку державних органів та швидкий розвиток інформаційних технологій створюють передумови відкритого і незахищеного простору у вчиненні кримінальних правопорушень, а, отже, й розбудові економіці [109].

Згідно з роз'ясненням Міністерства економічного розвитку і торгівлі України у листі № 3502-05/43517-14 від 19.11.2012 р. суб'єкти господарювання, які здійснюють комерційно-торгівельну діяльність за допомогою мережі Інтернет, повинні керуватися вимогами Правил продажу товарів на замовлення та поза торговельними або офісними приміщеннями [150]. Між тим, не дивлячись на існування цих Правил, законодавчо вимоги щодо порядку створення таких магазинів не достатньо визначені, що не заважає шахраям створювати інтернет-магазини, а потім їх ліквідовувати. Це створює підґрунтя для існування магазинів у мережі Інтернет, що діють за принципом фірм-одноденок [214].

Нормативно-правовим актом, що визначає організаційно-правові засади діяльності у сфері електронної комерції в Україні, встановлює порядок вчинення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем, визначає права і обов'язки учасників відносин у сфері електронної комерції, є Закон України «Про електронну комерцію» № 675-VIII від 03.09.2015. Натомість, В. Ю. Юдін справедливо звертає увагу на те, що, незважаючи на високу оцінку зазначеного нормативного акту серед представників електронного бізнесу, він не зміг охопити усі аспекти електронної комерції, які потребували регламентації до його прийняття, і має недосконалості, що заважають розвитку та успішному функціонуванню електронної комерції в Україні.

Зокрема, у Законі не прописано процедури підписання договорів, укладених в електронній формі. Відсутність належного нормативного регулювання порядку використання електронного підпису чи електронного цифрового підпису несе ризики для сторін угод, укладених в режимі реального часу. Наприклад, однією із таких угод може бути купівля-продаж, але відсутня паперова форма договору, підтвердження факту купівлі-продажу, здебільшого відсутня інформації про юридичну особу, яка надає послуги (чи про її статус), оскільки продавець і покупець спілкуються в електронній формі з використанням програмних засобів і мережі Інтернет без відповідної автентифікації та ідентифікації [232, с. 213]. Такої ж думки й О. С. Маковоз та Т. С. Передерій, адже забезпечення економічної безпеки у сфері електронної комерції – серйозна і непроста проблема, оскільки ця сфера молода, багато організаційно-правових відносин ще тільки формуються і закріплюються, комп'ютерні злочини набагато складніше виявити і розкрити, що пояснюється високою кваліфікацією самих злочинців, трудністю збору доказів і, отже, доведення винуватості підозрюваного, можливістю скоєння злочину фактично з будь-якої точки планети з використанням систем віддаленого доступу, Інтернету і т. ін. [109].

Процес криміналізації сфери використання комп'ютерів, систем та комп'ютерних мереж носить системний характер, а процес інформатизації суспільства розвивається дуже стрімко, що в свою чергу створює цілий ряд проблем. Серед них: забезпечення безпеки громадян, збереження конфіденційності персональних даних, захист комерційної та інших видів таємниць, втрата важливої інформації через технічні збої, протиправні посягання на електронні бази та інформаційні ресурси. Останні посідають одне з найважливіших місць у забезпеченні безпеки суспільства та країни [102, с. 305].

Проблемою є й те, що сферу е-комерції обрали сферою здійснення злочинної діяльності й організовані злочинні угруповання. Про це свідчить й аналіз судово-слідчої практики. Так, у 62 % випадків шахрайства у сфері

е-комерції вчиняються групою осіб за попередньою змовою, у 23 % випадків – організованою групою, у 3 % – злочинною організацією. З цього виходить, що лише 12 % таких фактів вчиняється одноосібно.

Наведемо приклад. Так, в ході досудового розслідування встановлено, що учасниками організованої групи були зареєстровані або перереєстровані на підставних осіб ряд підприємств, які використовують групу транзитно-конвертаційних підприємств, з метою прикриття незаконної діяльності, шляхом використання їх реквізитів та банківських рахунків у злочинних схемах зі створення штучної документальної видимості здійснення комерційних операцій для незаконного завищення валових витрат з податку на прибуток підприємств та податкового кредиту з податку на додану вартість підприємствам реального сектору економіки. Також на банківські рахунки вказаних суб`єктів господарської діяльності з ознаками «фіктивності» перераховувалися грошові кошти реально діючих підприємств за нібито надані послуги, виконані роботи чи поставлені товари з метою переведення грошових коштів у готівкову форму та повернення їх клієнтам за вирахуванням певних відсотків [184].

Практичні здобутки та надбання цифрової економіки активно використовуються транснаціональними організованими злочинними угрупованнями з метою отримання надприбутків шляхом вчинення злочинів економічної спрямованості на території однієї або декількох держав з використанням кіберпростору та його можливостей. Викладене зумовлює розкриття нагальних проблем протидії організованій злочинності у сфері цифрової економіки. Загалом, кримінальні мережі і групи хакерів постійно прагнуть використовувати новітні технічні розробки, такі як криптовалюта й анонімні (безконтактні) способи оплати. Швидка обробка транзакцій і поширення ефективних інструментів анонімізації ускладнюють діяльність правоохоронних органів щодо доказової ідентифікації реальних бенефіціарів доходів, одержаних злочинним шляхом. Зростаюча кількість онлайн платформ і додатків пропонують нові способи переказу грошей. Вони не

регулюються тією ж мірою, що й традиційні постачальники фінансових послуг, що робить їх привабливими для злочинців. Крім того, за даними Європолу, існує ймовірність, що деякі поширені платіжні системи на основі блокчейна через компанії-«метелики» можуть контролюватися міжнародним криміналом. Онлайн-банкінг також полегшує життя злочинцям. За даними Європолу, на «чорному» ринку активно продаються спеціальні програми, що дозволяють навіть обійти біометричну ідентифікацію власників рахунків фізичних та юридичних осіб [28, с. 299].

З цього виходить, що проблема шахрайства, у тому числі у сфері е-комерції, має комплексний характер, що зумовлюється багатьма факторами як організаційного, так і правового характеру. Саме тому значна частина юридичних наук і дисциплін покликані своїми науковими розробками та рекомендаціями сприяти ефективному розв'язанню проблеми боротьби зі злочинністю шляхом своєчасного та якісного запобігання, виявлення, розкриття та розслідування злочинів [40, с. 234].

Таким чином, сфера е-комерції характеризується, з одного боку, складними процедурами здійснення правочинів у різних секторах комерційної діяльності, з іншого – широким спектром можливостей вчинювати обманні дії у віртуальному просторі недобросовісними суб'єктами.

1.2. Способи вчинення шахрайства у сфері е-комерції

Побудова окремої криміналістичної методики є можливою завдяки виокремленню типових ознак кримінального правопорушення шляхом формування відповідної криміналістичної характеристики. Разом з тим, серед елементів криміналістичної характеристики домінуюче місце посідає спосіб вчинення кримінального правопорушення, що орієнтує слідчого на встановлення комплексу ознак, які вказують на професійні навички злочинця

та його зв'язок із потерпілим, механізм вчинення протиправних дій в цілому та ряд факторів, які мають значення для встановлення об’єктивної істини.

Шахрайство є найбільш різноманітним з усіх злочинів проти власності, має безліч проявів і вчинюється майже у будь-якій сфері людського життя. Шахраї вдаються до численних вивертів і хитрощів, застосовують новітні засоби і технології, майстерно користуються прогалинами в законодавстві. При цьому вони намагаються досягнути двох взаємопов’язаних цілей: 1) створити зовні легальну оболонку заволодіння чужим майном; 2) уникнути притягнення до кримінальної відповідальності [55, с. 208].

Для досягнення цієї мети шахраї ретельно готуються до вчинення шахрайських дій, у тому числі й заздалегідь продумують дії із приховування. Тобто, шахрайство у сфері у-комерції належить до кримінального правопорушення, спосіб якого є повноструктурним, тобто складається із трьох елементів: підготовки, безпосереднього вчинення та приховування.

Як показав аналіз судово-слідчої практики, в основному підготовчі дії у провадженнях даної категорії включають:

- обрання напряму комерційної діяльності, де планується вчинити шахрайські дії;

- знаходження співучасників та обрання схем шахрайських дій;

- визначення часу, місця та способу вчинення шахрайства;

- підготовка необхідного пакету документів із метою реєстрації суб’єкта комерційної діяльності або підробка документів шляхом внесення до них недостовірних даних;

- створення фіктивних віртуальних клубів, фірм із надання різноманітних послуг, інтернет-магазинів тощо;

- створення фіктивних сайтів, аккаунтів;

- відкриття банківського рахунку і внесення на нього грошових коштів;

- створення «фіктивної» електронної адреси для здійснення переписки із клієнтами комерційних угод;

- придбання низки сім карток для здійснення переговорів із клієнтами, з метою подальшої зміни телефонних номерів;

- підбір категорій товарів для продажу, створення їх характеристик та наповнення інтернет-магазину інформацією про ці товари;

- обрання способу здійснення розрахунків та способу доставки;

- створення рекламних роликів, портфоліо із демонстрацією успішності комерційних проектів;

- розміщення інформації на сайтах, у ЗМІ про можливості комерційних угод;

- забезпечення сприятливих умов для вчинення шахрайства (для переконання потенційної жертви у сумлінності дій);

- підготовка засобів учинення шахрайства (комп'ютерна техніка, антураж приміщення комерційного об'єкта, фіктивні документи, різноманітні предмети для пред'явлення тощо);

- налагодження корупційних зв'язків із органами державної влади, суб'єктами, що мають відношення до супроводження комерційної діяльності в онлайн просторі.

- продумування способів приховування шахрайських дій тощо.

В контексті даної проблематики В. С. Березняк зауважує, що спосіб слід ототожнювати з інструментом або прийомом для виконання конкретних алгоритмів, наприклад, здійснення шахрайства в Інтернеті. Вчений влучно наголошує, що останнім часом спостерігається тенденція урізноманітнення способів віртуального шахрайства, що відбивається в інформаційних слідах і є важливим джерелом відомостей про суспільно небезпечну поведінку правопорушника. Для того, щоб ефективно чомусь запобігати, необхідно не тільки розуміти особливості об'єкта запобігання, але й окремо дослідити його різновиди та їхні властивості [7, с. 191].

У криміналістичній літературі можна спостерігати неодноразові спроби виокремити способи шахрайства, вчиненого в онлайн-просторі.

Так, існує безліч шахрайських схем щодо заволодіння грошима громадян, які здійснюють угоди через мережу Інтернет. Покладаючи в основу такий критерій класифікації, як зміст вчинюваних дій, С. В. Чучко всі варіанти шахрайських дій при купівлі-продажу товарів через мережу Інтернет, класифікував у такий спосіб:

- розміщення фейкової інформації про продаж товару з подальшим отриманням на платіжну карту суми повної його вартості;

- розміщення фейкової інформації про продаж товару за умов накладної плати з подальшим отриманням частини його вартості на платіжну карту (передоплати);

- створення сайтів магазинів у мережі Інтернет або їх копій, що діють за принципом фірм-одноденок;

- кібер-втручання в обліковий запис сумлінного продавця, рівень довіри якого відповідає потребам споживачів, та здійснення шахрайських угод від його імені;

- отримання грошей за лот, виставлений на інтернет-аукціоні, від декількох покупців відразу;

- отримання грошей за фальсифікований чи заздалегідь зіпсований товар;

- отримання грошей за товар, що повинний складатися з великої кількості вузлів та комплектуючих без надання всієї складової (за умов, якщо це заздалегідь сплановано);

- шахрайські дії від імені несправжнього «покупця» шляхом отримання ним інформації про номер карткового рахунку, персональні дані та номер мобільного телефону продавця «під легендою» необхідності перерахування грошей з подальшим зняттям з рахунку всіх коштів;

- отримання покупцем товару, щодо якого передбачений накладний платіж, без його оплати;

- підміна товару представником відділень поштового зв’язку [214].

На думку А. В. Рейнгольда, шахрайство в інтернет-комерції може мати достатньо широкі межі. Так, протиправні дії можуть початися з розміщення оголошення про продаж товарів та послуг, створення фіктивних сайтів, крадіжки персональних даних тощо, а закінчитися отриманням грошей від потерпілих в обмін на «не існуючі товари» чи «не існуючі послуги». Залежно від кінцевої мети, дії можуть припинятися на певному етапі. шахраї не тільки ретельно здійснюють підготовку до злочину даної категорії, але й заздалегідь планують дії з приховування. При цьому, важливим здобутком вченого вважаємо його умовиводи, що в основу шахрайських дій можуть покладатися не тільки дії щодо пропонування товарів, а й і послуг, за які потерпілі також готові сплачувати значні кошти. Практично всі послуги, які, так чи інакше пов'язані з передачею інформації, можна здійснювати через Інтернет: юридичні, консалтингові, фінансові, туристичні, медичні, психологічні та інші. Крім інформаційних послуг в Інтернеті надаються і комунікативні послуги: електронна пошта, інтернет-телефонія, відео-конференції та ін. Туроператори мають свої Web-вузли оптової торгівлі туристичними послугами, за допомогою корпоративних систем бронювання КСБ пропонують турпродукти туристичним агентствам. Онлайнова система резервування (бронювання) турів через Інтернет дозволяє турагентствам не тільки одержати повну інформацію про тур-продукти, які пропонуються, включаючи ціни, дати вильоту, категорії готелів та інші необхідні відомості, але й бронювати обраний тур у режимі реального часу. Ефективність GDS різко знизилася у зв'язку з появою Інтернет технологій, що дозволяють пропонувати кінцевим покупцям придбання послуг на пряму, безпосередньо в системах авіакомпаній та в інших постачальників туристичних послуг. Деякі авіакомпанії стимулюють інтернет-клієнтів використати електронні квитки, пропонуючи безкоштовні послуги й бонуси при їхньому оформленні. Оскільки клієнти, що діють через Інтернет, бронюють квитки, вибирають місця й повідомляють інформацію про пластикові карти безпосередньо у Інтернеті, одержання ними електронного квитка замість паперового виглядає

цілком природно. На сайтах страхових компаній відвідувач може придбати страховий поліс безпосередньо через Інтернет, порівняти ціни. Оплативши поліс, клієнт одержує його поштою або в електронній формі з електронним цифровим підписом страхової компанії. Клієнти інтернет-страховника можуть заходити на персоніфіковані сторінки для перевірки дії страхового договору, для внесення чергової страхової премії або подачі заяви про страховий випадок [161; 203, с. 48].

Вважаючи види віртуального шахрайства достатньо різноманітними, В. С. Березняк спробував виокремити найбільш поширені серед них:

– шахрайство при покупці товарів у мережі Інтернет. Такий вид шахрайства є розповсюдженим через прагнення користувача придбати товар доброї якості за ціною нижче за ринкову, однак схема завершується на отриманні від покупця передоплати;

– шахрайство з банківськими картами у випадку придбання товару в мережі Інтернет. Це стосується повідомлення додаткової інформації про банківську картку, даних з інтернет-повідомлень, виконання певних операцій з банкоматом тощо;

– шахрайство з пропозицією інтернет-заробітку та допомоги в погашенні боргу МФО;

– шахрайство через віруси-шифрувальники і сайти-фальшивки [7, с. 192; 220].

С. В. Шапочка наголошує, що у сфері е-комерції вже давно відомі фейкові банки, розповсюдження фейкових листів від чужого імені, інтернет-аукціони та ін. Натомість, автор критично зауважує, що кіберзлочинці більше не концентрують увагу виключно на хакерських атаках проти користувачів, з метою отримання доступу до особистої інформації, а більше уваги приділяють постачальникам послуг. Здійснюючи відповідну атаку і злам комп’ютерних систем провайдерів, злочинці отримують доступ до великих обсягів даних, котрі вони можуть потім підпільно продати, використати для вчинення інтернет-шахрайства. До того ж, останнім часом

широкого поширення і популяризації набуло використання децентралізованих віртуальних криптовалют: Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin тощо. Нерегульована сфера обігу віртуальних валют стала користуватися великою популярністю також серед організованих злочинних угруповань, що приймають оплату за свої послуги у віртуальній валюті, використовуючи альтернативний «темний» Інтернет – DarkNet, що функціонує на основі системи The Onion Router. Досліджені особливості криптовалют свідчать про великі потенційні можливості їх використання під час вчинення шахрайства. Це створює реальні та потенційні загрози національній безпеці України в частині використання віртуальних грошей [216; 217, с. 92].

Спробуємо висвітлити найбільш поширені способи, які нами зустрічалися в результаті аналізу матеріалів судово-слідчої практики розслідування шахрайства у сфері е-комерції, а також, ті, що висвітлюються у криміналістичній літературі та засобах масової інформації.

Як показали матеріали кримінальних проваджень, переважну кількість складають шахрайства, що вчиняються при оплаті всіляких комерційних електронних операцій, зокрема: послуг мобільного зв’язку (32 %), послуг цифрового телебачення (21 %), послуг Інтернету (52 %), оплата посередницьких послуг (21 %), оплата онлайн-квитків (авіа-, залізничного та авто- призначення) (29 %), інтернет-банкінг (54 %) тощо. Не менш поширеним є шахрайство при здійсненні електронних комерційних угод щодо купівлі-продажу товарів через мережу Інтернет (76 %).

Натомість, найбільш небезпечним видом шахрайства в е-комерції залишається фішинг [165, с. 218], що уявляє собою вид інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків та іншої конфіденційної інформації [212].

Так, 31.08.2021 р. за матеріалами ВПК в Херсонській області направлено до суду кримінальне провадження з обвинувальним актом за ч. 4

ст. 190 КК України (8 епізодів) відносно учасників організованої злочинної групи у складі 3-х осіб, які з метою заволодіння чужим майном, шляхом обману та незаконних операцій з використанням електронно-обчислювальної техніки, використовуючи мобільні телефони, здійснювали дзвінки громадянам України, представляючись працівниками служби безпеки різних банківських установ та в ході спілкування шахрайським шляхом отримувала від громадян реквізити банківських карток та іншу інформацію, яка потрібна для доступу до мобільного додатку потерпілих та в подальшому переводили кошти на банківську картку АТ «Універсал банк». Від шахрайських дій організованої групи осіб, постраждало 9 громадян, яким завдано збитків на суму 253 тис. грн. [112].

Вказаний приклад свідчить, що співробітники комерційних структур можуть часто нехтувати правилами політики безпеки. Експлуатуючи цю вразливість системи захисту інформації та корпоративної інформаційної системи в цілому, за допомогою методів соціальної інженерії, зловмисник може отримати інформацію користувача для подальших шахрайських дій [88, с. 85].

В залежності від цілей кіберзлочинців і використаних технічних засобів і методів, у класичному варіанті фішинг може мати такі прояви: 1) цільовий фішинг – атаці піддаються «цінні» жертви і компанії. Цільовий фішинг дуже ефективний, так як атака відбувається з урахуванням індивідуальних особливостей одержувача; 2) фішингова атака, націлена на топ-керівництво компанії. Інформація, яку вони можуть вкрасти, цінніше, ніж та, яку може запропонувати звичайний працівник; 3) компрометація корпоративної пошти – це злом / підміна корпоративної пошти співробітників вищого ешелону управління тощо [61].

При цьому, підробка електронної пошти – характеризується отриманням даних від користувачів без їхнього відома, шляхом: відправлення поштових листів через знайоме ім’я користувача; відправлення поштових листів, через керівника або начальника, запитуючи важливі конфіденційні

дані про користувача або про організацію; видавання себе за легітимну організацію, в якій працює користувач, з метою запиту внутрішньої інформації; використання неправильних URL-адрес – характеризується використанням URL-адреси фішинг-сторінки для зараження цілі. Зловмисник використовує домени, схожі на популярні веб-сайти та створює відповідні ідентичні сайти, де просить жертву ввести свої персональні дані у визначенні поля авторизації; використання прихованого посилання – відрізняються наявність фрази «Натисніть тут» і схожих на неї. Перехід на приховане посилання призводить до переходу на сторінку зловмисника; використання реклами – фішери підроблюють сайти з «ексклюзивними пропозиціями» в якості приманки. Прикладом даної атаки є рекламна вкладка в пошуковому браузері, де фактично коштовні послуги або додатки визначаються як ексклюзивно безкоштовні протягом певного проміжку часу, що заманює жертву з більшою можливістю скористатись пропозицією [47, с. 75].

Більше того, на сьогодні фішинг виходить за межі інтернет-шахрайства, а підроблені веб-сайти стали лише одним з безлічі його напрямків. Листи, які нібито відправлені з банку, можуть повідомляти користувачам про необхідність подзвонити за певним номером для вирішення проблем з їхніми банківськими рахунками. Ця техніка називається вішинг (підвид фішингу) (голосовий фішинг). Зателефонувавши на зазначений номер, користувач заслуховує інструкції автовідповідача, які вказують на необхідність ввести номер свого рахунку та PIN-код. До того ж вішери можуть самі дзвонити жертвам, переконуючи їх, що вони спілкуються із представниками офіційних організацій, використовуючи фальшиві номери. Набирає свої оберти й такий підвид фішингу, як SMS-фішинг, також відомий як смішинг (англ. SMiShing – від «SMS» і «фітинг»). Шахраї розсилають повідомлення, що містять посилання на фішинговий сайт, – входячи на нього і вводячи свої особисті дані, жертва аналогічним чином передає їх зловмисникам. У повідомленні також може говоритися про необхідність подзвонити шахраям по певному номеру для вирішення «проблем, що виникли» [165, с. 219]. Разом з тим,

третім різновидом шахрайства з платіжними картками є фармінг, який, як і вішинг, є різновидом фішингу. Особливістю цього виду шахрайства є те, що фармінг-технології дають змогу змінити IP-адресу сайту і під час входу на web-сторінку легітимної організації проводиться перенаправлення на підроблену, яка створена для збору конфіденційної інформації. Найчастіше такі сторінки підмінюють сторінки банків. Фармінг здійснюється двома способами: 1) на комп'ютер хакерами встановлюється шкідливе програмне забезпечення, яке автоматично перенаправляє користувача на нелегітимний сайт для викрадення конфіденційної інформації; 2) хакери вражають вірусами сервер DNC (сервіс доменів сайтів), у результаті чого кожен відвідувач відповідного сайту автоматично буде переправлений на сайт шахраїв. Цей вид шахрайства дуже складно розпізнати, оскільки підроблений сайт роблять фахівці своєї справи і його дуже важко розпізнати [38, с. 94]. Втім, останнім підвидом фішинга з платіжними картками є трешинг. Трешинг – це найбільш нестандартний метод отримання реквізитів карткових рахунків, оскільки шахраї шукають конфіденційну інформацію у канцелярному смітті та перепродують її третім особам, для яких ця інформація є вагомою [38, с. 95].

Слід зауважити, що хакерські атаки на провайдерів послуг електронної комерції та викрадення даних про їхніх клієнтів також підпадають під цю категорію шахрайства, адже це здійснюється за допомогою шкідливих програм на комп'ютерах з метою скоєння крадіжки особистих даних (identitytheft). Найбільш поширені з них – це коли використовують взаємозв'язок між клієнтами й продавцями для того, щоб фіксувати дані для входу в систему. Також існують можливості перехоплення даних за кредитними картками через пошту або при відправленні копії кредитних карток в ресторанах, готелях або в банкоматах. При цьому очевидні справжні масштаби проблеми крадіжки особистих даних [178].

Крім атак на традиційну валюту, зловмисники використовують нові тактики для обману користувачів криптовалюти, зокрема нове шкідливе програмне забезпечення, орієнтоване на гаманці у вигляді розширення

браузера для користувачів цифрової валюти, а також інновації у схемах фішингу та соціальної інженерії [15].

Як показав аналіз судово-слідчої практики, здійснення комерційних угод із використанням вкрадених кредитних карток у сфері е-комерції мало місце у 24 % випадків. Проведення транзакцій під чужою особистістю (перед цим злам аккаунта) – у 13 % випадків. Фармінг, коли фіктивні сторінки в браузері перенаправляють клієнтів, які нічого не підозрюють, на веб-сайт шахраїв, спостерігався у 18 % випадків.

У 11% нами зустрічалися випадки підробки документів з подальшою реєстрацію фіктивного підприємства та здійснення комерційних операцій в Інтернеті.

Наведемо приклад. Так, досудовим розслідуванням встановлено, що у 2015 р. невстановлена досудовим слідством особа підробила офіційні документи від імені ОСОБА_4, який втратив паспорт громадянина України та ідентифікаційний код. В подальшому, 05.02.2015 в реєстраційній службі Ірпінського міського управління юстиції в Київській області зареєстровано товариство з обмеженою відповідальністю «Інтелект Інвестмент», керівником та головним бухгалтером якого є ОСОБА_4, ІНФОРМАЦІЯ_1, зареєстрований за адресою: АДРЕСА_1. Відповідно до даних з Єдиного державного реєстру юридичних осіб та фізичних осіб підприємців встановлено, що її керівник та головний бухгалтер - ОСОБА_4, здійснив внесок до статутного фонду в розмірі 1000 гривень, хоча проведеними процесуальними діями встановлено, що ОСОБА_4 відношення до діяльності ТОВ «Інтелект Інвестмент» не має, грошових коштів до статутного фонду він не вносив, банківські рахунки не відкривав, печаткою підприємства не володів, загальні збори учасників не скликав, фінансово-господарських документів не підписував, звітів до Державних податкових інспекцій не подавав, місцезнаходження товариства йому не відоме. В подальшому на виконання доручення слідчого в порядку статті 40 КПК України оперативними працівниками оперативного управління ДПІ у

Києво-Святошинському районі ГУ ДФС у Київській області в ході аналізу АС «Податковий Блок» встановлено, що не зважаючи на пояснення ОСОБА_4, ТОВ «Інтелект Інвестмент» здійснює фінансово-господарську діяльність з іншими підприємствами, у тому числі й в онлайн-форматі, а саме: ТОВ «Ідеал Компані Плюс», ТОВ «Дельта Бай» та ін. Одним з засновників ТОВ «Ідеал Компані Плюс» є ТОВ «Київперсонал», директором якого є ОСОБА_5. В ході допиту ОСОБА_5 встановлено, що вона жодного відношення до діяльності як ТОВ «Київперсонал», так і ТОВ «Інтелект Інвестмент» та ТОВ «Ідеал Компані Плюс» не має. В подальшому в ході аналізу даних з Єдиного реєстру податкових накладних встановлено, що ТОВ «НАІ Україна», яке є контрагентом ТОВ «Ідеал Компані Плюс» протягом жовтня-листопада 2015 року формувало податковий кредит з податку на додану вартість від ТОВ «Наст Консалт», керівником якого згідно реєстраційних даних є ОСОБА_6, в ході допиту якого останній повідомив, що жодного відношення до діяльності цього товариства не має. В подальшому допитано як свідка ОСОБА_7, який відповідно до реєстраційних даних є керівником ТОВ «Оверсолд». З показів ОСОБА_7, встановлено, що він погодився зареєструвати на себе вказане підприємство без наміру ведення фінансово-господарської діяльності, за проханням ОСОБА_6. Далі аналізуючи АС «Податковий Блок», встановлені контрагенти ТОВ «Ідеал Компані Плюс», тобто підприємства, яке формувало найбільші суми податкового кредиту з ПДВ для ТОВ «Інтелект Інвестмент» [185].

Обсяг торгів на ринку цінних паперів і товарно-сировинних ринках призвели до зростання шахрайства і неправомірних дій з боку інвесторів, керівників, акціонерів та інших учасників комерційного ринку. Шахрайство з цінними паперами стає все більш складним, так як галузь розвивається з більш складними інвестиційними коштами. Крім того, шахраї розширюють сферу їх впливу і шукають нові схеми для нових ринків та нових інвесторів. Відновлення активів з доходів від шахрайства з цінними паперами є ресурсноємним і дорогим заходом через спритність шахраїв в приховуванні

активів і відмивання грошей, а також тенденції багатьох злочинців, щоб бути марнотратними розтринькувачами. Іноді втрати, викликані шахрайством з цінними паперами важко піддаються кількісній оцінці. Наприклад, в інсайдерській торгівлі можна підвищити вартість капіталу для емітентів цінних паперів, тим самим знижуючи загальне економічне зростання [243]. Шахрайська інформація поширюється в чатах, форумах, інтернет-дошках і електронною поштою (у вигляді спаму), з метою різкого збільшення цін на торгові акції або акції підставних компаній . Коли ціна досягає певного рівня, злочинці одразу ж продають свої запаси таких компаній, отримуючи значний прибуток до того, як ціна акцій опуститься до звичайного низького рівня. Всі покупці акцій, які не знають про шахрайство стають жертвами, як тільки ціна падає [241].

Нерідкими у сфері е-комерції є вчинення шахрайства, пов’язаного із заволодіння обманним шляхом персональними даними з подальшим переказом грошей на електронний гаманець.

Так, досудовим розслідування встановлено, що у лютому 2014, ОСОБА_4, усвідомлюючи суспільно-небезпечний характер свого діяння, передбачаючи його суспільно-небезпечні наслідки у вигляді заподіяння майнового збитку потерпілому і бажаючи їх настання, діючи з прямим умислом, повторно, з корисливих мотивів, з метою особистого збагачення, попередньо представившись фахівцем в сфері ІТ-технологій, під приводом отримання високого прибутку при роботі в системі «Webmoney» (електронна система онлайн-платежів, інтернет-розрахунків, середовище для ведення бізнесу та електронної комерції для її учасників), а саме шляхом отримання відсотків при передачі учасником системи іншому учаснику (трансфері) майнових прав, облік яких здійснюється за допомогою спеціальних розрахункових розписок «титульних знаків», номінованих в прив`язці до різних валют і золота, а також пообіцявши повернути кошти з відсотками, зловживаючи довірою потерпілої ОСОБА_7 отримав від останньої персональну інформацію по картковому рахунку № НОМЕР_1 відкритого у

АТ «ПриватБанк», з якого в подальшому шляхом використання мережі Інтернет використовуючи агрегатор платіжних методів для інтернет-бізнесу Групи FinTech компаній Interkassa, в період з 25.02.2014 по 08.03.2014 здійснив ряд переказів з вказаного карткового рахунку на електронний гаманець № НОМЕР_2 відкритий у Wallet One - міжнародна платіжна система, що працює у всіх сегментах ринку електронних платежів, тим самим заволодів грошовими коштами на загальну суму 1864,77 доларів США, що згідно курсу НБУ на момент вчинення злочину складало 20522,5 гривень, без наміру їх повертати потерпілій ОСОБА_7 [181].

Шахрайські операції з обміном та обготівкування електронних грошових коштів між користувачами різноманітних платіжних систем також дедалі стають поширеними у сфері е-комерції.

Так, протягом 2016-2017 року гр. ОСОБА_7 та ОСОБА_8 з використанням інтернет-ресурсів здійснювали операції з обміном та обготівкування електронних грошових коштів між користувачами різноманітних платіжних систем, а також збирали данні, за допомогою яких неправомірно використовували ввірені їм електронні грошові кошти та засоби їх переказу [180].

У ході вивчення матеріалів судово-слідчої практики щодо шахрайства у сфері е-комерції нами зустрічалася низка випадків з приводу встановлення мобільного додатку із обіцянкою працевлаштування та оформлення кредиту.

Так, 26.10.2020 року приблизно о 13 год. 15 хв., ОСОБА_8 зустрівся із ОСОБА_4, яка мала намір працевлаштуватись кур`єром з допомогою ОСОБА_8, в м. Івано-Франківську на вул. Площа Ринок. В ході розмови, ОСОБА_8 повідомив потерпілій про те, що для того, щоб отримувати замовлення кур`єрської доставки на її мобільний телефон необхідно встановити мобільний додаток, за допомогою якого вона буде отримувати замовлення про доставку певного товару і виконуватиме вказане замовлення. Будучи переконаною в добросовісності намірів останнього, щодо допомоги у працевлаштуванні, ОСОБА_4 добровільно передала останньому власний

мобільний телефон марки «Huawei p30 lite» модель «MAR-LX1A», у якому була встановлена SIM карта оператора мобільного зв`язку ПрАТ «ВФ Україна» НОМЕР_2. Отримавши вказаний мобільний телефон, ОСОБА_8, діючи умисно, з метою протиправного заволодіння кредитними грошовими коштами, шляхом використання особистих даних потерпілої, усвідомлюючи суспільно-небезпечний характер своїх дій, встановив на мобільний телефон ОСОБА_4 додаток «Smartiway», за допомогою якого створив заявку НОМЕР_3 на отримання кредиту у сумі 3 000,00 гривень на рахунок потерпілої. Цього ж дня о 13 год. 16 хв. за допомогою встановлення додатку «Smartiway» та використання особистих даних ОСОБА_4, між останньою та ТОВ «СМАРТІВЕЙ ЮКРЕЙН» укладено електронний договір від 26.10.2020 у відповідності до статей 3, 11, 12 Закону України «Про електронну комерцію», у зв`язку із чим на банківському рахунку позичальника НОМЕР_4 згідно з наданими реквізитами платіжної картки було зараховано 3 000,00 грн. ідентифікаційний номер платежу НОМЕР_5. З метою доведення свого протиправного умислу до кінця, ОСОБА_8, діючи умисно, шляхом обману, повідомив потерпілій, що з метою перевірки правильності роботи мобільного додатку та коректного нарахування заробітної плати, перерахував на її рахунок особисті кошти і попросив йому їх повернути. ОСОБА_4, не знаючи про те, що вказані грошові кошти є кредитними та будучи переконаною про добросовісність намірів ОСОБА_8 щодо перерахування своїх власних коштів на її рахунок, здійснила переказ нарахованих на її банківський рахунок НОМЕР_4 грошових коштів двома платежами, а саме 26.10.2020 року о 13 год. 30 хв. у сумі 2 700,00 грн., а також 30.10.2020 року о 07 год. 56 хв. у сумі 250,00 грн. на рахунок по номеру банківської карти НОМЕР_6, яка зареєстрована на ОСОБА_8. В подальшому ОСОБА_8 грошовими коштами, якими заволодів шляхом обману потерпілої, розпорядився на власний розсуд, чим спричинив потерпілій ОСОБА_4 майнову шкоду на загальну суму 2 950 гривень [179].

Шахрайські дії під приводом прийняття внесків як інвестицій у криптовалюту, управління фінансовими активами, надання інших фінансових послуг в мережі Інтернет складають приблизно 11 % випадків.

Наведемо один із численних прикладів. Так, досудовим розслідуванням встановлено, що працівниками ВПК в Кіровоградській області в ході моніторингу всесвітньої мережі Інтернет отримана інформація про те, що група осіб, мешканців міста Кропивницького вчиняє протиправну діяльність, пов`язану із шахрайським заволодінням коштами громадян у сфері е-комерції, зокрема шляхом залучення коштів у віртуальні проекти (так званні «фінансові піраміди»). Під приводом прийняття внесків як інвестицій у криптовалюту, управління фінансовими активами, надання інших фінансових послуг в мережі Інтернет. Під час проведення слідчих (розшукових) дій встановлено, що Заворітній та ОСОБА_4 в мережі Інтернет в соціальній мережі Інтернет розміщували інформацію стосовно фіктивної інвестиційної діяльності, компанії «ІНФОРМАЦІЯ_2». Для реалізації своєї злочинної діяльності створювали спеціальні сайти. Так, мешканець м. Кропивницького гр. ОСОБА_5, будучи введений в оману за допомогою різноманітних онлайн-семінарів, тренінгів, які відбувались в мережі Інтернет та відеохостингах в дійсності інвестиційної компанії «ІНФОРМАЦІЯ_2», під психологічним впливом вищевказаних осіб та за їх прямими вказівками зареєстрував аккаунт в компанії «ІНФОРМАЦІЯ_2» на сайті «ІНФОРМАЦІЯ_2» та під виглядом інвестиційних внесків вніс грошові кошти у сумі 15 000 доларів США, та в подальшому вищевказана компанія припинила свою діяльність, та обіцяні відсотки від суми внеску та самі грошові кошти, які ОСОБА_6 вклав останній не отримав [180].

Через пандемію COVID-19 та повномасштабне вторгнення рф на територію України частішають випадки вчинення шахрайства у сфері волонтерської діяльності та благодійної допомоги, у тому числі під виглядом електронної комерційної діяльності.

Щодо способів приховування, то ними можуть бути: фальсифікація документації; використання соціальних мереж, месенджерів для мінімізації особистісних контактів правопорушника з іншими особами; використання корупційних зв'язків; використання разових (не особистих) номерів мобільних телефонів; використання службових можливостей; тощо. У цілому приховування зводиться до того, що правопорушники активно в механізмі протиправної діяльності використовують інформаційні та цифрові технології. Мова йде про те, що, наприклад, продаж товарів правопорушник може вчинити без відсутності прямого контакту з покупцем. Наприклад, оголошення про продаж здійснюється шляхом розміщення повідомлення на сайті «OLX»; обліковий запис створюється із зазначенням несправжніх особистих даних; переписка з імовірними покупцями відбувається через вказаний застосунок; оплата здійснюється в безготівковій формі; товар надсилається покупцеві за допомогою кур'єрської служби «Нова пошта» тощо[221, с. 56]. Способами приховування шахрайства може також виступати маскування зовнішності при спілкуванні через засоби відеозв'язку, зміна голосу при спілкуванні телефоном тощо.

Виходячи із наведених думок та на підставі аналізу судово-слідчої практики розслідування шахрайства у сфері е-комерції, спробуємо класифікувати способи їх учинення на такі групи:

- здійснення електронних комерційних угод із використанням вкрадених кредитних карток;

- здійснення електронних комерційних угод, проведення транзакцій із викраденими персональними даними (під «чужою особистістю»);

- здійснення електронних комерційних угод від імені фіктивного суб'єкта підприємницької (комерційної) діяльності;

- шахрайські операції під час інтернет-банкінга внаслідок здійснення електронних комерційних угод;

- шахрайські операції шляхом перенаправлення клієнтів в браузері на веб-сайт шахраїв для здійснення комерційних угод;

- шахрайське заволодіння персональними даними суб'єктів комерційної діяльності з подальшим переказом грошей на електронний гаманець;

- шахрайські операції з обміном та обготівкування електронних грошових коштів між користувачами різноманітних платіжних систем;

- шахрайські операції із встановленням мобільного додатку із обіцянкою виконання певних послуг (працевлаштування та оформлення кредиту тощо);

- шахрайства у сфері волонтерської діяльності та благодійної допомоги, здійснюваної через мережу Інтернет;

- шахрайські дії під приводом прийняття внесків як інвестицій у криптовалюту, управління фінансовими активами, надання інших фінансових послуг в мережі Інтернет;

- шахрайства з цінними паперами;

- шахрайські дії шляхом залучення коштів у віртуальні комерційні проекти;

- фішингові атаки на комп'ютерні системи суб'єктів комерційної діяльності, із подальшим вчиненням шахрайських дій тощо.

1.3. Обстановка та слідова картина шахрайства. Предмет злочинного посягання

Вагоме місце у структурі криміналістичної характеристики кримінальних правопорушень займає обстановка їх скоєння, оскільки, перебуваючи у закономірному взаємозв'язку з іншими елементами зазначеної характеристики, вона слугує підґрунтям для висунення й перевірки слідчих версій та зумовлює особливості побудови методики розслідування таких кримінальних правопорушень [142, с. 198]. Натомість, серед всіх елементів криміналістичної характеристики кримінальних правопорушень саме

обстановка є найбільш спірним елементом, що у криміналістичній літературі розглядається у різних аспектах.

Не піддаються сумніву з боку вчених лише два елемента – місце й час вчинення кримінального правопорушення, що входять в обстановку, адже діяльність винного неможлива поза простором і часом. Немає таких матеріальних об'єктів, виникнення, розвиток і зникнення яких не проходило б у певному місці й в певний час [173, с. 12]. Разом з тим, мусимо зауважити, що епоха динамічного розвитку інформаційно-комунікаційних технологій, однією з яких є Інтернет, призвела до виникнення віртуального простору – особливого електронного середовища взаємодії, в якому будь-які дії з інформацією вчиняються за допомогою цифрових сигналів [232, с. 213].

Говорячи про шахрайства в е-комерції, слід сказати, що в електронному середовищі існують технічні можливості для соціальних контактів, безвідносно місця перебування людини, з можливістю уникнення безпосереднього контакту. Завдяки електронним пристроям різного рівня складності, підключених до глобальної або локальної мережі, й виникає віртуальне середовище [235, с. 39]. При цьому, суттєвою особливістю кібершахрайств є те, що для них відсутнє просторове обмеження і вчинення злочину може виходити за рамки однієї держави. Протиправні дії можуть вчинятися в одній державі, а негативні наслідки настають в іншій [93, с. 874].

У цьому розрізі слушною вважаємо думку С. В. Чучко, який пропонує до обстановки вчинення кібершахрайств включити ще й інформаційне середовище та засоби комп'ютерної техніки, за допомогою яких здійснюють комерційні операції [214].

Отже, провівши ґрунтовний аналіз наукових думок, враховуючи специфіку здійснення комерційних операцій в онлайн-просторі, пропонуємо до обстановки шахрайств, вчинених у сфері е-комерції, включити такі елементи:

- зв’язки між особою шахрая та особою потерпілого та інші чинники об’єктивної реальності, які визначають можливість, умови та інші обставини вчинення шахрайства у сфері е-комерції;

- особливості нормативно-правового регулювання сфери е-комерції, що зумовили можливість для здійснення шахрайських операцій;

- час, протягом якого здійснювалися комерційні операції між суб’єктами;

- час, коли наступили наслідки від протиправних дій внаслідок здійснення комерційних операцій в онлайн-просторі;

- місце вчинення шахрайства у сфері е-комерції (віртуальне середовище, в якому вчиняються шахрайства і місця, де знаходяться точки доступу (Ір-адреси), з яких здійснювався контакт між суб’єктами комерційних операцій) тощо.

З цього приводу, слід зауважити, що у науковому колі місце вчинення кримінального правопорушення звичайно розглядають як у широкому розумінні, з позиції географічних координат, так і у вузькому – як конкретне місце його вчинення.

При цьому, безпосереднім місцем вчинення кримінального правопорушення, як правило, визнається не конкретний простір, який має точні координати, а певні ланки суспільно-виробничої або іншої громадсько-соціальної системи (конкретні підприємства, дільниці тощо) [142, с. 199].

Враховуючи специфіку кібершахрайств, В. М. Бутузов вірно підмічає, що можливо виокремити місця їх вчинення: фізичне середовище (ділянки місцевості) та електронне середовище (вузли мережі), де розташовані: програмно-технічні засоби (носії інформації), що зазнали злочинного впливу, та точки їхнього доступу до певних мереж; програмно-технічні засоби, які злочинець використовував опосередковано, та точки їх доступу до певних мереж; мережні вузли каналів зв’язку, з використанням яких відбувався обмін

інформацією між програмно-технічними засобами злочинця та потерпілого [21, с. 72].

З цього виходить, що у вузькому розумінні до місця вчинення шахрайств, учинених із використанням мережі «Інтернет», можна віднести місцезнаходження: а) банкоматів (магазин, вулиця тощо) (42 %); б) підключених до мережі «Інтернет» комп'ютерних систем (місце роботи, навчання, проживання, «Інтернет-кафе», зона вільного підключення до мережі «Інтернет» із використанням технології «Wi-Fi» - так звані «FrceWi-Fi-zone» romo) (78 %); в) установ, де впроваджено системи розрахунків за допомогою пластикових кредитних карток (36 %) тощо [171, с. 8].

До того ж, як свідчать матеріали судово-слідчої практики, у фізичному розумінні нерідко місцями вчинення шахрайства у сфері е-комерції виступають установи виконання покарань (41 %).

Так, 27.05.2021 за матеріалами ВПК у Вінницькій області направлено до суду кримінальне провадження з обвинувальним актом за ч. 4 ст. 190, ч. 5 ст. 27, ч. 2 ст. 190 КК України (7 епізодів) відносно учасників організованої злочинної групи у складі 4-х осіб, які під час відбування покарання в установі виконання покарань – Державній установі «Вінницька виправна колонія № 86», видаючи себе за працівників служби безпеки банків, вчиняли шахрайські дії спрямовані на заволодіння коштами громадян, шляхом отримання від постраждалих коштів за поповнення страхових рахунків. Від шахрайських дій організованої групи, постраждало 7 осіб, яким завдано збитків на суму 308,5 тис. грн. [113].

Якщо вести мову про місце вчинення шахрайства у сфері е-комерції у географічному розумінні, прив'язуючись до місця знаходження комп'ютерної техніки, за допомогою якої здійснювалися комерційні операції, слід відзначити, що 92 % усіх «віртуальних комерційних угод» здійснюється у великих містах мегаполісах. При чому, відсоток суб'єктів, які пропонують товари та послуги комерційного призначення, набагато більше, ніж відсоток

осіб, які потребують таких товарів та послуг, що пояснюється дефіцитом таких об’єктів у невеликих містах.

В контексті даної проблематики Т. В. Орехова та М. В. Дубель, оцінюючи вплив процесу діджиталізації на розвиток електронної комерції в Україні, наводять аргументи з приводу того, що українці звикають купувати в онлайні по всій країні, але традиційними лідерами з «поставки» для інтернет-магазинів є Київ і область. Наступною за комерційною активністю є Дніпропетровська область, далі розташувались Харківська та Одеська. Одним з найважливіших переваг онлайн-торгівлі є відсутність прив'язки до регіону. Досвідчений інтернет-комерсант отримує в якості клієнтів всіх жителів України [127, с. 22]. Втім, слід констатувати, що стрімко зростає й проникнення Інтернету в сільській місцевості. Років 5-7 тому різниця між проникненням доступу до Мережі в селі і місті була дуже великою. Зараз же більше 60% людей, які проживають в сільській місцевості, мають доступ до онлайну [127, с. 18]. При цьому, за інформацією С. А. Думчикова та В. В. Лукічова, мешканці сіл частіше натрапляють на продаж неіснуючого товару по передоплаті, а мешканці мегаполісів – на фішингові атаки. Місце проживання значно впливає на тип шахрайств. Наприклад, дві треті жителів селищ міського типу та сіл стикаються зі спробами продати їм неіснуючий товар за передоплатою, а от жителі міст у 1,5 рази частіше отримують фішингові посилання. Жителі райцентрів на третину частіше за інших стикаються з підробленими квитанціями про оплату. У селах в цілому менше обізнаних з базовими правилами кібербезпеки. Якщо понад 42% містян не ведуть спілкування за межами платформи, де здійснюють угоду, та не відкривають посилання від незнайомих людей, то серед мешканців сіл – це тільки 33% опитаних. Водночас жителі столиці найбільше потерпають від фішингу (36% від всіх видів онлайн-шахрайств у Києві), а от у Дніпрі, Одесі, Харкові та Львові половина випадків пов’язана з передоплатою неіснуючого товару. Найбільш відповідально до звернень у Кіберполіцію ставляться у Львівській області – кожний 8-ий ошуканий подасть заяву, а найменш – в

Одеській – тут звернеться тільки кожний 14-ий [42]. Понад 90% комерційних операцій робились з персонального комп'ютера, а частка мобільних пристроїв у цьому рейтингу склала навіть менше 10 %. 38 % українських онлайн-покупців не менш ніж раз у рік роблять покупку в закордонному інтернет-магазині. Але 45 % користувачів ніколи не купували на закордонних ресурсах, а основним стримувальним фактором називають мовний бар'єр [127, с. 24].

Як показав аналіз судово-слідчої практики, специфікою обстановки вчинення шахрайств у сфері е-комерції є розпливчастість часових меж, адже дуже складно визначити початок вчинення шахрайських дій та їх закінчення.

Хоча, не всі науковці вважають проблемою встановлення часових меж при розслідуванні шахрайств, вчинених у кіберпросторі. Так, на думку В. О. Голубєва, встановлення часу вчинення кіберзлочинів не складає великих проблем, оскільки операційна система електронного пристрою детально стежить практично за кожною важливою операцією, інформація про які відображається в статистичних файлах. За допомогою програм загальносистемного призначення можна встановити поточний час роботи комп'ютерної системи. Це дозволить за відповідною командою вивести на екран дисплею інформацію про день, години, хвилини та секунди виконання тієї або іншої операції [27, с. 101]. Натомість, Я. Неділько з цього приводу справедливо наголошує, що не відкидаються випадки, коли час вчинення кримінального правопорушення установити неможливо. Це може бути зумовлено технічними причинами, зокрема під час перезавантаження електронного пристрою повністю або частково обнуляються чи стираються дані тощо. Тому в таких випадках час вчинення необхідно встановлювати шляхом проведення судової комп'ютерно-технічної експертизи. Крім того, час вчинення кібершахрайства можна встановити проведенням слідчих (розшукових) дій. Також слід звертати увагу чи час виставлений на електронному пристрою співпадає з поточним і чи не корегувався він [122, с. 361].

Переходячи до наступного елемента криміналістичної характеристики – слідової картини, слід зазначити, що більшість вчених її розглядають як сукупність матеріальних, ідеальних та віртуальних (інформаційних) слідів які відображають картину події злочину, поведінку злочинця, потерпілого та інших осіб як на місці вчинення злочину, так і поза його межами, що дозволяє висунути найбільш обґрунтовані версії щодо його вчинення та приймати найбільш раціональні процесуальні рішення під час проведення досудового розслідування [92, с. 451].

Слід сказати, що шахрайство з використанням комп'ютерних мереж, незважаючи на еволюційні процеси, залишається злочином проти власності, що вчиняється з використанням обману чи зловживання довірою. Різниця полягає лише в тому, що обман відбувається не під час безпосереднього фізичного вербального чи невербального контакту з жертвою, а дистанційно, тобто з використанням можливостей комп'ютерно-телекомунікаційних пристроїв, систем або мереж [219, с. 159]. Тому, окрім традиційних ідеальних та матеріальних слідів, у криміналістичній характеристиці шахрайства у сфері е-комерції слід виокремлювати й віртуальні (електронні, цифрові) сліди, які мають важливе значення.

Цифрові (віртуальні) сліди, що утворюються під час вчинення кіберзлочинів – це інформація, яка зафіксована у цифровому форматі, міститься в різного роду цифрових пристроях зі створення, обробки, збереження та передачі цієї інформації, причинно пов'язана з подією кіберзлочину та дозволяє встановити як обставини вчиненого правопорушення, так і особу кіберзлочинця [124, с. 461].

У теорії криміналістики є різні думки про те, що варто розуміти під віртуальними слідами: 1) віртуальні сліди як зміна автоматизованої інформаційної системи; 2) віртуальні сліди з точки зору фізичної і квантової теорії; 3) віртуальні сліди як результат логічних і математичних операцій з двійковим кодом і багато інших. Натомість, дотепер немає точного визначення віртуальних слідів. Автори розглядають поставлене питання з

різних точок зору: одні з точки зору впливу людини на комп'ютерні системи, інші з точки зору фізичних зв'язків комп'ютерних систем, треті – з точки зору здійснення певних операцій [119, с. 305]. При цьому, як наголошує Н. М. Ахтирська, сліди вчинення кіберзлочинів можуть знаходитись не лише безпосередньо в комп'ютерній техніці, на флеш-носіях, а і в кіберпросторі – середовищі (віртуальному просторі), яке надає можливості для здійснення комунікацій та реалізації суспільних відносин, комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет або інших глобальних мереж передачі даних [5, с. 138].

О. В. Кузьменко до слідів, як елементів криміналістичної характеристики кіберзлочинів, відносить: матеріально фіксовані сліди (документи, відбитки, технічні пристрої тощо); відомості та дані, зафіксовані в цифровій формі на матеріальних носіях; електронна інформація, створена комп'ютером чи людиною; програмне забезпечення; комп'ютерні системи [98, с. 165].

Я. Найдьон для розкриття кримінальних правопорушень у кіберпросторі вважає за можливе використання таких видів слідів: електронна поштова скринька. Тут можуть бути залишені віртуальні сліди у вигляді переписки з питань створення та поширення інформації; інтернет-сайт. Зазвичай це популярні ресурси в мережі Інтернет; профіль у соціальних мережах («ВКонтакте», «Instagram», «Фейсбук», «Одноклассники», «Твіттер» та ін.); рахунок в електронних платіжних системах («Qiwi-гаманець», «Яндекс. Деньги», Perfect Money та ін.); база даних (абонентів операторів зв'язку та ін.); локальна мережа. Можливість доступу до ресурсів (програм, файлів, папок та ін.) усіх з'єднаних між собою за допомогою кабелів (телефонних ліній, радіоканалів) комп'ютерів; сліди на жорсткому диску, що містить інформацію про його включення, застосування різних матеріалів, надсилання рахунків, виконання інших маніпуляцій. Завдяки роботі пам'яті комп'ютера відомості про активності ресурсів

операційної системи зберігаються, тому їх можна використовувати як джерело доказів у кримінальному процесі [119, с. 305].

Ще більше звужує перелік віртуальних слідів Т. В. Романенко, яка виділяє серед них: реєстраційні дані на доменне ім'я; логи від взаємодії з реєстратором доменних імен; сліди від проведення платежу цього реєстратора; сліди при налаштуванні DNS-сервера, що підтримує домен шахраїв; сліди від взаємодії з хостинг-провайдером, в якого розміщений веб-сайт: замовлення, оплата, настройка; сліди від рекламування веб-сайта: взаємодія з рекламними майданчиками, системами банерообміну, розсилка спаму; сліди від відстеження активності користувачів на сайті тощо. При взаємодії з жертвами обману шахраї залишають сліди при прийомі замовлень – електронною поштою, через СМСповідомлення, через ICQ або веб-форму; від листування з потенційною жертвою [164, с. 53].

Важливість віртуальних (цифрових, електронних) слідів важко переоцінити. Натомість, матеріальні та ідеальні сліди також відіграють важливу роль при виявленні шахрайства у сфері е-комерції. Так, ідеальні сліди можуть знаходитися в пам'яті осіб, які можуть надати інформацію з приводу вчиненого шахрайства, осіб, які до нього причетні. Здебільшого інформацію про зовнішність шахрая потерпілі можуть надати у випадку безпосередньої зустрічі до, або після здійснення комерційної електронної угоди, або якщо спілкування здійснювалося у форматі відеоконференції. Матеріальні сліди можуть міститися у роздрукованих документах, скриншотах переписки, квитанціях тощо, а також можуть залишатися на комп'ютерній техніці, на магнітних носіях і оптичних дисках тощо.

Переходячи до предмету шахрайства у сфері е-комерції, слід зазначити, що у більшості випадків під час вчинення шахрайства у сфері е-комерції безпосереднім предметом злочину є грошові кошти, у тому числі й віртуальні, але, як правило, заволодіння правом на майно також має місце [20, с. 221]. При цьому, об'єкти віртуального простору можуть виступати предметом шахрайства, якщо вони відповідають таким вимогам: а) вони

створені особою або придбані нею за гроші; б) вони мають споживчу цінність; в) ними можна користуватися та розпоряджатись у віртуальному просторі; г) їхня оцінка дає можливість визначити ринкову вартість [56, с. 236].

У сегмент електронної комерції заходять все нові категорії, користувачі все частіше купують через Інтернет товари та послуги, які раніше віддавали перевагу шукати в офлайні. За рахунок цього зростає весь ринок e-commerce в Україні [205, с. 45]. Так, українці шукають в Інтернеті інформацію про такі товари і послуги: 1) про готелі і кредити – 92%; 2) про міжміський транспорт – 90%; 3) про авіаквитки, музику, а також вітаміни і ліки – 87%; 4) про ноутбуки і нерухомість – 81%; 5) про інструменти та DYI (інструкції з ремонту та будівництва) – 79%; 6) про побутову техніку – 77%; 7) про телефони і телевізори – 76%; 8) про квитки в кіно і меблі – 74%; 9) про одяг і взуття – 64%; 10) про ресторани і косметику – 58%; 11) про страхування авто і догляд за волоссям – 53%; 12) про продукти – 31% [127, с. 24].

Втім, як слушно наголошує А. В. Рейнгольд, починаючи з 2019 року нашу країну охопила пандемія Covid-2019, внаслідок чого об’єктами комерціалізації в мережі Інтернет стали ліки від цієї хвороби, маски, апарати штучного дихання тощо. Відповідно, дані об’єкти стали фігурувати й у провадженнях щодо шахрайства в інтернет-комерції. До того ж, на момент повномасштабного вторгнення рф на територію України 24 лютого 2021 року електронна комерція пережила спочатку шокове падіння, потім сплеск попиту на окремі категорії товарів і нарешті певну стабілізацію після масового переміщення людей, релокації складів та виробництв. Облаштування людей на новому місці або повернення їх додому поступово повертає продажі в Інтернеті до зростання. Проте попит змінився. Прихильність до брендів у споживачів дуже низька – купують те, що є. Динаміку зростання зберігають категорії, які закривають базові потреби: продукти харчування, сигарети, медикаменти, взуття та одяг, гігієнічні та господарчі товари, товари для тварин. По мірі відновлення країни у топі продажів опиняться будматеріали,

товари для дому, техніка та електроніка. Шахраї дуже швидко реагують на потреби українців, намагаючись пристосуватися до реалій сьогодення. Так, під час воєнного стану частішають випадки, коли предметом шахрайства в інтернет-комерції виступають речі, необхідні для несення служби у зонах бойових дій (воєнний одяг (14 %), бронежилети (3 %), каски (3 %), воєнна техніка (2 %) тощо) [160].

Разом з тим, дедалі частіше можна спостерігати наукову думку про віднесення інформації до предмета посягання шахрайства, зокрема: а) особистої конфіденційної інформації, якою може бути таємниця листування, телефонних розмов, поштових, телеграфних чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер; інформації, що є об'єктом авторських і суміжних прав; інформації щодо персональних даних тощо б) конфіденційної інформації юридичних осіб: службової таємниці; комерційної або банківської таємниці тощо. До того ж, останнім часом збільшилася кількість випадків заволодіння інформацією про власників платіжних банківських карток та їх реквізити. До такої інформації, як правило, належить: а) ім'я та прізвище держателя картки; б) назва/код структурного підрозділу банку, що випустив картку; в) термін дії картки; г) номер картки [16, с. 42; 86, с. 45].

Таким чином, у провадженнях щодо шахрайства у сфері е-комерції предметом злочинного посягання можуть бути: товари; послуги; цінності; цінні папери: корпоративні акції, облігації, векселі (у тому числі електронні);гроші (як у готівковій, так і у безготівковій формі); право на майно; інформація комерційного призначення.

1.4. Характеристика особи злочинця та потерпілого

Розвиток і гіперактивний прогрес сучасних ІТ-технологій в реаліях сьогодення стосується кожної людини, і всі суб'єкти господарювання, які

надзвичайно цінують свій час і витрачені ресурси (матеріальні, грошові, трудові тощо), не є винятком і все частіше намагаються здійснювати комерційні операції за допомогою інформаційно-комунікаційних технологій, що включає всі фінансові та торгові трансакції, які проводяться за допомогою ІКТ, та бізнес-процеси, пов'язані з проведенням таких трансакцій [187].

Отже, фактично потерпілим від шахрайства у сфері е-комерції може стати будь-який громадянин, який віддає перевагу веденню бізнесу в електронному режимі.

Разом з тим, потерпілими інтернет-шахрайства можуть стати не тільки громадяни, але й юридичні особи, підприємства, установи та організації різних форм власності [7, с. 191]. Цю думку підтверджує й В. Г. Хахановський. Це зумовлено тим, що процес комп’ютеризації широко охоплює, насамперед, юридичних осіб (організації, установи), а значно меншою мірою – фізичних осіб [202, с. 92].

Натомість, як показав аналіз судово-слідчої практики, кількість потерпілих у особі фізичних осіб у провадженнях щодо шахрайства у сфері е-комерції також є достатньо великою (44%). В основному фізичні особи виступають потерпілими при здійсненні роздрібної купівлі-продажу товарів або послуг на онлайн-платформах, на інтернет-аукціонах, під час здійснення інтернет-банкінгу тощо.

Водночас, юридичні особи (підприємства, установи, організації, корпорації та ін.) можуть стати потерпілими у таких випадках:

- при здійсненні господарських операцій між юридичними та фізичними особами (постачання та придбання товарів та послуг шляхом використання електронних технологій);

- при здійсненні матеріально-технічного постачання з використанням засобів електронної комерції у виробничому циклі підприємства;

- при пошуку нових ринків збуту;

- у процесі обміну певними товарами та послугами;

- при наданні логістичних послуг;

- при здійсненні брендингу та просування торгової марки компанії;

- при забезпеченні фінансовими установами трансакцій між суб’єктами;

- при наданні іншим підприємцям власно-створеного онлайн-майданчику для створення магазинів і торгівлі своїм товаром (маркетплейси) тощо.

Більшість потерпілих становлять молоді люди з вищою освітою, які проживають в містах. Трохи більше 36 % з них – жителі міст з населенням понад 500 000 чоловік, 20,5 % – проживають в сільській місцевості [127, с. 18]. Натомість, серед всіх вікових категорій 80 % випадків онлайн-шахрайств відбуваються у месенджерах (Viber, Telegram, WhatsApp). Пенсіонерам утричі частіше надсилають шахрайські SMS, у сім раз електронні листи. Водночас 57 % українців віком від 46 до 65 років натрапили на шахраїв, які просили зробити передоплату за неіснуючий товар. Молодь віком 18-25 років у кожному третьому випадку натрапляє на фішинг, а кожний четвертий неповнолітній втратив гроші після переходу за шкідливим посиланням на сайт підробку відомого бренду. Це пов’язано з тим, що молодь більше за старше покоління проводить час в онлайні, але так само слабо обізнана з базовими правилами кібербезпеки. Молодь більш обізнана з базовими правилами кібербезпеки, однак загальний рівень навичок онлайн-поведінки лишається невисоким [42]. Разом з тим, при вчиненні шахрайств у сфері е-комерції, пов’язаних із цінними паперами, будь-який інвестор може стати жертвою. Втім, людина у віці п'ятдесяти років і старша, найчастіше стає жертвою як прямий покупець цінних паперів або непрямий покупець через пенсійні фонди. Мало того, що жертвами можуть стати інвестори, але ними можуть стати і кредитори, податкові органи, співробітники тощо [242].

Як показав аналіз судово-слідчої практики щодо розслідування шахрайства у сфері е-комерції, стать практично не впливає на вірогідність натрапити на шахрая, адже як чоловіки, так і жінки отримують шкідливі посилання від шахраїв у соціальні мережі, здійснюють платіжні операції

через Інтернет, укладають електронні угоди купівлі-продажу, здійснюють інші комерційні операції шляхом використання електронних технологій.

Щодо особи шахрая, слід сказати, що специфіка вчинення шахрайства більшою мірою вимагає від злочинців винахідливості, хитрості, комунікабельності, вміння фантазувати та схиляти на свій бік опонентів, освіченості та обізнаності у юридичних питаннях тощо. Особи, які вчиняють шахрайство часто є фахівцями у різних галузях: економіки, права, інформаційних технологій та банківської справи. Якщо навіть шахраї не є фахівцями у певній галузі, вони мають корупційні зв'язки із обізнаними особами та отримують від них консультаційну допомогу. Нерідко їм відомі методи роботи правоохоронних органів. У 23% випадків простежується факт сприяння держслужбовців у вчиненні шахрайства. В цілому для вчинення злочину даної категорії характерний високоінтелектуальний підхід. Вказане свідчить про важливість характеристики особи з позиції громадянства, регіону проживання, соціального становища, освіти, професії, сімейного стану тощо [99].

Говорячи про вікові особливості, то переважна більшість шахрайств у сфері е-комерції вчиняються у віці від 16 до 50 років. Це можна пояснити активністю використання цифрових технологій саме особами даної вікової категорії та адаптацією до процесів діджиталізації.

Спостерігається переважна більшість шахраїв чоловічої статі (68%). 62% шахраїв мали вищу освіту, більшість з них одружені (заміжні) (56 %).

Слід зауважити, у криміналістичному аспекті особа сучасного кіберзлочинця має певну індивідуальну специфіку, що обумовлюється наявністю у таких осіб спеціальних знань та навичок з використання інформаційних технологій для досягнення злочинного наміру [121, с. 203]. До того ж, лише деякі злочинці інтернет-шахрайства діють без співучасників, тоді як більшість із них скоюють кримінальні правопорушення у складі організованих злочинних угрупувань [11, с. 83].

О. М. Брисковська і В. А. Пустовіт акцентують, якщо раніше зловмисники вчиняли інтернет-шахрайства одноосібно, то сьогодні вони стали згуртовуватися, починаючи від групи осіб за попередньою змовою до більш складного рівня організованості, формуючи організовані групи та об'єднання, щоб діяти більш масштабно та зухвало, за короткий термін часу значно збільшуючи суму збитків та кількість постраждалих від такого шахрайства, забезпечуючи прикриття від виявлення, контролю та відповідальності. Такі організовані злочинні групи, як правило, є організованими злочинними групами економічної спрямованості [20, с. 221].

На цьому зосереджує увагу й С. В. Шапочка, який зазначає, що має місце швидке налагодження та зміцнення зв'язків між злочинними угрупованнями, що дає змогу забезпечити оперативний обмін інформацією щодо об'єктів шахрайського посягання шляхом надання у користування бот-мереж, здійснення обміну прийомами та способами вчинення злочинів, способами переведення електронних коштів у готівку тощо [217, с. 93].

Наведемо приклад. Так, ОСОБА 1 перебуваючи з лютого 2016 році в СІЗО, познайомився там з ОСОБОЮ 3 та ОСОБОЮ 2, які також раніше були судимі за майнові злочини та відповідно з липня 2016 та квітня 2015 перебували в СІЗО. Для реалізації своїх злочинних намірів ОСОБА 1 розробив злочинний план, який полягав у заволодінні майном громадян шляхом шахрайства, для чого вирішив створити стійку злочинну організовану групу. До складу вказаної групи, на початку вересня 2016 року, як співучасників залучив на добровільних засадах своїх нових знайомих ОСОБУ 2 та ОСОБУ 3, яким довів розроблений єдиний план злочинної діяльності щодо вчинення шахрайств, розподіливши при цьому їх функції, спрямовані на досягнення цього плану, шляхи прикриття своєї злочинної діяльності, отримання та розподілу незаконних матеріальних благ між членами організованої групи. Розуміючи, що перебуваючи в СІЗО ОСОБА 1, ОСОБА 2 та ОСОБА 3, не зможуть в повній мірі реалізувати свої злочинні наміри у зв`язку з чим, як співвиконавців, в вересні 2016 року, залучили до

складу групи ОСОБУ 4 та в подальшому, з жовтня 2016 року, ОСОБА_6, які перебували на волі. Згідно розробленого плану, ОСОБА 1 взяв на себе роль організатора та виконавця злочинів ОСОБА 2, ОСОБА 3, ОСОБА 4 та ОСОБА_6 виступили співвиконавцями вчинення злочинів. Дані особи підтримували між собою відносини та перебували у дружніх і близьких стосунках, а саме ОСОБА 1, ОСОБА 3 та ОСОБА 2 на час вчинення злочинів перебували в СІЗО м. Хмельницького. Також, ОСОБА 3 тривалий час перебував в дружніх стосунках із ОСОБОЮ 4, з яким раніше разом відбував покарання і який перебуваючи на волі через спільних знайомих познайомився із ОСОБА_6. Стійкість організованої групи виражалася в стабільних, міцних внутрішніх зв`язках між її учасниками, існуванні певних правил поведінки, спільної мети, яка базувалася на бажанні кожного з них отримувати стабільні незаконні прибутки для задоволення власних потреб у виді грошових коштів, а також в обізнаності кожного учасника організованої групи у плані вчинення злочинів, розробленого ОСОБОЮ 1 і узгодженого з іншими учасниками організованої групи, який полягав у поетапному його виконанні. Таким чином, підготувавши знаряддя і засоби для полегшення вчинення злочинів, учасники групи з вересня 2016 року зорганізувались для спільної злочинної діяльності у стійку злочинну групу і згідно розподілених між собою ролей вчиняли заволодіння майном громадян шляхом шахрайства [183].

Щодо професійної зайнятості, слід сказати, що вчені наводять перелік різних осіб, які можуть мати причетність до шахрайства у сфері е-комерції. Так, С. В. Чучко вважає, що суб’єктом шахрайства може стати будь-який суб’єкт інформаційних правовідносин, який є носієм інформаційних обов’язків та прав [214]. На думку Т. А. Костецької, потенційно учасниками інформаційних правовідносин можуть стати юридичні й фізичні особи, але тільки ті, які наділені правосуб’єктністю [87, с. 69]. Розширює цей перелік А. В. Рейнгольд і серед осіб, які можуть мати відношення до шахрайства в онлайн просторі називає таких: фізичних осіб, які пропонують товар, у тому числі не існуючий; юридичних осіб, дані про яких розміщені в Єдиному

державному реєстрі юридичних осіб; банківських працівників; операторів в системі мережі Інтернет та інших суб'єктів, що надають різноманітні види послуг; покупців [160].

Щодо представників банківських установ, то до цієї широкої групи можна включити представників державних та недержавних банківських закладів. Структура даної групи правопорушників включає у себе: 1) керівники банківських установ чи філій та їх заступники; 2) керівники структурних відділів банківської установи (кредитних та кредитно-фінансових відділів, валютних операцій, інноваційного розвитку тощо) та головні бухгалтери банків; 3) інші працівники банку: кредитні інспектори, економісти, операціоністи, касири, фахівці з інформаційно-програмного забезпечення тощо [126, с. 38].

Відповідно до результатів закордонних та вітчизняних досліджень, на першому місці серед кібер-злочинців, які вчиняють шахрайства в е-комерції – колишні банківські співробітники та технічні фахівці. Спокуса продати наявні в розпорядженні дані за великі гроші виявляється занадто великою. Тому користуючись сервісом, що зберігає платіжні дані користувачів, навряд чи можна бути на 100% спокійним за їхню схоронність: або хакери зацікавляться, або звільнений адмінпродасть [165, с. 218].

Особливу небезпеку представляють випадки входження у змову з керівниками підрозділів і служб самої комерційної структури або пов'язаних з нею систем [126, с. 38]. Втім, деякі вважають, що до вчинення шахрайства здебільшого мають відношення й провайдери. Однак слід зазначити, що дії інформаційних провайдерів з надання послуг мають наступні особливості: провайдер не виступає ініціатором інформаційних відносин; не обирає зміст інформації, що передається, та її отримувача; не впливає на зміст інформації і зберігає її лише в часових рамках, що визначені відповідними технічними стандартами і протоколами. Відповідальність провайдерів базується на тому, що вони мають організаційно-технічну можливість в будь-який проміжок часу впливати на інформаційні суспільні відносини своїх користувачів.

Форма такого впливу може бути доволі різноманітною: від блокування інформаційного обміну до інформування третіх осіб про зміст такого обміну. Як повідомляє Н. Краморенко, існує три альтернативні підходи до визначення відповідальності провайдера: провайдер несе відповідальність за всі дії користувачів, незалежно від наявності у нього, як в суб'єкта права, інформації щодо цих дій; провайдер не несе відповідальності за дії користувачів, якщо дотримується визначених умов, пов'язаних з характером надання послуг і взаємодією з суб'єктами інформаційного обміну та особами, чиї права порушуються внаслідок дій користувачів; провайдер не відповідає за дії користувачів [89, с. 79].

Втім, слід визнати, що шахрайство здійснюється нерідко й сторонніми особами шляхом використання фальшивих ідентифікаційних документів, без відома особи, чия особа використовується для здійснення шахрайства. Сюди ж відноситься шахрайська діяльність, пов'язана з незаконним отриманням конфіденційних даних клієнтів банків, ПІН-кодів та CVV2-кодів банківських карток, логінів та паролів від інтернет-банкінгу, заволодіння мобільними фінансовими номерами клієнтів, за якими здійснюється аутентифікація, тощо [188, с. 68].

Цікавою є думка О. В. Кузьменко, який, не здійснюючи прив'язку до професійної зайнятості, до осіб, які вчиняють кібершахрайства, відносить: 1) осіб, які займаються поширенням вірусів, несанкціонованим використанням комп'ютерів, відповідних систем та мереж тощо; 2) спеціально підготовлених осіб, які займаються комп'ютерним шпіонажем з метою отримання важливих стратегічних даних в економічній, політичній, технічній та інших сферах; 3) професійних комп'ютерних злочинців, які вчиняють певні дії з корисливою метою [98, с. 165]. У цьому розрізі слід звернути увагу, що значного поширення з розвитком глобалізації інформатизації суспільства набуває таке соціальне явище, як хакерський рух – формування неформальних корпорацій осіб, одержимих знаннями до комп'ютерних технологій. Зафіксовані непоодинокі випадки коли організовані

злочинні формування використовують учасників цього руху для вчинення комп'ютерних злочинів. Українські хакери тісно контактують зі своїми «колегами» з інших країн, співпрацюють з ними, обмінюються досвідом, широко використовуючи для цього канали глобальних телекомунікаційних мереж (Інтернет) [201].

З цього виходить, що особа, яка вчиняє шахрайства у сфері е-комерції, є інтелектуально розвинутою особистістю із високим освітнім рівнем, із прагненням до наживи та здатністю інтерпретувати реальність за допомогою методів маніпуляції людською свідомістю, виявляє кмітливість і винахідливість у різних галузях, у тому числі у сфері використання комп’ютерних технологій, орієнтується у питаннях щодо здійснення електронних комерційних операцій, є здатною до адекватної поведінки в нових, заздалегідь не передбачених ситуаціях, легко робить висновки з наявних фактів.

Висновки до розділу 1

1. Рівень комерційних угод у дистанційному форматі дедалі збільшується. Популярність комерційної діяльності у віртуальному просторі створила підґрунтя для шахраїв, які діють навіть на транснаціональному рівні. Не дивлячись на прибутковість електронних комерційних угод, існує ряд загроз та невирішених проблем, пов’язаних із колізіями в законодавстві, що регулює електронний бізнес, недостатнім контролем з боку державних органів за діяльністю підприємців, які здійснюють комерційні операції в електронному режимі, порушенням конфіденційності персональних даних, незахищеністю електронних баз та інформаційних ресурсів тощо. Середовище е-комерції значно прискорилося й через пандемію COVID-19 та війну в Україні.

2. Спосіб вчинення шахрайства у сфері е-комерції має повноструктурний характер і включає дії із підготовки, безпосереднього вчинення та приховування протиправних дій. Дії з підготовки до вчинення шахрайства даної категорії включають: обрання напряму комерційної діяльності, де планується вчинити шахрайські дії; знаходження співучасників та обрання схем шахрайських дій; визначення часу, місця та способу вчинення шахрайства; підготовка необхідного пакету документів із метою реєстрації суб'єкта комерційної діяльності або підробка документів шляхом внесення до них недостовірних даних; створення фіктивних віртуальних клубів, фірм із надання різноманітних послуг, інтернет-магазинів тощо; створення фіктивних сайтів, аккаунтів; відкриття банківського рахунку і внесення на нього грошових коштів; створення «фіктивної» електронної адреси для здійснення переписки із клієнтами комерційних угод;придбання низки сім карток для здійснення переговорів із клієнтами, з метою подальшої зміни телефонних номерів;підбір категорій товарів для продажу, створення їх характеристик та наповнення інтернет-магазину інформацією про ці товари; обрання способу здійснення розрахунків та способу доставки; створення рекламних роликів, портфоліо із демонстрацією успішності комерційних проектів; розміщення інформації на сайтах, у ЗМІ про можливості комерційних угод; забезпечення сприятливих умов для вчинення шахрайства (для переконання потенційної жертви у сумлінності дій); підготовка засобів учинення шахрайства (комп'ютерна техніка, антураж приміщення комерційного об'єкта, фіктивні документи, різноманітні предмети для пред'явлення тощо); налагодження корупційних зв'язків із органами державної влади, суб'єктами, що мають відношення до супроводження комерційної діяльності в онлайн-просторі; продумування способів приховування шахрайських дій тощо.

Розкрито й систематизовано типові способи вчинення шахрайства у сфері е-комерції, приділено увагу способам їх приховування, зокрема: знищення інформації, що міститься на електронних носіях (79 %),

використання разових номерів мобільних телефонів (81 %), уникнення зорового контакті із потерпілим (81 %), внесення неправдивої інформації в електронні бази даних (27 %), фальсифікація доказів (78 %) тощо.

3. Найбільш спірним елементом криміналістичної характеристики є обстановка вчинення шахрайства даної категорії, адже внаслідок здійснення електронних комерційних операцій виникає віртуальне середовище, в якому будь-які дії з інформацією вчиняються за допомогою цифрових сигналів і можуть виходити за рамки однієї держави, що ускладнює визначення просторово-часових характеристик.

Виокремлено віртуальні (електронні, цифрові) сліди, характерні для шахрайства у сфері е-комерції. Натомість, наголошено, що матеріальні та ідеальні сліди також відіграють важливу роль при виявленні шахрайства даної категорії. Здебільшого інформацію про зовнішність шахрая потерпілі можуть надати у випадку безпосередньої зустрічі до, або після здійснення комерційної електронної угоди, або якщо спілкування здійснювалося у форматі відеоконференції. Матеріальні сліди можуть міститися у роздрукованих документах, скриншотах переписки, квитанціях тощо, а також можуть залишатися на комп’ютерній техніці, на магнітних носіях і оптичних дисках тощо.

Особливу увагу приділено предмету шахрайського посягання у сфері е-комерції, з урахуванням умов воєнного стану.

4. Фізичні особи виступають потерпілими при здійсненні роздрібної купівлі-продажу товарів або послуг на онлайн-платформах, на інтернет-аукціонах, під час здійснення інтернет-банкінгу тощо. Юридичні особи стають потерпілими внаслідок здійснення господарських операцій між юридичними та фізичними особами; при здійсненні матеріально-технічного постачання з використанням засобів електронної комерції у виробничому циклі підприємства; при наданні логістичних послуг; при здійсненні брендингу та просування торгової марки компанії; при забезпеченні

фінансовими установами трансакцій між суб’єктами; при наданні іншим підприємцям власно-створеного онлайн-майданчику для створення магазинів і торгівлі своїм товаром (маркетплейси) та ін.

5. Здійснено опис характеристики осіб, які вчиняють шахрайства у сфері е-комерції. Щодо вікових особливостей, то переважна більшість зазначених шахрайств вчиняються у віці від 16 до 50 років, що пояснюється активністю використання цифрових технологій саме особами даної вікової категорії та адаптацією до процесів діджиталізації. Більшість шахраїв чоловічої статі (68%), 62% з них мали вищу освіту, 56 % з них одружені (заміжні). Наголошено на наявності у таких осіб спеціальних знань і навичок з використання інформаційних технологій та здійснення електронних комерційних операцій. Акцентовано на великому відсотку вчинення шахрайств у сфері е-комерції у складі організованої групи.

РОЗДІЛ 2
ОРГАНІЗАЦІЙНО-ТАКТИЧНЕ ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВ У СФЕРІ Е-КОМЕРЦІЇ

2.1. Криміналістичний аналіз первісної інформації та організація розслідування шахрайства

Весь процес розслідування є організаційною діяльністю, що полягає у постійному аналізі, синтезі та узагальненні інформації, та виокремленні серед її потоку тієї, що є важливою у провадженні [137, с. 194].

У практичному розумінні організація розслідування передбачає переважно роботу з наявною інформацією, її опрацювання та оцінку. В результаті цієї діяльності відбувається висунення версій та визначаються завдання досудового розслідування: ухвалюються відповідні рішення, забезпечується їх виконання. Надалі цей процес триватиме шляхом уточнення завдань та ухвалення нових рішень із урахуванням отриманих даних та результатів завдяки чому слідчий має можливість прогнозувати процес розслідування в цілому [189, с. 156].

Організація розслідування кримінальних правопорушень перетинається із забезпеченням в одній зі своїх частин – створення сприятливих умов розслідування, що по суті є забезпеченням. З одного боку, саме криміналістичне забезпечення як специфічна діяльність потребує організації, з іншого – організація розслідування кримінальних правопорушень представляє собою й інший, окрім забезпечення, вид діяльності, що пов’язаний ще з упорядкуванням елементів розслідування [123, с. 9]. Втім, до предмету організації можна віднести закономірності щодо упорядкування елементів розслідування, створення сприятливих для нього умов,застосування найбільш ефективних шляхів і способів реалізації поставлених завдань розслідування,забезпечення узгодженості та

упорядкованості дій органів й осіб при вирішенні цих завдань тощо [136, с. 53].

Отже, для правильної організації розслідування уповноважена особа повинна правильно визначити тактичні завдання та обрати шляхи їх реалізації [71].

Досить розширений перелік заходів, що відносяться до організації розслідування, надає В. Ю. Шепітько. Зокрема, він до них відносить: розроблення плану заходів місцевих органів кримінальної юстиції; взаємодія в процесі досудового розслідування (між слідчим, оперативними працівниками, спеціалістами, експертами); чіткий розподіл обов'язків між учасниками розслідування; кваліфіковане керівництво слідчо-оперативною групою або бригадою; наради слідчої групи; обмін інформацією та звітністю про результати роботи слідчої групи й кожного слідчого; необхідні умови праці; розроблення й виконання плану розслідування та інші організаційні заходи з успішного розкриття й розслідування злочину [225, с. 99].

Слід зазначити, що організація розслідування шахрайства у сфері е-комерції може починатися ще з моменту надходження до правоохоронних органів інформації про зазначене кримінальне правопорушення.

Так, згідно ст. 214 КПК України, слідчий зобов'язаний внести відповідні відомості до ЄРДР, розпочати розслідування та через 24 години з моменту внесення таких відомостей надати заявнику витяг з ЄРДР у разі:

1) надходження заяви про обставини, що можуть свідчити про вчинення кримінального правопорушення;

б) надходження повідомлення про обставини, що можуть свідчити про вчинення кримінального правопорушення;

в) самостійного виявлення слідчим чи прокурором з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення [96].

У юридичній літературі дані джерела називають приводами для початку кримінального провадження [79, с. 34].

Не дивлячись на те, що у чинному кримінальному процесуальному законодавстві ані приводи, ані підстави прямо не вказані, це все одно стає підґрунтям для ряду дискусій у цьому напряму. Ряд науковців вважає, що формально вони залишилися і навіть акцентують увагу на численних спробах виділити ознаки приводу, серед яких наступні:

- він повинен бути актом вольової дії особи, що містить дані про ознаки злочину, адресованим уповноваженим суб'єктам кримінального провадження, чи вольовим актом уповноваженого суб'єкту, спрямованим на виявлення ознак злочину в ході реалізації ним своїх функцій;

- передбачатися кримінально-процесуальним законом;

- містити достатні дані, що вказують на ознаки злочину чи містити обставини, що можуть свідчити про вчинення кримінального правопорушення (за КПК України 2012 року);

- мати визначену законом процесуальну форму (якщо вона встановлена);

- являти юридичний факт, що породжує кримінально-процесуальні правовідносини;

- бути початком кримінально-процесуальної діяльності [148, с. 96; 30; 135, с. 31].

Ґрунтуючись на таких критеріях, В. Г. Дрозд надає більш розширений перелік приводів, аніж вказаний в кримінальному-процесуальному кодексі, зокрема: на її думку, приводами до початку кримінального провадження є:

- заяви про вчинене кримінальне правопорушення, які можуть бути усними або письмовими (заяви можуть надійти від фізичних чи юридичних осіб);

- повідомлення про вчинене кримінальне правопорушення, якими можуть бути: а) повідомлення підприємств, установ, організацій і посадових осіб; б) повідомлення представників влади, громадськості або окремих громадян, які затримали підозрювану особу, відповідно до ч. 2 ст. 207 КПК України; в) повідомлення в засобах масової інформації;

- самостійне виявлення слідчим із будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, у тому числі під час досудового розслідування;

- самостійне виявлення прокурором із будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зокрема за результатами перевірки в порядку нагляду, у тому числі під час здійснення нагляду за додержанням і застосуванням законів;

- самостійно виявлені посадовою особою правоохоронних і контролюючих державних органів факти вчинення чи підготовки до вчинення кримінальних правопорушень [39, с. 271].

Слід зауважити, що більшість вчених саме з наявністю підстав пов’язують момент початку розслідування. Зокрема, підстави до початку досудового розслідування законодавець визначив як «обставини, що можуть свідчити про вчинення кримінального правопорушення». До того ж, Н. В. Глинська, Л. М. Лобойко і О. І. Марочкін наголошують, що підстави до початку розслідування хоч до внесення до ЄРДР, хоч після цього мають бути. Підходи до визначення їх наявності й у тому і в іншому випадку є однаковими. Оскільки встановлювати підстави до початку досудового розслідування за допомогою матеріальних засобів пізнання заборонено законом, то ці підстави варто «шукати» виняткова у первинних відомостях про діяння, а не про «кримінальне правопорушення» [25, с. 130].

У цьому аспекті актуально було б говорити про те, що одні й ті самі ознаки бувають властиві як злочинному, так і незлочинному діянню. Так, одні й ті самі дані про протиправне діяння можуть мати різну кримінально-правову кваліфікацію. Наприклад, незаконні дії з використання платіжних карток, інших засобів доступу до банківських рахунків та електронних грошей можуть виникнути внаслідок викрадення картки, отримання її за допомогою підроблених документів, використання підробленої платіжної картки за допомогою певних комп’ютерних технологій, зловживання повноваженнями відповідальних працівників

кредитнофінансових установ, втручання в роботу систем або цілої комп'ютерної мережі тощо. Таким чином, як вірно наголошують В. І. Завидняк та Н. Л. Пушина, зробити навіть припущення про те, що мало місце кримінальне правопорушення з використанням комп'ютерних технологій, на основі однієї будь-якої ознаки особі, яка вносить відомості до ЄРДР, досить проблематично. Тому навіть для попередньої кваліфікації кримінального правопорушення в процесі внесення відомостей до ЄРДР необхідна наявність низки ознак, які будуть свідчити про можливе вчинення злочинного діяння. Така ситуація як раз вказує на те, що саме на початковому етапі досудового розслідування на слідчого покладається доволі складна й кропітка організаційна робота з виявлення та перевірки необхідної сукупності ознак вчинення конкретного кримінального правопорушення [50, с. 199].

Як показало опитування практичних працівників, які розслідували шахрайства у сфері е-комерції, суть проблеми в тому, що до 2023 року здебільшого органи досудового розслідування, процесуальні керівники та суди кваліфікують усі онлайн-шахрайства за ст. 190 ч.3 КК України, як вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. При цьому в якості основної ознаки для подібної правової кваліфікації навіть для найпростішої схеми шахрайства «не постачання замовленого онлайн товару» є місце розміщення оголошення про «продаж» – всесвітня мережа Інтернет (онлайн-магазини, інтернет-аукціони, соціальні мережі тощо).

Вбачається, що для розмежування звичайного шахрайства (ч.1 ст. 190 КК України) від кваліфікованого (ч.3 ст. 190 КК України) вже на первинному етапі, під час розгляду заяви потерпілого (іншого повідомлення), слідчий (дізнавач), встановивши наявність ознак кримінального правопорушення, задля вірної правової кваліфікації діяння має детально дослідити обставини скоєного шахрайства та порядок дій, як шахрая, так і потерпілої особи. Надзвичайно важливу роль в цьому процесі відіграє якісне опитування

потерпілого та витребування в нього з подальшим дослідженням наявних у потерпілого документів (листування в месенджерах або електронній пошті зі зловмисниками, виписки руху коштів з особистого банківського рахунку потерпілого, надані операторами зв'язку роздруківки вхідних та вихідних телефонних дзвінків потерпілого тощо).

На жаль, практичні працівники наголошують на тому, що на цей час серед правників відсутній єдиний підхід в правовій кваліфікації онлайн-шахрайств, стала судова практика також не сформована. Крім того, зважаючи на виключний правовий характер цієї проблеми та не однакове застосування судами норм матеріального права під час розгляду справ зазначеної категорії, потрібно узагальнити судову практику та сформувати єдину правову позицію. Якщо раніше правники дотримувались постанов Пленуму Верховного суду України, на сьогодні єдина позиція судових органів може полягати у висновках Великої Палати Верховного Суду, куди справа, що перебуває на касаційному розгляді, може бути направлена за ініціативою колегії суддів або за клопотанням сторін.

В контексті даної проблематики О. А. Самойленко визначила джерела, які дають змогу отримати офіційні відомості, що підтверджують або спростовують інформацію про факт вчинення протиправних дій у кіберпросторі:

1) державні органи (мають контрольні та ліцензійні функції та можуть надати копії документів про діяльність підприємств, установ та організацій, виявлені порушення процесів, що контролюється державою): – спеціально уповноважені державні органи в сфері телекомунікацій, зокрема орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язок) і підпорядковані їй регіональні органи (управління в областях)); – орган державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, що здійснює також повноваження органу ліцензування, дозвільного органу,

регуляторного органу та органу державного нагляду (контролю) (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ)); – Національна рада України з питань телебачення і радіомовлення; – Державне підприємство «Український державний центр радіочастот»; – Національний банк України;

2) громадські об'єднання/організації (можуть надати офіційні аналітичні огляди; статистичні дані, повідомити щодо виявлення факту вчинення злочинів), наприклад, Інтернет асоціація України, Всеукраїнська громадська організація «Всеукраїнське агентство з авторських та суміжних прав», Державна організація «Українське агентство з авторських та суміжних прав», Асоціація «Телекомунікаційна палата України» та інші;

3) суб'єкт господарювання (оператори та провайдери) у сфері зв'язку та телекомунікацій (може документально підтвердити реєстраційні і технічні відомості, що дають змогу ідентифікувати власника, розробника, адміністратора інтернет-ресурсу, факт надання послуг зв'язку конкретному користувачу/відправнику/отримувачу в конкретну дату та час, надання послуг хостингу, надати відомості про фінансово-господарську діяльність, технічні аспекти функціонування мережі тощо);

4) комерційні банківські установи, суб'єкти господарювання у сфері платіжних систем (можуть документально підтвердити рух (обіг) коштів на рахунках підприємств, установ і організацій, окремих громадян, поточні та депозитні рахунки, надати інформацію про штат співробітників та інше);

5) засоби масової інформації (можуть підтвердити документально факт реклами, оголошення, динаміку розвитку ринку товарів і послуг, проведення офіційних заходів (виступів, спортивних заходів, ярмарків і аукціонів); надати результати журналістських розслідувань);

6) міжнародні правоохоронні організації (можуть документально підтвердити місце розташування адміністратора та користувачів інтернет-ресурсу, що використовується підчас вчинення злочину на території

України, при цьому фізично розміщується на серверах, розташованих поза її межами) [170, с. 145-146].

Інформацію, отриману зі вказаних та інших джерел слід ретельно проаналізувати, після чого прийняти рішення про її прийняття або спростування.

Правильне сприйняття особою, яка проводить досудове розслідування, доказової інформації, її зіставлення з ознаками суспільно-небезпечного діяння, передбаченого кримінальним законом, є дуже важливим, оскільки може підтвердити чи заперечити наявність певного діяння та здійснити його юридичну оцінку [66, с. 10].

Слід сказати, що організація розслідування шахрайства у сфері е-комерції здебільшого залежить від того, яка саме слідча ситуація склалася на певному етапі розслідування. Як показали матеріали судово-слідчої практики, при розслідуванні шахрайства у сфері е-комерції можуть складатися такі ситуації: а) шахрайство мало місце, є інформація про шахрая, достатньо інформативна слідова картина; б) шахрайство мало місце, достатньо інформативна слідова картина, але відомостей про шахрая немає; в) факт вчинення шахрайства викликає сумнівів через можливість цивільно-правових відносин тощо.

Відповідно, із кожної ситуації витікає необхідність визначення відповідних тактичних завдань розслідування [76, с. 33].

Низка вчених серед тактичних завдань виділяють психологічні тактичні завдання розслідування, що пов’язані з необхідністю встановлення слідчим комунікативних зв’язків з учасниками кримінального процесу, а також з працівниками правоохоронних органів, з якими взаємодіє слідчий. Водночас, поряд із психологічними, існують й організаційні тактичні завдання розслідування, що полягають у створенні необхідних умов для успішного проведення запланованих слідчих дій та оперативно-розшукових заходів, забезпеченні їх необхідними засобами (транспортом, криміналістичною технікою, засобами зв’язку). Як правило ці завдання пов’язані з

налагодженням взаємодії слідчого з іншими підрозділами і службами правоохоронних органів, здійснення сумісного планування розслідування, розподіленням обов'язків та координації роботи [140; 155; 107].

Н. П. Бортник і М. М. Коваль вважають, що всі тактичні завдання можуть бути розділені на дві групи: а) завдання організаційно-управлінського характеру, що забезпечують відповідні умови для постановки і вирішення другої групи завдань; б) завдання розшукового і тактичного характеру, безпосередньо спрямовані на встановлення обставин розслідуваної події. До першої групи завдань вони відносять: 1) з'ясування і оцінка слідчої ситуації, що склалася на момент внесення до ЄРДР даних про злочин; 2) визначення джерел інформації про обставини події, що розслідується, їхній характер та місцезнаходження; 3) вибір форми і прийомів взаємодії з органами і службами, що ведуть оперативно-розшукову роботу; 4) визначення напряму розслідування і складання плану дій. До другої групи завдань, що постають на початковому етапі розслідування, належать: 1) отримання даних про спосіб, обстановку та інші обставини події, що дають можливість орієнтуватися в її змісті й характері; 2) збір та вивчення даних про потерпілого, що допомагає точніше з'ясувати мотиви і цілі злочинця, висунути версії про причетних до злочину осіб; 3) отримання й аналіз інформації про злочинця та його спільників [19, с. 301].

Втім, нам імпонує підхід В. В. Тіщенко, який пропонує розглядати завдання розслідування, прив'язуючись до етапів розслідування. Так, до завдань початкового етапу він відносить: 1) виявлення і фіксація доказової інформації про злочин, який розслідується за «гарячими слідами»; 2) вжиття заходів для запобігання втраті доказової інформації, що міститься в слідах, документах, інших об'єктах, її своєчасне виявлення та фіксація; 3) з'ясування й оцінка слідчої ситуації; 4) виявлення джерел інформації про розслідуваний злочин; 5) визначення напряму розслідування і розробка плану розслідування; 6) обрання форм і методів взаємодії з органами і службами, що здійснюють оперативно-розшукову роботу; 7) пошук і одержання

інформації про механізм і обстановку вчиненого злочину; 8) збирання і вивчення відомостей про особистість потерпілого; 9) пошук, одержання й аналіз інформації про осіб, що вчинили злочин, їхній розшук і затримання [195, с. 137; 155].

Як показав аналіз судово-слідчої практики та опитування респондентів у провадженнях щодо шахрайства у сфері е-комерції, основними тактичними завданнями, які слідчий повинен ставити перед собою, є: встановлення механізму вчинення шахрайства в е-комерції; з'ясування всіх обставин події, що розслідується; підтвердження факту шахрайського заволодіння майном чи правом на майно; встановлення точок доступу, з яких здійснювалися всі шахрайські дії; ідентифікація осіб, які здійснювали незаконні комерційні операції через електронні інформаційні системи та електронні комунікаційні мережі; встановлення всіх епізодів злочинної діяльності шахраїв; пошук свідків події; пошук документів, у тому числі електронних, щодо комерційної діяльності «суб'єктів господарювання»; обрання форм і методів взаємодії з органами і службами, що будуть задіяні під час проведення досудового розслідування шахрайства у сфері е-комерції; обрання форм використання спеціальних знань під час проведення досудового розслідування шахрайства у сфері е-комерції; визначення алгоритму розслідування, залежно від слідчої ситуації, і розробка плану розслідування; вжиття заходів для запобігання спробам протидії розслідуванню тощо.

Особливості взаємодії слідчих з іншими правоохоронними органами, а також установами, підприємствами та організаціями, громадськими формуваннями тощо належать до числа вагомих складників організації розслідування [78, с. 22].

Взаємодію правоохоронних органів та інших державних органів і посадових осіб у процесі розкриття та розслідування кримінальних правопорушень доцільно розглядати як узгоджену діяльність різних ланок однієї чи кількох організованих систем, спрямовану на досягнення загальної мети з найменшими втратами сил, засобів і часу [51, с. 209].

У свою чергу, ряд вчених вважає, що потреба в організації взаємодії обумовлена конкретними факторами, які розподіляються за такими групами, як інформаційні, тактичні та організаційні. Інформаційні фактори визначають ступінь поінформованості слідчого про обставини вчиненого злочину та його учасників, можливі докази, місця приховування шуканого, осіб, що протидіють слідчому. Тактичні фактори включають у себе докази і їх джерела, наявність надійних ще не використаних каналів орієнтуючої інформації, дані про плани, наміри і дії підозрюваних осіб чи інших учасників розслідування, про їх позицію, можливість обрання відповідних заходів забезпечення. Організаційні фактори – це комплекс сил, засобів, часу, що є у розпорядженні слідчого, та можливостей їх оптимального використання. З їх допомогою він впорядковує організаційну структуру своєї діяльності. При цьому, залежно від наявності та оцінки інформаційних і тактичних факторів, що виникли, слідчий може обрати такі види співпраці: 1) оптимальне компонування й послідовне проведення слідчих дій та оперативно-розшукових заходів; 2) найбільш доцільні напрями взаємодії з працівниками карного розшуку. А для того щоб слідчому знайти потрібний варіант взаємодії, необхідно: своєчасно визначити форму організаційно-управлінської структури взаємодії, оптимальної для конкретної слідчої ситуації; поставити чіткі та конкретні завдання перед всіма суб’єктами; правильно розподілити обов’язки відповідно до компетенції і функцій; узгодити планування, яке повинно визначати характер спільних і узгоджених дій, їх послідовність, зв’язок і строк проведення; організувати обмін інформацією [18, с. 135; 51, с. 210].

Як показав аналіз судово-слідчої практики та опитування практичних працівників, при розслідуванні шахрайства у сфері е-комерції, взаємодія слідчого здійснюється із: оперативними службами Департаменту кіберполіції (100 %); оперативними підрозділами Національної поліції України (100 %); підрозділами Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ (7 %); підрозділи Департаменту

спеціальних телекомунікаційних систем та захисту інформації СБУ (4 %); підрозділами у складі Департаменту оперативно-технічних заходів (92 %) та ін.

Слід визнати, що найпоширенішою є взаємодія із Департаментом кіберполіції Національної поліції України. Утворення СОГ за участю оперативних працівників Департаменту кіберполіції Національної поліції України, його структурних підрозділів, які діють за міжрегіональним принципом, для розслідування кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку здійснюється за спільним наказом керівників органу досудового розслідування та Департаменту кіберполіції Національної поліції України [34, с. 356].

Відповідно до Положення про Департамент кіберполіції Національної поліції України (далі – ДКП), затвердженого наказом Національної поліції України (далі – НПУ) від 07.11.2019 № 1136, основними завданнями кіберполіції визначено: попередження та протидію кримінальним правопорушенням, механізм підготовки, учинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. При цьому, пріоритетним напрямком роботи ДКП є боротьба з онлайн-шахрайствами.

Особливо дієвою є взаємодія слідчого із представниками кіберполіції при документуванні діяльності так званих «Call-center», які дедалі частіше, використовуючи методи соціальної інженерії та маніпулятивні техніки, пропонують громадянам інвестувати кошти в псевдокомерційні проекти. Незаконні «Call-center» все частіше відкриваються у великих містах, маскуючи свою діяльність під інтернет-магазини, центри обслуговування клієнтів, гарячі лінії тощо.

Шахраями забезпечується функціонування «кол-центрів» зазначених вище інтернет-магазинів, за допомогою яких здійснювався зворотній зв'язок із замовниками товарів в фіктивних Інтернет - магазинах. Договори про

надання послуг Інтернет зв'язку та телефонії, також оформлюються на підставних осіб.

Наведемо приклад документування працівниками кіберполіції діяльності одного із «Call-center». Так, особи, які виконували функції операторів, приймали та вели облік замовлень, висилали клієнтам реквізити для сплати, заносили телефони ошуканих клієнтів до «чорного списку», щоб вони не заважали роботі «Call-center» та якнайдовше не здогадувались, що відносно них було скоєно шахрайство. Оператори «Call-center» за допомогою послуг інтернет-телефонії, знаходячись за місцем мешкання на території України, зв'язувались та спілкувались з замовниками фіктивних інтернет–магазинів, створюючи враження реального «Call-center», приймали замовлення на неіснуючий товар, а саме електронну побутову техніку, мобільні телефони та аксесуари до них, тощо. Заволодіння грошовими коштами громадян відбувалося шляхом їх зняття підконтрольними організатору схеми особами та безпосередньо самим організатором, з банкоматів розташованих у м. Києві. З метою приховування злочинної діяльності, організатор та учасники шахрайської схеми створили систему конспіративних заходів, спрямованих на забезпечення безпеки осіб, які приймали участь у вчиненні шахрайства, та попередження виявлення і запобігання загрозам викриття з боку правоохоронних органів. Зокрема, передбачали заборону користуватись телефонними терміналами та абонентськими номерами, спілкування та обмін інформацією, координування дій учасників злочинної групи здійснювався в основному через мобільне обладнання, що підключене до 3G-Інтернету. На мобільних пристроях та ноутбуках злочинців було встановлено програму призначену для інтернет-листування, в якій створювались зашифровані чати, з автовидаленням повідомлень після їх перегляду, усі учасники шахрайських дій використовують програми для приховування та зміни реальної IP-адреси. Внаслідок документування злочинної діяльності оперативними працівниками поліції у взаємодії із представниками Департаменту кібезполіції, за місцем

фактичного місця проживання організатора шахрайської схеми вилучено готівкові кошти у сумі майже 19 тис. доларів США, 8 банківських карток різних банківських установ, 4 ноутбуки, планшет, 8 мобільних телефонних апаратів, близько 50 сім-карток різних мобільних операторів, скретч-карти від використаних сім-карт, 2 мобільні інтернет-модеми, договори на отримання телекомунікаційних послуг, чорнові записи, предмети одягу, які використовувалися шахраями під час вчинення злочинів тощо [209].

Кіберполіція встановила, що зловмисники телефонували громадянам сусідньої країни та випитували в них конфіденційну інформацію, зокрема CVV-коди, номери та пін-коди банківських карт. Далі, використовуючи ці дані, фігуранти виводили гроші з карток потерпілих на підконтрольні рахунки [68].

В основному взаємодія між слідчим та вказаними органами здійснюється у формі виконання доручень на проведення слідчих (розшукових), а також негласних слідчих (розшукових) дій. Втім, не менш поширеною є взаємодія при проведенні інших процесуальних заходів: затриманні, здійсненні приводу, застосуванні інших заходів забезпечення кримінального провадження.

Серед не процесуальних форм організації взаємодії у провадженнях щодо шахрайства у сфері е-комерції найпоширенішими є: спільна участь у складі слідчо-оперативної групи (97 %), обмін інформацією (98 %), спільне обговорення матеріалів слідчими й співробітниками оперативних підрозділів (96 %), використання слідчими можливостей ЗМІ (81 %), спільне планування слідчих (розшукових) дій та розшукових заходів (81 %), консультаційна допомога різноманітних спеціалістів (88 %).

Окрім оперативних підрозділів, слідчий під час розслідування шахрайства у сфері е-комерції організовує взаємодію із постачальниками електронних комунікаційних послуг, операторами послуг платіжної інфраструктури, адміністраторами, що присвоюють мережеві ідентифікатори, та іншими суб'єктами, що забезпечують передачу та зберігання інформації з

використанням інформаційно-комунікаційних систем, а також банківськими представництвами [162, с. 212]. До того ж, для якісного проведення розслідування кримінальних правопорушень, вчинених із використанням комп'ютерних технологій, слід робити акцент також на взаємодії органів досудового розслідування з представниками служб безпеки банків або інших кредитно-фінансових установ. Основні напрями, за якими необхідно будувати взаємодію між правоохоронними органами і службами безпеки банків щодо кримінальних правопорушень цієї категорії (пов'язаних із незаконними операціями з використанням платіжних карток та інших засобів доступу до банківських рахунків, електронних грошей, обладнання для їх виготовлення; незаконні операції, пов'язані з неправомірним доступом до комп'ютерної мережі; підроблення документів, які подаються для проведення реєстраційних дій) належать: своєчасне виявлення таких кримінальних правопорушень; швидке та ефективне реагування на виявлені факти злочинних посягань; швидке і безперешкодне отримання необхідної інформації в міжнародних платіжних системах; взаємні консультації відповідно до повноважень; допомога у збиранні доказів за фактами вчинення кримінальних правопорушень цієї категорії; аналітична робота, створення методологічної бази, навчання, законодавчі ініціативи; здійснення загальних профілактичних заходів [50, с. 200].

Взаємодія із комерційними представництвами, які здійснюють торгівельно-комерційні операції через електронні системи та комп'ютерні мережі також може стати в нагоді.

2.2. Організаційно-тактичні особливості проведення окремих процесуальних дій

Як свідчить практика, найбільш трудомісткою слідчою (розшуковою) дією, спрямованою на вилучення інформації з матеріальних об'єктів, є

обшук. Натомість, при розслідуванні шахрайства у сфері е-комерції, з метою вилучення певних об'єктів, застосовуються й інші процесуальні дії.

Так, згідно ч. 2 ст. 168 КПК України, тимчасове вилучення майна може здійснюватися під час обшуку, огляду. Крім того, надати стороні кримінального провадження особою, у володінні якої знаходяться речі і документи, що мають значення для провадження, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку) вимагає положення статті 159 КПК України (Тимчасовий доступ до речей та документів). Вилучення речей і документів, які мають значення для кримінального провадження, та речей, вилучених з обігу, дозволяється й під час проведення огляду (стаття 237 КПК України) [96].

Спосіб вилучення здебільшого обирається, виходячи із тактичних міркувань та тяжкості кримінального правопорушення [73, с. 419].

Втім, одним із необхідних засобів доказування на початковому етапі досудового розслідування ряду кримінальних правопорушень є організація і проведення обшуку, метою якого є виявлення й вилучення предметів і документів, які мають значення для встановлення істини в провадженні. Обшук – одна з проблематичних слідчих (розшукових) дій, що, очевидно, пов'язано з дотриманням конституційних прав особи, складною процесуальною процедурою прийняття рішення про проведення обшуку та необхідністю врахування певних факторів, які впливають на його результативність. Головна відмінність обшуку від інших слідчих (розшукових) дій полягає у його примусовому й пошуковому характері [215, с. 72].

З цього приводу ряд вчених звертає увагу, що прогресивним кроком стало чітке визначення у статті 87 КПК України підстав недопустимості фактичних даних як доказів. Так, недопустимими є докази, отримані внаслідок істотного порушення прав і свобод людини, гарантованих Конституцією та законами України, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також будь-які інші

докази, здобуті завдяки інформації, отриманій внаслідок істотного порушення прав і свобод людини. З чого виходить, що у результаті злочинного нехтування нормами, які визначають умови і порядок збирання та перевірки доказів та їхніх джерел, всі здобуті фактичні дані вважаються недопустимими. Тому, під час проведення слідчих (розшукових) дій, які є основним засобом збирання доказів, слід дотримуватися як кримінальних процесуальних, так і конституційних вимог та не ставати на заваді реалізації прав усіх учасників кримінального судочинства, окрім випадків, визначених законом. Натомість проведення слідчих (розшукових) дій часто супроводжується обмеженням прав людини, що передбачає примусовий вплив, який застосовують до учасників слідчих (розшукових) дій уповноважені органи й особи з метою забезпечення процесуального порядку, здійснення кримінально-процесуального доказування [130, с. 279; 222, с. 26; 100, с. 101].

Тому, готуючись до обшуку, слід з’ясувати всі обставини справи та ретельно спланувати проведення обшуку, виявити підстави для правомірного втручання в особисте життя особи та підстави для порушення недоторканості приватної власності тощо.

Значення обшуків у розслідуванні кримінальних правопорушень обумовлюється тим, що нерідко їх результати містять початкові відомості, які доводять причетність осіб до організованої злочинної діяльності і можуть бути основою висунення криміналістичних версій та планування розкриття злочинів. Крім того, усі виявлені під час обшуків матеріальні сліди порівнюються з інформацією, яка отримана після проведення слідчих оглядів. Тому виявлення зв’язків між предметами, які вилучені під час проведення обшуків, дозволяє пов’язати їх з конкретною особою (лідером або членом злочинної групи) та довести їх причетність до злочинної діяльності [206, с. 82].

Рішення на проведення обшуку необхідно приймати після виконання певних дій розумового й діяльнісного характеру (визначення об’єкта

тактичного впливу; системний аналіз слідчої ситуації та прогнозування поведінки учасників розслідування й фігурантів у справі; прогнозування перебігу обшуку, розроблення можливих варіантів ходу обшуку, з урахуванням непередбачених обставин тощо). При цьому, основною тактичною вимогою є необхідність використання фактору раптовості, запобігаючи при цьому витоку інформації. У зв'язку із тим, що члени злочинного угруповання можуть підтримувати корупційні зв'язки із правоохоронними органами, про проведення обшуку повинно знати обмежене коло осіб. Як свідчать матеріали судово-слідчої практики, нерідко після отримання ухвали слідчого судді про проведення обшуку на кількох об'єктах одночасно, ухвали були паковані в окремі конверти і роздавалися керівникам слідчо-оперативних груп безпосередньо перед виїздом на слідчі дії. Таке рішення є цілком аргументованим, оскільки до шахрайства можуть мати відношення службові особи, високопосадові, працівники правоохоронних органів, і витік інформації в таких умовах є неприпустимим [210; 48]. Обов'язково слід зібрати інформацію про власників та володільців приміщення, в якому проводитиметься обшук, з'ясувати правильність юридичної адреси об'єкту обшуку.

Як свідчить аналіз кримінальних проваджень та судової практики, у провадженнях щодо шахрайств, учинених у сфері е-комерції, нерідко об'єктами обшуку є приміщення підприємств, установ та організацій, а також комп'ютерні клуби, інтернет-кафе тощо [130].

Утім, доволі часто слідчі в ухвалі вказують юридичну адресу підприємства, організації, установи, що містить велику кількість об'єктів (офісів, кабінетів). Це призводить до того, що пошукові дії проводяться навіть у тих офісах, володільці та власники яких не мають відношення до вчинення шахрайських дій, що зумовлює скарги від таких осіб. Вирішенням цієї проблеми є вказування в ухвалі не тільки юридичної адреси, а й номерів, місця розташування офісів, які знаходяться та території проведення обшуку. Крім того, є ще одна проблема, яку слід враховувати вже при підготовці до

обшуку. Так, згідно з КПК України та ст. 23 Закону України «Про адвокатуру та адвокатську діяльність», обшук у володінні адвоката проводиться лише на підставі судової ухвали про дозвіл на обшук у адвоката за клопотанням Генерального прокурора, його заступників, прокурора області тощо. Це пов'язано із необхідністю збереження адвокатської таємниці. Цю вимогу законодавця шахраї швидко взяли на озброєння і стали оформлювати на адвоката, з яким укладено угоду про надання адвокатських послуг, оренду окремого приміщення в офісі, в якому зберігаються всі документи та комп'ютерна техніка, що містить в собі цінну інформацію. Звісно, прибувши із ухвалою про проведення обшуку на конкретну адресу, відразу втрачається можливість провести пошукові дії на об'єкті, що орендується адвокатом до отримання такого дозволу. Якщо слідчий, прокурор, отримавши таку інформацію, проігнорують законодавчі вимоги щодо особливого порядку проведення обшуку у приміщенні, що належить адвокату, результати такого обшуку можуть у майбутньому визнатися недопустимими, а права осіб порушені. Тому на етапі підготовки до обшуку слід прорахувати можливі варіанти володіння житлом чи іншим приміщенням адвокатом чи іншими особами, щодо яких передбачено особливі порядки кримінального провадження [130, с. 282].

Як показав проведений нами аналіз, розслідування шахрайства у сфері е-комерції, сполучається із трудомісткими заходами, пов'язаними із вилученням низки документів, предметів, які використовувалися для досягнення злочинного умислу, а також комп'ютерної техніки і електронних носіїв інформації.

Адже розвиток цифрових технологій зумовлює вилучення окрім традиційних об'єктів ще й інформаційних слідів, які утворюються внаслідок впливу на комп'ютерну інформацію (шляхом знищення, перекручення). Насамперед вони залишаються на магнітних носіях інформації і пов'язані зі змінами, які відбулися у самій інформації, порівняно з початковим її станом. Також до інформаційних слідів належать наслідки роботи антивірусних і

тестових програм, які можуть бути виявлені під час вивчення комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм та програмного забезпечення [141, с. 8].

Необхідність вилучення комп'ютерної техніки та її носіїв під час розслідування шахрайства у сфері е-комерції підвищує роль фахівця під час проведення процесуальних дій, спрямованих на отримання інформації з матеріальних об'єктів, у тому числі й обшуку.

Згідно ст. 236 КПК України, з метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в обшуку має право запросити спеціалістів. Виходячи з цього, злам можливих захисних систем повинен здійснюватися тільки висококваліфікованим спеціалістом в особливих умовах [54]. Не можна дозволяти нікому, окрім компетентного спеціаліста, доторкатись до техніки і пристроїв електроживлення. Виключені пристрої не варто вмикати. Всю підключену до комп'ютера периферію слід сфотографувати або описати в протоколі, щоб було зрозуміло, які були з'єднання. Також варто звернути увагу на місце, де знаходиться комп'ютерна техніка, поруч можуть бути записані паролі, мережеві адреси та інші дані, - часто такі записи лежать поруч, приклеєні до монітора, висять на стіні. Якщо принтер щось друкує, слід дочекатися закінчення друку. Усе, що знаходиться у вихідному лотку принтера, описується і вилучається на ряду з іншими носіями комп'ютерної інформації. Після цього комп'ютери треба вимкнути, це повинен зробити спеціаліст [230, с. 65].

Важливим напрямом під час безпосереднього проведення обшуку є ретельна перевірка записів, документації у комп'ютерній системі; вихідна та оперативна інформація про діяльність підприємства; особисті дані про співробітників; список структур, з якими організація співпрацювала чи співпрацює тощо. Більш вужче коло питань підлягатиме дослідженню, коли відомий підозрюваний і якого вже ідентифіковано. Тоді можна швидше зафіксувати виявлені та вилучені речові докази, які мають відношення до

справи та розглянути інший об’єм питань, що виник у ході проведення даного заходу [116, с. 176].

Як показав аналіз судово-слідчої практики, під час розслідування шахрайства у сфері е-комерції, об’єктами пошуку можуть бути:

- реєстраційні документи, що посвідчують законність діяльності суб’єкта комерційної діяльності;

- фотографії, відеозаписи, на яких міститься інформація, що має значення для справи (факт знайомства певних осіб між собою, факт перебування особи у певному місці тощо);

- документи, що відображають особливості комерційної діяльності осіб, які мають відношення до шахрайських дій;

- документи, які містять відомості про можливих покупців;

- електронні та паперові договори про комерційні угоди;

- документи, що посвідчують особу (їх копії, підроблені документи на ім’я інших осіб);

- сім картки;

- квитанції про проведення банківських операцій;

- мобільні телефони, де міститься адресна книга (прізвища й адреси покупців, дані про організатора злочину);

- записні книжки, рукописні тексти на папері, у журналах тощо;

– комп’ютерна техніка (ноутбуки, планшети, системні блоки), де може міститися інформація про протиправну діяльність шахрая;

- електронні носії інформації;

- документи, що підтверджують відкриття розрахункових рахунків у банківській установі;

- договори з іншими організаціями, підприємствами та приватними підприємцями, які беруть участь у комерційних операціях;

- печатки та штампи як справжні, так і підроблені, кліше підписів тощо.

З цього виходить, що об’єктами вилучення здебільшого є документи як в паперовій, так і в електронній формі, а також комп’ютерна техніка.

Отже, вбачається істотна роль магнітних, електронних носіїв інформації та копій електронних документів, включаючи обов’язкові реквізити документа. Для виявлення та огляду подібних слідів необхідно залучити спеціаліста з комп’ютерної техніки та програмного забезпечення. До того ж, ще одним важливим моментом, на який слід звернути увагу при проведенні обшуку, це наявність пристроїв відеозйомки (відеокамер), як в офісних, так і в житлових приміщеннях. У зв'язку з чим, в ході проведення обшуку необхідно досліджувати приміщення на наявність зазначених пристроїв, в разі виявлення яких, необхідно вилучати сервер, на який здійснюється відеозапис. Оскільки дії шахраїв можуть бути зафіксовані на будь-який носій інформації, що відіграватиме велику роль у доказуванні, всі зусилля слідчого повинні бути спрямовані на правильне вилучення таких носіїв [64, с. 188].

Слід зазначити, якщо є підстави вважати, що речі та документи будуть надані сторонами, у володінні яких вони знаходяться, у добровільному порядку, слід провести тимчасовий доступ до речей та документів:

- з банківських установ про власників банківських карток/рахунків, на які здійснювався переказ грошей потерпілих, місце зняття коштів та фото- і відеозаписи з камер, встановлених на банкоматах або у відділеннях банку. Якщо гроші перераховувались на інші рахунки, то також IP-адреси користування web-банкінгом;

- у операторів мобільного зв’язку щодо абонентських номерів мобільних телефонів та банківських установ (належність банківського рахунку, IP-адреси користування web-банкінгом, фото-відео зняття коштів у банкоматах, у відділеннях банку) тощо.

Як показав аналіз судово-слідчої практики, об’єктами вилучення під час тимчасового доступу до речей та документів, ще можуть бути:

- протокол за результатами проведення оперативно-технічного заходу;

- диски;

- акт огляду електронної сторінки мережі Інтернет тощо.

У випадку, якщо під час шахрайських дій фізичних розмов з шахраєм не було, а мало місце лише листування у месенджері, то скоріш за все використовувався віртуальний телефонний номер за технологією IP-телефонії, в таких випадках не потрібні мобільні термінали для фізичного розміщення сім-карти і вказана процесуальна дія не дасть очікуваного результату.

При тимчасовому доступі до речей та документів такі носії інформації можуть бути оглянуті, їх вміст може бути скопійовано, а у випадках, коли сторона кримінального провадження доведе наявність достатніх підстав, вони можуть бути вилучені. Такі підстави закріплені п. 7 ст. 163 КПК України, де, зокрема, йдеться про випадки, коли без вилучення об'єктів тимчасового доступу існує реальна загроза зміни або знищення таких речей чи документів, або таке вилучення необхідне для досягнення мети отримання доступу до речей і документів [80, с. 185].

У будь-якому випадку, об'єкти, що вилучаються у ході проведення обшуку, як і ті, до яких надається тимчасовий доступ особами, у володінні яких вони знаходилися, підлягають ретельному огляду.

Особливу увагу слід приділити огляду електронної інформації, що розміщена у відкритому доступі в мережі Інтернет, а також такої, що знаходиться на фізичних носіях інформації і у хмарних сервісах зберігання електронної інформації.

Така інформація в основному зберігається у вигляді веб-сторінок, які складаються з окремих електронних документів, що містять дані у вигляді тексту, графічних зображень, електронних таблиць, відео тощо і можуть бути переглянуті за допомогою спеціальних комп'ютерних програм – веб-переглядачів (браузерів): Internet Explorer, MozilaFirefox, GoogleChrome, Opera та ін. [169, с. 39].

Один із варіантів фіксації інформації, яка є в публічному доступі, здійснюється шляхом скріншоту (програмному фотографуванні зображення з екрану монітору), або створенням дублікату частини або цілого web-сайту за

допомогою спеціальних програм. При дублюванні даних, як містять ознаки порушення авторських та суміжних прав, шкідливий код (віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери тощо) – необхідно вказати web-адресу та зробити скріншот джерела розповсюдження, а також вказати контрольну суму файлу (значення, розраховане на основі набору даних з використанням певного алгоритму, що використовується для перевірки цілісності даних при їх передачі або збереженні) одним або декількома алгоритмами хешування: CRC32, MD5 та SHA-1 [36, с. 106].

У протоколі огляду електронного документа в обов'язковому порядку мають зазначатися технічні характеристики та серійні номери обладнання, назви та версії програмного забезпечення, що використовуються в ході даної слідчої (розшукової) дії. Також мають бути вивчені та відображені у протоколі усі реквізити електронного документа. Так, наприклад, при огляді електронного документа у відкритому доступі в Інтернеті, у протоколі огляду слід зазначити серійний номер службового комп'ютера, назву та версію операційної системи, якою керується даний комп'ютер, назву та версію програми-браузера, за допомогою якої здійснюється доступ до мережі Інтернет. Веб-сторінка має бути масштабована у браузері на повний розмір (100%). У браузері мають бути відключені усі додатки та надбудови, що можуть змінити вигляд веб-сторінки, яка оглядається. Основними реквізитами такого електронного документа можуть бути адреса у мережі Інтернет, на якій розміщено веб-сторінку; назва веб-сайту, категорія чи жанр публікації, якщо вони зазначені на веб-сторінці; назва публікації; основний текст публікації; прикріплені зображення та аудіо- чи відеофайли; відомості про автора публікації (якщо публікація не є анонімною). Крім того, у протоколі має бути перелічено та коротко описано фото-, відео та аудіофайли, прикріплені до публікації, із зазначенням посилання на кожний із таких файлів у мережі Інтернет [80, с. 187].

У разі отримання пароля від власника облікового запису у хмарному сховищі, інформація, що знаходиться у віртуальному форматі, копіюється з

сервера на флеш або диск, або роздруковується на папір, після чого підлягає огляду.

Натомість, якщо авторизаційні дані (логін та пароль) для доступу до аккаунта у хмарному сервісі отримати не вдалося, отримати тимчасовий доступ до електронних інформаційних систем компанії, що надає послуги хмарного зберігання інформації, можна в порядку ст. 159 КПК України, або в межах такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем у порядку ст. 264 КПК України [80, с. 189].

Оскільки при вчиненні шахрайства у сфері е-комерції шахраї використовують електронні системи (наприклад для здійснення переказу потерпілими грошових коштів через систему електронних платежів з використанням технічних приладів, створення сайтів – копій тощо), при розслідуванні такого виду кримінального правопорушення така НСРД є досить поширеною. При цьому, ідентифікаційними ознаками електронної інформаційної системи є: IP-адреса (IP − InternetProtocol), яка є унікальним ідентифікатором (адресою) пристрою (звичайно комп'ютера або маршрутизатора), підключеного до локальної мережі або Інтернету; доменне ім'я, що дозволяє ідентифікувати в мережі Інтернет веб-сайт або адресу електронної пошти; серійний номер та характеристики автоматизованої системи та ЕОМ [108].

Серед поширених негласних слідчих (розшукових) дій, що проводяться при розслідуванні шахрайства у сфері е-комерції, є зняття (вилучення) інформації з електронних комунікаційних мереж (49 %).

Необхідність зняття інформації з електронних комунікаційних мереж у провадженнях даної категорії може виникнути у випадках: підозрюваний може зв'язуватися із своїми спільниками, іншими особами; потерпілому передбачається надіслання повідомлення від злочинця або в роботу його комп'ютера можливе несанкціоноване втручання; з певною особою (родичі, знайомі, співучасники злочину) може зв'язатися підозрюваний, який

знаходиться у розшуку; відомі телефонний номер, електронна пошта чи інші параметри адресата, але особа, яка користується каналом зв'язку, не встановлена [229, с. 156].

Ця процесуальна дія полягає у проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою та має значення для досудового розслідування, а також одержанні, перетворенні та фіксації різних видів сигналів, що передаються каналами зв'язку. Як правило, зняття інформації з електронних комунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції й органів безпеки. Керівники та працівники операторів телекомунікаційного зв'язку зобов'язані сприяти виконанню дій зі зняття інформації з електронних комунікаційних мереж, вживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді [214].

Якщо при розслідуванні кримінального провадження є підстави вважати, що у кореспонденції особи містяться відомості про обставини, які мають значення для досудового розслідування, доцільно проводити таку НСРД, як накладення арешту на кореспонденцію, її огляд та виїмку. Відповідно до ч. 4 ст. 261 КПК України кореспонденцію, на яку можна накласти арешт, є листи усіх видів, бандеролі, посилки, поштові контейнери, перекази, телеграми, інші матеріальні носії передавання інформації між особами. Натомість, ряд науковців до кореспонденції, на яку може бути накладено арешт, крім зазначеної у частині 4 статті 261 КПК України, відносять також: електронні повідомлення (охоплює електронну пошту, SMS- та MMS-повідомлення); фіксовані голосові повідомлення; радіограми та повідомлення факсом, комерційні відправлення [24, с. 37-38; 52; 176, с. 83].

Серед слідчих (розшукових) дій, спрямованих на отримання інформації від особистісних джерел, найпоширенішим є допит.

При цьому, слід сказати,що специфіку допиту визначає предмет даної слідчої (розшукової) дії, що залежить не тільки від процесуального

становища допитуваного та інформації, якою він володіє, а й від способу вчинення шахрайства і характеру слідчої ситуації [136].

Зважаючи на специфічність кримінальних правопорушень, вчинених шляхом застосування комп'ютерних технологій, та наявність у шахрая професійних знань і навичок, з метою якісного проведення допиту необхідно досить серйозно поставитись до його планування. Так в загальному вигляді слідчий повинен для себе з'ясувати наступні аспекти: специфіку провадження, особливо питання, що стосуються технічних аспектів підготовки та реалізації злочинних намірів; визначити обставини, які потребують з'ясування або уточнення; підготувати доказові або інші матеріали для пред'явлення в процесі допиту; визначитись із часом та місцем проведення допиту, а також способом виклику допитуваного [166, с. 106].

Крім того, перед початком проведення допиту слідчому необхідно: отримати кваліфіковані консультації відповідних спеціалістів з даного напряму; в окремих випадках доцільно запросити спеціаліста для участі у слідчій (розшуковій) дії, який може роз'яснити слідчому показання, що містять відомості технічного характеру; ознайомитися зі спеціальною літературою, що стосується предмета допиту; приділити увагу пізнанням у сфері електронного документообігу, режиму конфіденційної інформації, засобів і методів її захисту та безпечної обробки; детально ознайомитися з результатами проведених слідчих (розшукових) дій (документами, предметами, протоколами тощо); визначитись із колом питань, що будуть ставитись допитуваному (питання доцільно розділити на блоки, наприклад, питання що стосуються підготовки до злочину, безпосереднього вчинення злочину та приховання його слідів); підготувати додаткові засоби фіксації допиту (диктофони, відеокамери, так як предмет допиту зазвичай складний і насичений великою кількістю технічних термінів) [166, с. 106].

На перший погляд, проведення допиту не становить особливих труднощів. Однак ця легкість лише удавана, оскільки допитувані далеко не завжди дають правдиві, повні й об'єктивні свідчення, тому досягти бажаного

результату вдається, використовуючи при цьому певний комплекс тактичних прийомів. Основне місце серед окреслених тактичних прийомів займає психологічний контакт. Його необхідно встановити з підозрюваним для успішного проведення допиту [46, с. 146].

Натомість, як показало опитування практичних працівників, які розслідували кримінальні провадження щодо шахрайства у сфері е-комерції, під час допиту вони найчастіше використовують такі тактичні прийоми, як: зміна темпів допиту (52 %), створення уявлення про недостатню поінформованість про подію шахрайства (41 %), створення уявлення про повну поінформованість слідчого щодо події шахрайства (61 %), пред'явлення речових, письмових та електронних доказів (82 %); фактор раптовості (71 %), використання асоціативних зв'язків (32 %), оголошення показань інших осіб (37 %), використання конфліктів у групі (29 %) тощо.

Особливістю допиту потерпілого є те, що у слідчого, як правило, немає достатнього часу для його підготовки, як рекомендують у підручниках із криміналістики. Однак у тактичному плані такий допит є дуже важливим, оскільки завдяки його проведенню слідчий отримує первинну інформацію, яка в подальшому впливає на планування розслідування, визначення первинних дій, обрання їх тактики. Так, у випадку вчинення шахрайства у сфері е-комерції шляхом несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, під час допиту потерпілого необхідно з'ясувати: 1) коли, як, за яких обставин було виявлено кримінальне правопорушення; 2) які докази вчинення саме протиправних дій у нього наявні; 3) у чому полягає виток, втрата, підробка, блокування інформації або спотворення процесу її обробки; 4) які системи захисту від несанкціонованого втручання встановлено так який алгоритм їх роботи; 5) чи були раніше позаштатні ситуації при роботі комп'ютерів чи електронних систем; 6) в яких протиправних цілях злочинці можуть використовувати інформацію або проблеми з її обробкою; 7) хто може вчинити протиправні дії,

хто може їх замовити; 8) які є докази на підтвердження цих припущень; 9) які дії було здійснено власником інформації (уповноваженою ним особою), законними користувачами після виявлення кримінального правопорушення; 10) хто може бути свідками та яку корисну інформацію для слідства можуть повідомити ці особи [102, с. 306].

Результати опитування практичних працівників, які мали відношення до розкриття та розслідування шахрайства у сфері е-комерції, показали, що при спілкуванні із потерпілим першочерговими завданнями є:

- отримати інформацію, що допоможе встановити аккаунт (обліковий запис) шахрая;

- відобразити URL-адресу (посилання) на його оголошення (надрукувати його у тексті допиту, зробити скріншот або фотознімок тощо);

- відобразити механізм спілкування потерпілого з шахраєм – чи було таке спілкування фізичним за допомогою телефонного зв'язку або у чатах соціальних мереж, або в мессенджерах;

- встановити наявну контактну інформацію про шахрая, у тому числі номер карткового рахунку, номер електронного гаманця, номер телефону, електронної адреси, тощо.

При цьому, до допиту слід обов'язково долучити:

- зображення (скріншоти) переписки;

- зображення (скріншоти) безпосереднього змісту і стилістики самого оголошення;

- зображення (скріншоти) сторінки, облікового запису шахрая в соціальній мережі або в мессенджері,

- документу, що підтверджує сплату коштів;

- виписку по банківському рахунку постраждалого із зазначенням платіжних систем, за допомогою яких здійснювалась транзакція. Такі виписки потерпілий може сформувати через системи онлайн-доступу (web-банкінг) до карткового чи електронного рахунку або отримати у відділенні банку роздруківку за своїм рахунком;

- у разі, якщо потерпілий зробив аудіозапис розмови з шахраєм, долучити копію такого запису для отримання зразку голосу злочинця.

Разом з тим, повнота і правдивість показань свідків залежать від вирішення таких тактичних завдань, що повинні враховуватись слідчим:

- правильне визначення кола осіб, які володіють інформацією, що має значення для розслідування;

- визначення можливої зацікавленості свідків у тих або інших результатах розслідування чи залежності від осіб, які зацікавлені в цьому;

- нейтралізації чинників, які негативно впливають на поведінку під час допиту (відмова, ухилення від дачі показань, неправдиві показання);

- врахування соціальних та психологічних особливостей допитуваного;

- вжиття заходів, спрямованих на попередження подальшої відмови від даних правдивих показань [23].

Серед кола осіб, що підлягають допиту як свідки у досліджуваній категорії проваджень, можна назвати: працівники, що супроводжують комерційні угоди в онлайн-режимі; представники та працівники юридичної особи, яка використовувалася під час вчинення злочину тим чи іншим способом; спеціалісти, що мають професійний досвід у галузі інформатики та комп’ютерної техніки, програмування, в тому числі особи, які приймали участь у якості спеціалістів підчас слідчих (розшукових) дій. Свідки часто володіють спеціальною, професійною освітою (у сфері КТ, банківського електронного обігу коштів) або в цілому є обізнаними у питаннях використання інформаційних технологій та ІТ-технологіях; особи, які знаходилися у приміщенні інтернет-кафе, банку; банківські працівники; родичі та знайомі потерпілого; родичі та знайомі підозрюваних тощо [160].

Говорячи про допит, слід мати на увазі, що тактика допиту підозрюваного істотно різниться від допиту інших осіб, тобто, якщо потерпілий чи свідок здебільшого ідуть на контакт і схильні до спілкування, то у відношенні підозрюваних слід використовувати великий арсенал тактичних прийомів [129]. При цьому, тактичні прийоми проведення допиту

підозрюваного обираються залежно від слідчої ситуації. Якщо підозрюваний дає правдиві показання, завдання слідчого полягає в уточненні цих відомостей, максимальній деталізації показань та ін. Якщо ж він дає неправдиві показання, то необхідно вжити заходів для викриття неправди: роз'яснити положення кримінально-процесуального законодавства про обставини, що пом'якшують вину, деталізувати його показання, провести повторні допити з тих самих обставин, пред'явити письмові і речові докази: документи, складені ним, експертні висновки, акти документальних ревізій, показання свідків, інших осіб тощо [46, с. 149].

Як показав аналіз судово-слідчої практики, допит підозрюваних осіб в основному спрямований на встановлення наступних обставин: біографічні дані; характер злочинної діяльності (час, протягом якого вчинялися протиправні дії, які саме, в чому вони полягали, кількість епізодів; механізм шахрайства; чи були співучасники і яка роль кожного, який склад групи, хто лідер); характер зв'язку із потерпілою особою; наявність корупційних зв'язків із представниками влади; ставлення шахрая до своїх дій та їхня оцінка; обставини, які обтяжують, а які пом'якшують відповідальність тощо.

2.3. Використання спеціальних знань як засіб тактичного забезпечення розслідування шахрайства у сфері е-комерції

Під час розслідування шахрайства виникає необхідність у залученні до процесу розслідування фахівців із інших галузей знань. Участь таких спеціалістів розширює практичні можливості слідчого у виявленні, закріпленні і дослідженні джерел доказової інформації [8].

При вчиненні шахрайства у сфері е-комерції також без використання спеціальних знань взагалі неможливо довести вину шахрая [72, с. 370].

Як зазначає Г. С. Бідняк, на законодавчому рівні не передбачено визначення поняття спеціальних знань та їх форм. У криміналістичній літературі теж не існує єдиної точки зору в цьому питанні, але зазначено, що форми використання спеціальних знань під час досудового слідства є значно ширшими за ті, що передбачені в законі. Науковці звертають увагу на структуру, суть, мету використання спеціальних знань та їх використання на різних стадіях кримінального процесу в різних формах, класифікують за різними підставами [12, с. 44].

Отже, вчені покладають різну змістовну складову у визначення поняття «спеціальні знання». Втім, єдність думок полягає в тому, що всі вони в основу даного терміну покладають наукові, технічні та практичні знання, набуті в результаті професійного навчання певною особою, що мають значення для встановлення об’єктивної істини у провадженні.

Не без уваги науковців залишилися й форми використання спеціальних знань.

Зокрема, В. В. Тіщенко поділяє їх використання на наступні форми: безпосередні, тобто такі, що безпосередньо спрямовані на збирання й отримання доказів; опосередковані, тобто ті, що сприяють збиранню і оцінці доказів [194, с. 351].

Досить громіздку класифікацію форм застосування спеціальних знань, як на нашу думку, запропонував В. Ревака, до яких він відніс: дослідження (передекспертне, у тому числі ревізія, й експертне); техніко-прикладна форма (застосування спеціальних знань при провадженні процесуальних дій); оперативно-розшукова форма; знаковолінгвістична форма (переклад); консультаційна форма [159, с. 35].

Зі свого боку, Д. В. Пашнєв стверджує, що форми використання спеціальних знань можуть бути диференційовані на обов’язкове і факультативне залучення їх при проведенні процесуальних дій. Крім того, процесуальні форми використання спеціальних знань поділяються за характером дій, при проведенні яких вони застосовуються, на ті, що

використовуються при проведенні слідчих та інших процесуальних дій. Непроцесуальні форми застосування спеціальних знань можуть бути розділені за ознаками сфери використання і суб'єкта їх застосування [144, с. 89].

За суб'єктами розподілив форми використання спеціальних знань В. К. Лисиченко, зокрема: використання спеціальних знань слідчим і особою, що провадить дізнання; використання спеціальних знань спеціалістом під час провадження слідчих дій; використання спеціальних знань експертом [105, с. 24].

З цього видно, що більшість вчених виділяє серед форм використання спеціальних знань як ті, що мають прояв у процесуальній, так і в не процесуальній формі.

Водночас у науковій літературі висловлюються полярні точки зору стосовно неприпустимості виділяти процесуальну і непроцесуальну форми використання спеціальних знань. Одні вчені стверджують, що непроцесуальна форма не може існувати апріорі і використовуватися при встановленні істини у кримінальному провадженні, адже розслідування злочинів є кримінально-процесуальною діяльністю, а тому використання спеціальних знань, яке не передбачене кримінально-процесуальним законодавством виходить за межі дії кримінального процесу. Інші ж стверджують, що законодавчо просто неможливо охопити всі випадки застосування спеціальних знань, а тому головним є те, щоб вони не суперечили кримінально-процесуальним нормам. Натомість, більшість вчених приєднується до другої точки зору, адже реалізація непроцесуальних форм використання спеціальних знань має на меті не набути однакового доказового значення з процесуальним використанням, а прагне створити умови для процесуального впровадження спеціальних знань у процес розслідування [10, с.191].

Натомість, слід погодитися із Т. О. Калюгою, яка наголошує, що за кримінальним процесуальним законодавством використання спеціальних

знань і проявляється у залученні спеціаліста до участі у слідчих (розшукових) діях і при призначенні та проведенні судової експертизи. Між тим, реальні потреби та напрямки застосування спеціальних знань у стадії досудового розслідування є набагато ширшими і більшість авторів допускають використання спеціальних знань у практиці розслідування як у процесуальних, так і в непроцесуальних формах [63, с. 184].

Досліджуючи питання щодо використання спеціальних знань при розслідуванні шахрайств, Г. С. Бідняк дійшла висновку, що для сучасних шахраїв характерне використання як традиційних прийомів, пристосованих до нових соціальних умов, так і нових, раніше невідомих. Так, залежно від способу вчинення шахрайства доцільними є такі форми використання спеціальних знань: призначення судових експертиз; довідково-консультаційна діяльність; ревізії та перевірка за обліками; залучення спеціаліста при проведенні слідчих (розшукових) дій; допит експерта; присутність слідчого при проведенні експертизи [13, с. 86].

Як показав аналіз судово-слідчої практики, при розслідуванні шахрайства в е-комерції найчастіше зустрічаються такі форми використання спеціальних знань: використання консультативної допомоги спеціаліста, призначення і проведення судових експертиз; участь спеціаліста при проведенні слідчих (розшукових) дій.

Низка вчених наголошує, що особливого значення під час зазначених процесуальних дій набуває професійна робота спеціалістів з документами, які у даному випадку бувають як паперового типу, так і електронного. Спеціалісти документознавці під час огляду паперових документів звертають увагу не тільки на загальні ознаки, як необхідний формат документу, папір, наявність певних реквізитів (дати, підписів, відбитків печаток та штампів), а і на приватні ознаки, які вказують на внесення змін у початковий зміст документу чи повну підробку. В залежності від способу посягань можлива необхідність залучення і спеціалістів-економістів, які звертають увагу на змістовну складову цих документів [30; 9].

Водночас, аналізуючи способи вчинення шахрайських посягань в умовах сучасності, зрозуміло, що в більшості випадків неможливо уникнути використання комп'ютерної техніки. Так, ряд способів вчинення шахрайства залишає відповідну слідову картину у вигляді віртуальних, комп'ютерних, електронних, цифрових слідів. І, незважаючи на те, що вчені остаточно не визначилися із загальноприйнятою назвою цих слідів, для професійної роботи з ними у вигляді пошуку, виявлення, вилучення та дослідження в якості спеціалістів залучають фахівців управління боротьби з кіберзлочинністю, судових експертів Експертної служби МВС України. Спеціаліст надасть допомогу під час огляду веб-сторінок та веб-сайтів, акаунтів користувачів у соціальних мережах з подальшим зберіганням та роздруківкою скриншоту із криміналістично значимою інформацією. Огляд веб-сторінки, на якій розміщено сайт певної фірми, з проведенням подальшого експертного дослідження у сфері телекомунікації, надає змогу вивчити зміст інформації стосовно діяльності певних суб'єктів, які мають відношення до події кримінального правопорушення, а також зафіксувати IP-адресу комп'ютерного обладнання, з якого здійснювалось управління веб-сайтом та визначити інтернет-провайдера, який надавав доступ до веб-сайту [133, с. 65; 30].

Роль спеціаліста простежується й під час огляду документів на електронних носіях, а також комп'ютері, під час якого може проводитися фотографування або відеозапис зображення на екрані дисплея. Під час огляду комп'ютера спеціаліст допомагає: зупинити програми й зафіксувати в протоколі результати своїх дій, відобразити зміни, що відбулися на комп'ютері; визначити наявність у комп'ютера зовнішніх пристроїв-накопичувачів інформації на твердих магнітних дисках (вінчестері), відобразити в протоколі й на схемі, яка до нього додається, місцезнаходження комп'ютера і його периферійних пристроїв (принтера, модему, клавіатури, монітора тощо); відобразити в протоколі призначення кожного пристрою, назву, серійний номер, комплектацію (наявність і тип

дисководів, мережних карт й ін.), наявність з’єднання з локальною обчислювальною мережею й (або) мережами телекомунікації, стан пристроїв (цілі або зі слідами зламу); точно описати порядок з’єднання між собою зазначених пристроїв, за необхідності зазначити сполучні кабелі й порти їхнього підключення, після чого від’єднати пристрої від комп’ютера [97, с. 96].

Втім, невміле поводження з комп’ютером може призвести до того, що необхідну інформацію не буде виявлено або взагалі буде знищено. У той же час при залученні спеціаліста до участі в огляді місця події слідчому важливо переконатися у його компетентності. На практиці має місце велика кількість помилок через залучення некомпетентного спеціаліста, що викликало труднощі у проведенні слідчої (розшукової) дії (наприклад, в якості спеціаліста використовують побутового користувача ПК, який не володіє навичками роботи на великих обчислюваних комплексах) [101, с. 306].

До участі в обшуку, у разі виявлення та вилучення різних документів (як паперових, такі електронних) доцільно залучати таких спеціалістів, як бухгалтери, товарознавці, ревізори, які можуть повідомити слідчому нові, мало або зовсім невідомі йому відомості, що мають суттєве значення для подальшого розслідування та допоможуть визначити, які саме документи варто вилучати. У процесі вилучення ж комп’ютерної техніки (жорстких дисків системних блоків комп’ютерів, флеш-носіїв, дискет тощо) доцільно запросити спеціаліста у цій галузі [200, с. 172]. Зокрема, при проведенні обшуку у кримінальних провадженнях даної категорії обов'язкова участь такого спеціаліста, як програміст, системний інженер і т.д., які надають допомогу слідчому з питань функціонування комп'ютера і системи в цілому. Спеціаліст визначає особливості комп'ютерного середовища, допомагає оглядати функціональну частину комп'ютера і зовнішні носії даних, а також технічну документацію. Спеціаліст допомагає в дослідженні інформації, вживає заходів для її перенесення на зовнішні носії інформації після визначення відношення інформації до розслідуваної події [197, с. 323].

До того ж, слід зазначити, що захист комп‘ютерної інформації здійснюється шляхом ідентифікації (користувач повідомляє своє ім’я) і автентифікації (перевірки справжності) – інша сторона впевнюється, що суб‘єкт дійсно той, за кого себе видає. Справжність підтверджується знанням пароля, особистого ідентифікаційного номеру, криптографічного ключа та інше; особистою карткою або іншим приладом аналогічного призначення; голосом, відбитками пальців і іншими біометричними характеристиками і т.д. [126, с. 54].

Допомога спеціаліста може стати в нагоді при необхідності подолання системи логічного захисту інформації та входження до комп’ютерних систем.

Не менш важливою є участь спеціаліста під час проведення допиту, особливо, якщо показання надає особа, яка є компетентною у певній галузі економіки, комерційної, банківської діяльності, а також знається на комп’ютерних технологіях.

Дана необхідність викликана тим, що слідчий, насамперед, має обмежені знання щодо спеціальної термінології, яку може використовувати допитуваний. По-друге, під час допиту може виникнути необхідність у роз’ясненні особливостей здійснення комерційної діяльності у дистанційному форматі, а також правил користування комп’ютерною технікою для здійснення комерційних операцій тощо. Спеціаліст може допомогти правильно сформулювати питання допитуваній особі.

Як показав аналіз судово-слідчої практики, під час розслідування шахрайства у сфері е-комерції можуть бути залучені такі спеціалісти: бухгалтери, економісти та інші особи, обізнані у комерційній діяльності; дистриб'ютори, дилери та інші посередники, які допомагають довести товар до споживача; виробники товарів та послуг; банківські працівники; психолог; постачальники електронних комунікаційних послуг; оператори послуг платіжної інфраструктури; реєстратори (адміністратори), що присвоюють мережеві ідентифікатори, та інші суб’єкти, що забезпечують передачу та

зберігання інформації з використанням інформаційно-комунікаційних систем тощо.

Такі спеціалісти сприятимуть: точному та повному тлумаченню показань допитуваного, який застосовує спеціальну термінологію; допоможуть проаналізувати чинні спеціальні правила, інструкції та інші документи; сформулювати запитання, що потребують уточнення деталей, пов'язаних зі спеціальними знаннями; встановити спосіб учинення злочинних дій; виявити неправдиві показання, які стосуються спеціальних питань тощо [190, с. 317].

Специфіка шахрайства зумовлює необхідність у отриманні певної інформації консультативного характеру (як у письмовій, так і в усній формі) про порядок укладання угод, права та обов'язки учасників цивільних правовідносин, особливості правового регулювання вказаної сфери правовідносин; наданні інформації про функціонування та призначення електронних реєстрів щодо здійснення правочинів та допомоги у правильному здійсненні доступу до реєстрів, в яких зафіксовані незаконні дії осіб при укладанні правочинів; наданні інформації про функціонування та призначення облікових, реєстраційних, довідкових, звітних паперових документів у паперовому вигляді, в яких відображаються дії щодо здійснення правочину щодо нерухомого майна громадян, та отримання доступу до таких документів; допомогу у правильному визначенні переліку документів, інших речових доказів, які необхідно вилучити під час обшуку, тимчасового доступу до речей та документів тощо. Крім того, в нагоді стане отримання професійної допомоги при оцінюванні висновку експерта, вивченні змістовної частини документів, а також при перевірці певної інформації за обліками криміналістичного та іншого призначення [155].

Натомість, серед всього спектру можливості використання спеціальних знань в кримінальних провадженнях особливе місце займає проведення експертиз. Відповідно до чинного КПК України процесуальний порядок їх призначення віднесено до проведення слідчих (розшукових) дій. Експертизи

проводяться конкретною особою – експертом. Але можуть призначатися як стороною обвинувачення, так і стороною захисту. При розслідуванні кримінальних правопорушень проводяться різноманітні експертизи з огляду на конкретну ситуацію. Тому їх дослідження є надзвичайно важливим для надання рекомендацій щодо їх призначення працівникам правоохоронних органів» [4, с. 231].

Як показали матеріали кримінального провадження щодо шахрайств у сфері е-комерції, найчастіше призначаються такі експертизи: технічна експертиза документів (95 %); почеркознавча експертиза (32 %); експертиза у сфері інтелектуальної власності (33 %); економічна експертиза (31 %); судова телекомунікаційна експертиза (24 %); трасологічна експертиза (11 %); комп'ютерно-технічна експертиза (42 %); експертиза відео звукозапису (15 %); портретна експертиза (9 %) та ін.

При розслідуванні кіберзлочинів доцільним може виявитись будь-який вид експертизи, проте найчастіше мова йде про комп'ютерно-технічну експертизу, яка, з точки зору чинного КПК України, є різновидом інженерно-технічної експертизи [37, с. 13]. При цьому, залежно від завдання, специфіки дослідження та видів об'єктів, які досліджують, у теорії виокремлюють різні її види, а саме: апаратно-комп'ютерну експертизу, програмно-комп'ютерну експертизу; експертизу даних (інформаційно-комп'ютерну); комп'ютерно-мережеву експертизу; комплекс цих експертиз. Об'єктами такої судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, карт-ридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання [169, с. 28].

Запорукою вдалої експертизи є правильність постановки завдань слідчим. Визначити вичерпні рекомендації щодо таких питань уявляється неможливим, і їхнє формулювання залежить від конкретних обставин справи

та рівня технічної підготовки слідчого. Водночас, слідчий повинен встановити ряд загальних питань, які спрямовані на виявлення основних рис досліджуваних подій. Це питання про можливість скоєння шахрайства за допомогою конкретного виду комп'ютерної техніки, про використання цієї техніки в момент скоєння шахрайства, про можливість використання техніки підозрюваним тощо [37, с. 13].

Так, якщо виникає необхідність з'ясувати, якого типу фізичний носій інформації містить документи, що підлягають огляду та, відповідно, яке обладнання потрібне для роботи з таким носієм, і при цьому носій захищено будь-яким типом захисту від зчитування чи копіювання, слід призначити судову експертизу комп'ютерної техніки і програмних продуктів та поставити перед експертом питання про можливість отримання доступу до вмісту такого носія, файлів, що розміщені на носії та їх атрибутів. За допомогою такої експертизи також можливо встановити технологію та хронологію створення конкретного електронного документа [80, с. 185; 153].

До найбільш актуальних ідентифікаційних завдань судової телекомунікаційної експертизи відносяться ототожнення конкретного телекомунікаційного засобу, що знаходиться у мережі, та ідентифікація конкретного користувача телекомунікаційного засобу [85, с. 13]. Об'єктами цієї експертизи часто є: Інтернет IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо) [169, с. 30].

Комплекс КТЕ й експертизи відеозвукозапису є також типовим під час розслідування шахрайств, учинених у кіберпросторі, адже шахраї активно використовують мультимедійні технології, що ґрунтуються на представлених даних у цифровому форматі відеозображення із застосуванням анімації та звукового супроводу. У цій експертизі спільні (інтеграційні) питання пов'язані зі встановленням їх оригінальності та незмінності (відсутністю

монтажу) запису за допомогою комп’ютерної техніки. Основним об’єктом дослідження є файли зі звуковими, відеоформатами. Їх носіями, що відправляють на дослідження, переважно є мобільні телефони, смартфони. Ця техніка становить різновид терміналу стільникового зв’язку, SIM-карти до неї є необхідним компонентом для функціонування такого терміналу як телекомунікаційного засобу. Тому дослідження їх є завданням експертизи телекомунікаційних систем (обладнання) та засобів. Проте, виконуючи функції цифрового органайзера або персонального комп’ютера (спеціалізованого комп’ютера з відповідним програмним забезпеченням для роботи з електронною поштою, перегляду текстових або мультимедійних файлів тощо), ця техніка одночасно є об’єктом КТЕ. Мобільні телефони оснащені слотом для карти пам’яті, та/або їх можна підключити до комп’ютера як звичайний зовнішній накопичувач інформації з файловою системою [169, с. 29].

Як показали матеріали судово-слідчої практики, суб’єкти комерційних відносин у 78 % випадків мали свої сторінки у соціальних мережах, в яких відображалися фотографії. До того ж, 28 % учасників дистанційних комерційних угод виходили на зв'язок між собою у форматі відеоконференції. 9 % потерпілих від шахрайства у сфері е-комерції надали правоохоронним органам скрини з екрана із зображенням шахрая.

Разом з тим, цифрові фотографічні зображення з соціальних мереж не завжди об’єктивно та достовірно відтворюють реальність, що є обов’язковою умовою для провадження судової портретної експертизи. Через застосування різноманітних ефектів фотокорекції зображень, особа, що на них відтворена, може отримати інші ознаки зовнішності, тому використання таких даних може привести до гносеологічної експертної помилки з об’єктивних причин. Все вищезазначене є важливим для врахування під час проведення судової портретної експертизи, оскільки, метою такої експертизи є ідентифікація особи за ознаками зовнішності за матеріальними зображеннями, зафіксованими у вигляді об’єктивних зображень на різних носіях, з

використанням спеціальних методів і прийомів дослідження. Так, фото особи вилучене з аккаунтів в соціальних мережах може бути використано наприклад для з'ясування чи зображена на обох фото одна й та сама особа (фото підозрюваного з камер відеоспостереження та фото з соціальних мереж). Втім, на заваді експертів стає спотворення зовнішності при редагуванні фотографій або зовнішнього вигляду особи на ній. З метою профілактики експертних помилок під час дослідження цифрових фотографічних зображень при провадженні судових портретних експертиз, необхідно перш за все встановити оригінальність таких зображень, зокрема, якщо вони вилучені з аккаунтів в соціальних мережах та надані як порівняльні матеріали для судово-експертного дослідження. Для цього можна ліцензовано використовувати вже розроблене програмне забезпечення. Але в такому випадку можна зіткнутись з деякими перешкодами. Незважаючи на те, що така програма може дозволити експертам легко виявляти модифікації зображення (включаючи операції масштабування, обрізки та повторного збереження), аналіз ELA залежить від якості зображення. Робота із зображенням, отриманим у результаті численних операцій повторного збереження, є неефективною. Якщо зображення повторно зберігається багато разів, воно може мати мінімальний рівень помилки, при якому більша кількість повторних збережень не змінює зображення [81, с. 428].

Як підкреслює ряд науковців, сталими лишаються об'єкти дослідження – документи як джерела криміналістично значущої інформації, – а також закономірності відображення та вивчення такої інформації в процесі розслідування злочинів. Ці питання можна вирішити шляхом почеркознавчої експертизи та технічної експертизи документів, які мають специфіку у провадженнях щодо шахрайства. При цьому, об'єктом почеркознавчого дослідження у провадженнях даної категорії здебільшого є підписи на комерційних угодах, на заявах, на квитанціях тощо [136; 94, с. 23].

Як відомо, всі почеркознавчі дослідження поділяються на три типи: ідентифікаційні (вирішення питання про тотожність виконавця почерку),

діагностичні (визначення умов виконання рукописного тексту або підпису), класифікаційні (встановлення статі й віку виконавця почерку). Однак на практиці суворо розмежувати ці види дослідження вкрай складно. Так, наприклад, під час проведення конкретної судово-почеркознавчої експертизи, пов’язаної з дослідженням почеркового об’єкту, виконаного у незвичних умовах, експерт у процесі дослідження одночасно вирішує як ідентифікаційне (за наявності порівняльного матеріалу), так і діагностичне завдання, навіть якщо питання ставиться лише в плані визначення тотожності виконавця даного почеркового об’єкту. Або вирішення класифікаційних завдань щодо встановлення похилого чи старого віку виконавця рукописного тексту чи підпису найтіснішим чином пов’язане з вирішенням діагностичних питань щодо стану його здоров′я на момент виконання досліджуваного почеркового об’єкту, наявності чи відсутності у нього захворювань, що впливають на писемно-рухові функції, зовнішніх умов виконання почеркового об’єкту (поза, пишучий прилад, підкладинка) і т. ін. [58, с. 24; 155].

Разом з тим, основними завданнями технічної експертизи документів в основному є: встановлення фактів і способів унесення змін до документів, що мають юридичне значення (договорів установчих документів, накладних, журналів тощо) та виявлення їх первинного змісту; встановлення документів, виготовлених шляхом монтажу із застосуванням копіювально-розмножувальної та комп'ютерної техніки; встановлення факту вибиття чеку на конкретному касовому апараті; встановлення цілого по частинам (у разі, якщо документ був навмисно розірваний або розрізаний зацікавленою особою); ідентифікація печаток, штампів, факсиміле тощо за їх відтисками тощо [62]. Нерідко слідчий стикається з необхідністю одночасного залучення фахівців і у сфері судової бухгалтерії, і у фінансовій галузі. В таких випадках рекомендується призначати комплексну судово-економічну експертизу [158, с. 12].

Отже, під час розслідування шахрайств у сфері е-комерції використання спеціальних знань у різноманітних формах відіграє велике значення та сприяє покращенню ефективності розслідування.

Висновки до розділу 2

Констатуючи сказане у розділі, спробуємо підсумувати зазначене таким чином.

1. Найсуттєвішою проблемою на початку кримінального провадження є визначення кримінально-правової кваліфікації, адже одні й ті самі дані про протиправне діяння можуть мати різну кримінально-правову кваліфікацію. Для розмежування звичайного шахрайства (ч. 1 ст. 190 КК України) від кваліфікованого (ч. 3 ст. 190 КК України) вже на початковому етапі, під час розгляду заяви потерпілого (іншого повідомлення), слідчий (дізнавач), встановивши наявність ознак кримінального правопорушення, задля вірної правової кваліфікації діяння має детально дослідити обставини скоєного шахрайства та порядок дій, як шахрая, так і потерпілої особи. Надзвичайно важливу роль в цьому процесі відіграє ретельний допит потерпілого та витребування в нього з подальшим дослідженням документів (листування в месенджерах або електронній пошті зі зловмисниками, виписки руху коштів з особистого банківського рахунку потерпілого, надані операторами зв'язку роздруківки вхідних та вихідних телефонних дзвінків потерпілого тощо).

2. Розглянуто приводи та підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції, висвітлено особливості взаємодії слідчих з іншими правоохоронними органами, а також установами, підприємствами та організаціями, громадськими формуваннями тощо.

3. Найбільш проблемною слідчою (розшуковою) дією у досліджуваній категорії проваджень є обшук. Задля закріплення доказів, отриманих у ході проведення обшуку, важливим є визначення підстав для правомірного

втручання в особисте життя особи та порушення недоторканості приватної власності тощо. Висвітлено організаційно-підготовчі заходи, що сприятимуть отриманню успішних результатів обшуку (визначення підстав для проведення обшуку; створення умов для дотримання процесуальних вимог та визнання допустимими доказів, отриманих у ході обшуку; створення сприятливих тактичних умов проведення обшуку; визначення правильної юридичної адреси об'єкта обшуку; визначення чіткого переліку об'єктів пошуку тощо).

Об'єктами вилучення можуть бути: реєстраційні документи, що посвідчують законність діяльності суб'єкта комерційної діяльності; фотографії, відеозаписи, на яких міститься інформація, що має значення для справи (факт знайомства певних осіб між собою, факт перебування особи у певному місці тощо); документи, що відображають особливості комерційної діяльності осіб, які мають відношення до шахрайських дій; документи, які містять відомості про можливих покупців; електронні та паперові договори про комерційні угоди; документи, що посвідчують особу (їх копії, підроблені документи на ім'я інших осіб); сім картки; квитанції про проведення банківських операцій; мобільні телефони, де міститься адресна книга (прізвища й адреси покупців, дані про організатора злочину); записні книжки, рукописні тексти на папері, у журналах тощо; комп'ютерна техніка (ноутбуки, планшети, системні блоки), де може міститися інформація про протиправну діяльність шахрая; електронні носії інформації; документи, що підтверджують відкриття розрахункових рахунків у банківській установі; договори з іншими організаціями, підприємствами та приватними підприємцями, які беруть участь у комерційних операціях; печатки та штампи як справжні, так і підроблені, кліше підписів тощо.

4. Важливим є огляд електронної інформації, що розміщена у відкритому доступі в мережі Інтернет, а також такої, що знаходиться на фізичних носіях інформації і у хмарних сервісах зберігання електронної інформації. У разі отримання пароля від власника облікового запису у хмарному сховищі, інформація, що знаходиться у віртуальному форматі,

копіюється з сервера на флеш або диск, або роздруковується на папір, після чого підлягає огляду. Натомість, якщо авторизаційні дані для доступу до аккаунта у хмарному сервісі отримати не вдалося, проводиться зняття інформації з електронних інформаційних систем.

5. Висвітлено організаційно-тактичні особливості проведення допиту та одночасного допиту різної категорії осіб, враховуючи специфіку розслідування шахрайства у сфері е-комерції.

6. Важливою є роль спеціаліста при проведенні окремих процесуальних та слідчих (розшукових) дій, зокрема: обшуку, тимчасовому доступу до речей та документів, у ході яких ведеться пошук та вилучається інформація, яка міститься у комп'ютерах, на електронних носіях інформації, у хмарних сховищах тощо, а також у пам'яті мобільних телефонів. Описується роль спеціаліста при необхідності подолання системи логічного захисту інформації та входження до комп'ютерних систем, а також при огляді носіїв комп'ютерної інформації, комп'ютерної техніки та інших вилучених об'єктів.

Наголошено на ролі судових експертиз при розслідуванні шахрайств у сфері е-комерції та сформульовано їх перелік. Висвітлюються особливості підготовки та проведення таких експертиз: технічної експертизи документів; почеркознавчої; портретної; судової телекомунікаційної; трасологічної; комп'ютерно-технічної експертизи; експертизи відеозвукозапису та ін.

РОЗДІЛ 3
НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ШАХРАЙСТВА У СФЕРІ Е-КОМЕРЦІЇ

3.1. Тактичні операції як засіб оптимізації розслідування шахрайства у сфері е-комерції

Тактична операція є засобом діяльності слідчого, що використовується для вирішення тактичних завдань, які виникають при розкритті, розслідуванні і попередженні злочинів [168, с. 79]. При цьому, Р. Л. Степанюк уточнює, що типові тактичні операції – це визначені на підставі узагальнення й аналізу слідчої практики комплекси слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів, спрямованих на вирішення типових проміжних завдань, що виникають на певних етапах розслідування в типових слідчих ситуаціях [186, с. 193]. В. Ю. Шепітько вказує, що тактичні операції є алгоритмами, програмами дій слідчого, працівника оперативного підрозділу, інших осіб щодо завдань, які виникають, і слідчих ситуацій [226, с. 179].

С.Ф. Здоровко запропонував визначення тактичної операції як системи однойменних або різнойменних процесуальних або непроцесуальних дій і заходів (слідчих, оперативно-розшукових, організаційних), які спрямовані на вирішення проміжного завдання розслідування, об’єднані єдиним планом і єдиним задумом, характеризуються вибірковістю і ситуаційною обумовленістю та виконуються правомочними посадовими особами під керівництвом слідчого [57, с. 6].

Є вчені, які у структурі тактичної операції наводять доволі складну її конструкцію: а) суб’єкт доказування як умова планування, організації та проведення методу з урахуванням суб’єктно-об’єктної природи останнього; б) складна особлива система цілей (завдання), до змісту якої, як окремий

випадок, можуть входити техніко-криміналістичні окремі та тактико-криміналістичні прості особливі системи цілей (завдання); в) засоби – процесуальні та непроцесуальні (організаційні та технічні) дії та заходи, методи пізнання, спеціальні криміналістичні методи (техніко-криміналістичні та структурно-криміналістичні), криміналістичні рекомендації, техніко-криміналістичні та тактико-криміналістичні прийоми, технічні та інші прийоми і методи; реставрація; реконструкція; тактико-криміналістичні комбінації; техніко-криміналістичні операції та ін.; г) зв'язки між наведеними компонентами. Проте, К. О. Чередник цілком вірно підмічає, що такий підхід є доволі громіздким і перевантажує зміст тактичної операції, приховуючи основні вагомі складові [210, с. 82].

З цього приводу М. С. Казаренко додає, що у кожній окремій методиці розслідування тактичним операціям повинен передувати перелік тактичних завдань, на вирішення яких вони мають бути спрямовані. Перелік таких тактичних завдань формується, виходячи із вивчення практики розслідування певних злочинів, які мають суттєві особливості, що накладають відбиток на процес їх розслідування. Урахування цих особливостей дає підстави для виділення основних типових тактичних завдань розслідування і відповідних їм тактичних операцій [60, с. 73].

Загалом, під час розслідування перед органами досудового розслідування постає низка завдань, пов'язаних із збиранням інформації про: обставини, що передували вчиненню шахрайства; місце та час вчинення шахрайства; способи шахрайства та кількість епізодів, причетність певних осіб до кожного з епізодів злочинної діяльності; кількість потерпілих, які постраждали внаслідок дій шахраїв; збір даних про сайт, який фігурував як об'єкт комерційного призначення, через який здійснювалися шахрайські операції; осіб, які можуть надати криміналістично-значиму інформацію про обставини вчинення шахрайства тощо.

Виходячи з цього, формуються тактичні операції, спрямовані на вирішення конкретних та проміжних завдань [70, с. 303].

За механізмом зв'язку між елементами тактичної операції в процесі її проведення тактичні операції поділяють на такі, що передбачають: а) послідовне здійснення усієї системи дій та заходів у найбільш оптимальній послідовності; б) паралельну реалізацію елементів системи; в) змішане проведення тактичної операції, коли одна частина слідчих дій та оперативно-розшукових заходів здійснюється паралельно, інша – послідовно. За тривалістю проведення тактичні операції вчені поділяють на: а) наскрізні (проводяться протягом кількох етапів розслідування), б) локальні (реалізуються в рамках одного етапу розслідування). Можна зустріти поділ тактичних операцій й за змістом, зокрема: а) неоднорідні, що мають у своєму складі слідчі дії, оперативно-розшукові заходи та інші дії; б) однорідні, що складаються з однієї слідчої дії, котра виконується за допомогою кількох взаємопов'язаних тактичних прийомів, або такі, що складаються лише із слідчих дій або лише оперативно-розшукових заходів [149, с. 162].

В контексті даної проблематики В. М. Шевчук наголошує на потребі в розробленні універсальних класифікаційних підстав, які б мали наскрізний характер, могли успішно використовуватися до будь-яких злочинних проявів, ситуацій, тактичних завдань. Вчений вважає за доцільне запропонувати такі класифікаційні підстави розподілу тактичних операцій, зокрема, за змістом: а) базові (універсальні); б) специфічні. Останні розробляються до особливостей розслідування злочинів більш вузької групи для вирішення завдань, властивих лише процесу розслідування певної категорії злочинних проявів [224, с. 188].

Після прийняття рішення про проведення певної тактичної операції відбувається побудова моделі цієї операції і створення програми її реалізації. До програми має бути включено системний перелік методичних рекомендацій та конкретних дій щодо вибору засобів розв'язання сформульованих тактичних завдань, визначення послідовності їх застосування, з урахуванням часу, місця і початку операції. Поряд із цим до загальної моделі програми тактичної операції можуть входити моделі дій кожного з її учасників або

моделі здійснення тієї чи іншої слідчої дії, що входить до складу тактичної операції [223].

Різноплановість завдань криміналістики і неможливість у зв'язку із цим використовувати єдиний, універсальний алгоритм вимагає від слідчого пошуку оптимальних шляхів вирішення завдань. Їх реалізація можлива тільки тоді, коли будь-яке загальне завдання розслідування піддається розчленуванню на свої складові частини, що мають доволі вузьку, індивідуалізовану сферу застосування. Розглядаючи криміналістичні алгоритми, необхідно враховувати те, що їх побудова відбувається на основі повторюваності явищ, наявності в них внутрішніх закономірностей, а саме змінюваності і відносної сталості. Тому тактична операція є засобом алгоритмізації процесу розслідування злочинів і такі операції є необхідними програмами дій слідчого, виконують важливу методичну функцію і дозволяють вибирати правильний напрямок у розслідуванні [29, с. 148].

Вважаємо за необхідне визначити перелік типових тактичних операцій і розглянути їх з урахуванням специфіки розслідування шахрайств, вчинених у сфері е-комерції.

Як показав аналіз судово-слідчої практики та аналіз літературних джерел, до типових тактичних операцій під час розслідування шахрайств, вчинених в мережі Інтернет, здебільшого відносять такі: «Збирання вихідної інформації про шахрайство», «Відмежування шахрайських дій від інших складів», «Пошук та викриття шахрая», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному просторі», «Встановлення ознак організованості», «Епізод», «Нейтралізація протидії розслідуванню», «Забезпечення відшкодування матеріальних збитків», «Фіктивний комерсант», «Встановлення умислу», «Затримання» тощо. До того ж, як показав аналіз матеріалів практики, останнім часом під час розслідування шахрайств у сфері е-комерції, виникає потреба у проведенні тактичної операції «злочинець-в'язень».

Характеризуючи особливості проведення тактичної операції «Збирання вихідної інформації про шахрайство», необхідно зауважити, що початковий етап розслідування незаконного збирання та розголошення комерційної таємниці зазвичай характеризується гострим дефіцитом інформації щодо низки важливих елементів характеристики цих кримінальних правопорушень, і саме за допомогою такої тактичної операції виявляється інформаційна сутність, інформативність конкретної слідчої ситуації. Розроблення вказаної тактичної операції спрямовує увагу та дії слідчого на збирання інформації про елементи структури злочинної діяльності та визначення оптимальних засобів та умов досягнення цієї мети. У процесі проведення тактичної операції «Збирання і фіксація вихідної інформації про шахрайство» розрізнені відомості накопичуються за певною схемою, в якій враховуються джерела криміналістично значущої інформації, способи її виявлення, засоби формування на її підставі доказів у кримінальному провадженні. Виявлена, відповідним чином оброблена криміналістично значуща інформація групується, узагальнюється та аналізується [149, с. 163].

Залежно від наявної в розпорядженні слідчого інформації висувається більш обґрунтована версія про конкретний спосіб (і окремі його елементи) вчинення шахрайства, що видозмінює й індивідуалізує комплекс рекомендованих слідчих (розшукових) дій і інших заходів. Особливого значення в цьому аспекті набувають оперативно-розшукові дані, здобуті до початку й під час здійснення тактичної операції [117, с. 142].

Разом з цим, основним тактичним завданням слідчого є не тільки виокремлення шахрайства від інших кримінальних правопорушень, а й розмежування з цивільно-правовим деліктом. Як показало анкетування працівників, які мають досвід розкриття та розслідування шахрайств, найскладнішим у розслідуванні є установлення справжнього наміру особи на момент здійснення правочину (93% респондентів) [99]. Як справедливо наголошує Н. В. Павлова, щоб дійти висновку про наявність чи відсутність ознак шахрайства, необхідно точно знати, який був намір у особи під час

заволодіння чужим майном чи правом на нього. Тільки у такому разі можна правильно розмежувати цивільно-правовий делікт від шахрайства [132, с. 76].

Виходячи з цього, доцільним в рамках вказаної тактичної операції провести комплекс заходів, спрямованих на встановлення ознак шахрайства, залежно від певного етапу злочинної діяльності. Втім, для вирішення завдань тактичної операції необхідно:

1) провести ретельний аналіз дій з підготовки до вчинення шахрайства та з'ясувати момент і обставини виникнення злочинного умислу, його спрямованість. З цією метою проводяться оперативно-розшукові заходи, спрямовані на встановлення свідків, які можуть надати інформацію про обставини підготовки та всіх причетних до цього осіб, допити, одночасні допити, пред'явлення для впізнання, тимчасовий доступ до речей та документів, які використовувалися для отримання певних дозволів та ін.;

2) встановити обставини та умови укладання договору, характер та можливість виконання заявлених зобов'язань між сторонами, залучені до цього процесу особи, порядок розрахунків. З цією метою проводиться допит потерпілих із докладним описанням часу, місця, обставин укладання договору, його змісту, характеру заявлених обіцянок, сприйняття потерпілим всього, що відбувалося. Необхідну інформацію можна отримати у ході аналізу змістовної частини документів, що використовувалися при укладанні договорів, а також шляхом направлення запитів й одержання офіційних довідок тощо;

3) збір даних про компанію та аналіз її діяльності на предмет законності. Вивчаються установчі, реєстраційні документи, документи фінансово-облікової звітності та ін., проводяться допити потерпілих, свідків, підозрюваних, одночасні допити між ними. В деяких випадках доцільно включити до тактичної операції НСРД;

4) з'ясувати причини невиконання заявлених зобов'язань. Встановлюється у ході допитів, одночасних допитів, співставлення змісту ряду документів, проведення експертиз тощо [99].

Розглянута тактична операція тісно переплітається із тактичної операцією «Відмежування шахрайських дій від інших складів». Як ми вже зазначали, під час розслідування шахрайства у сфері е-комерції виникають труднощі із відмежуванням шахрайських дій від інших складів. Для визначення кваліфікації таких правопорушень необхідно розуміти порядок дій шахраїв шляхом їх моделювання та, за необхідності, звертатися за допомогою до працівників кіберполіції.

Як показали матеріали судово-слідчої практики та опитування практичних працівників, які розслідували шахрайства у сфері е-комерції, з метою єдиного підходу до кваліфікації кримінальних правопорушень, учинених із використанням високих інформаційних технологій, за частинами третьою статті 190 КК України необхідно враховувати:

- дії, скоєні з використанням соціальної інженерії, коли правопорушниками вбачається отримання у держателів платіжних карток їхніх реквізитів та іншої конфеденційної інформації шляхом імітації діяльності у кіберпросторі державних соціальних програм, компаній, банків-емітентів з використанням не голосових засобів комунікації під різними приводами (надання соціальної допомоги вимушеним переселенцям, є-підтримка, фінансова допомога від державних та міжнародних інституцій, благодійних фондів, банків тощо);

- дії, учинені шляхом створення фіктивних оголошень про продаж товарів в соціальних мережах, якщо потерпілі самостійно здійснили оплату затовар;

- дії, які передбачають оформлення шахраями онлайн-кредитів у фінансових установах із використанням конфіденційних (персональних) даних інших осіб без відома особи, крім частини третьої статті 190 КК України, додатково ще кваліфікуються за статтею 182 КК України.

- заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою необхідно кваліфікувати за частиною першою статті 190 КК України у випадках, коли шахрайство учинене шляхом

використання засобів мобільного зв'язку та створення в потерпілої особи уявної необхідності передачі коштів стороннім особам, перерахування грошей особисто потерпілим на рахунки шахраїв тощо. Винятком є отримання телефонного дзвінка від шахрая (вішинг), коли потерпілий обов'язково вчинятиме певні дії, через які з його карткового рахунку буде знято кошти. Так, за командою шахрая потерпілий натискає клавіши мобільного телефону, надає дані платіжної картки (номер, термін закінчення дії, PIN-код, CVV-код тощо). Такі дії потрібно кваліфікувати за частиною третьою статті 190 КК України.

У разі встановлення факту несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, такі дії додатково підлягають кваліфікації за ст. 361 КК України.

Одним із центральних завдань тактичної операції «Епізод» є визначення кола постраждалих від шахрайського посягання, а також встановлення всіх осіб, які можуть надати криміналістично значиму інформацію про обставини шахрайства та осіб, які причетні до кожного епізоду [99].

Тактична операція «Епізод» полягає у проведенні комплексу слідчих (розшукових), негласних слідчих (розшукових) дій, оперативно-розшукових, організаційних та інших заходів, спрямованих на вирішення тактичного завдання з виявлення всіх епізодів злочинної діяльності конкретної особи та з'ясування їх взаємозалежностей. Реалізується згадана тактична операція в залежності від етапу розслідування та криміналістичної ситуації шляхом проведення таких заходів:

- оперативна перевірка підозрюваного на причетність до вчинення інших кримінальних правопорушень;

- здійснення перевірки за Інтегрованими інформаційно-пошуковими системами Національної поліції України, Єдиними та Державними реєстрами, іншими пошуковими системами в електронних мережах

загального користування з метою отримання довідково-аналітичної та оперативно-пошукової інформації, у тому числі про аналогічні нерозкриті кримінальні правопорушення;

- отримання консультаційної допомоги від фахівців;

- вилучення документації, пов'язаної зі службовою діяльністю підозрюваного, шляхом проведення відповідних обшуків, тимчасового вилучення чи отримання тимчасового доступу до неї;

- огляд вилученої документації, аналіз її змісту та виявлення слідів імовірної фальсифікації;

- призначення технічних і почеркознавчих експертиз документів;

- проведення ревізій, зустрічних та інших перевірок;

- отримання зразків для експертизи, за необхідності – негласне отримання зразків, необхідних для порівняльного дослідження;

- призначення судово-економічної та інших судових експертиз;

- допит підозрюваного та свідків;

- здійснення аудіо-, відеоконтролю особи злочинця та місця;

- зняття інформації з електронних комунікаційних мереж, отримання розшифрування телефонних розмов і проведення їх аналізу;

- зняття інформації з електронних інформаційних систем тощо [156, с. 291].

Мета тактичної операції «Незаконна транзакція» полягає у перевірці історії проведених транзакцій, здійснених особами, які є фігурантами у провадженні щодо шахрайства в е-комерції, та виокремленні фактів, що визначають кримінальну відповідальність осіб, які їх здійснювали. До того ж, у ході такої тактичної операції можна встановити факт зламу аккаунта та крадіжки персональних даних, які використовувалися для проведення незаконних транзакцій тощо.

Важливу роль у реалізації такої тактичної операції відіграє Департамент кіберполіції, який надає істотну допомогу органам досудового

розслідування та підрозділам карного розшуку у виявленні та доведенні фактів шахрайства у мережі Інтернет [160, с. 173].

З метою встановлення всіх транзакцій, і виявлення серед них незаконних, слід отримати виписку по банківському рахунку із зазначенням платіжних систем, за допомогою яких здійснювалась транзакція. Разом з тим, слід звернутись із клопотанням про тимчасовий доступ до інформації банківських установ про власників банківських карток/рахунків, на які здійснювався переказ грошей потерпілих, місце зняття коштів та фото- і відеозаписи з камер, встановлених на банкоматах або у відділеннях банку. Якщо гроші перераховувались на інші рахунки, то також IP-адреси користування web-банкінгом. Важливою є інформація від операторів мобільного зв’язку, з метою встановлення IMEI мобільних терміналів, в яких працювала дана сім-карта, місце виходу її на зв'язок та коло її інших абонентів. Дана інформація дозволить встановити інших потерпілих, через коло зв’язків прив’язати сім-карту до шахрая, знайти під час обшуку мобільні термінали, в яких вона використовувалась та ідентифікувати їх із злочинцем.

Як ми вже зазначали, шахрайства у сфері е-комерції нерідко вчиняються у складі групи.

Натомість, внаслідок використання шахраями корупційних зв’язків з посадовими особами владно-управлінських органів та протидії розслідуванню виникає складність доведення факту вчинення шахрайства організованою групою [125, с. 19].

У положенні статті 28 КК України законодавцем визначаються ознаки, які мають бути встановлені для того, щоб віднести злочинну групу до організованої. До таких відносяться: наявність декількох осіб та їх попередня зорганізованість у спільне стійке об’єднання для готування або вчинення злочинів; об’єднаність злочинів єдиним планом з розподілом функцій учасників групи, спрямованих на реалізацію цього плану; обізнаність усіх учасників такої групи з цим планом [95]. Втім, у юридичній літературі можна побачити більш розширене, аніж в законі бачення ознак організованості.

Так, І. І. Іванчишин до ознак ОЗГ відносить: ієрархічність ЗГ; тривалість злочинної діяльності ЗГ та кримінальну спрямованість на отримання значимих прибутків; плановий характер злочинної діяльності; стійкість, цілісність та постійність складу ЗГ; висока технічна оснащеність; створення спеціального грошового фонду; наявність корумпованих зв'язків [59, с. 7]. Ще більш розширений перелік ознак, які слід встановити слідчому для того, щоб вважати групу організованою, окреслює В. М. Варцаба. На його переконання, ознаками психологічного механізму функціонування організованих злочинних груп є: 1) ієрархічна побудова організованих угруповань; 2) певна стійкість і тривалість існування; 3) спеціалізація у спрямованості злочинного формування; 4) сувора внурішньогрупова дисципліна; 5) існування злочинних норм і правил поведінки; 6) наявність лідера (декількох лідерів) з владними повноваженнями; 7) розподіл функціональних обов'язків серед членів групи; 8) корислива спрямованість (кримінальний бізнес) злочинної діяльності; 9) наявність системи захисту від викриття; 10) створення єдиної каси («общака»); 11) існування власної системи «заохочення» і «покарання»; 12) підтримка тих, кого притягують до кримінальної відповідальності; 13) існування системи втягування до злочинної групи; 14) використання корумпованості в органах влади і управління, а також в правоохоронних органах; 15) наявність стосунків із корумпованими особами органів влади і управління та працівниками правоохоронних органів; 16) підтримання стосунків та вирішення проблем між організованими злочинними угрупованнями в різних регіонах країни та за її межами; 17) наявність системи проникнення у владні структури та створення механізму лобіювання власних інтересів [22, с. 7].

Цікавою є думка К. О. Чаплинського, який ознаки організованої злочинної групи поділяє на основні чотири групи за наступними підставами:

1. За ознаками організованості:

- виражені організаційно-управлінські структури та ієрархічність злочинних груп, наявність єдиних норм й правил поведінки, системи санкцій та їх практична реалізація;

- наявність лідера (організатора) та чіткий розподіл ролей й функцій в злочинній групі.

2. За характером діяльності:

- стійкий, запланований і законспірований характер злочинної діяльності, наявність спільних цілей, орієнтація на отримання максимально високих злочинних прибутків;

- постійний та тривалий характер злочинної діяльності групи;

- прагнення до встановлення міжрегіональних зв'язків;

- активне розповсюдження антигромадської ідеології;

- учинення нетрадиційних злочинів (зокрема, викрадення людей, торгівля людьми, незаконна трансплантація органів тощо);

- встановлення контактів із працівниками правоохоронних органів з метою використання цих корумпованих зв'язків для прикриття злочинної діяльності організованої групи.

3. За ознаками матеріального забезпечення:

- висока технічна забезпеченість злочинної групи;

- використання сучасних науково-технічних засобів, транспорту;

- наявність значних грошових сум, матеріальна підтримка членів злочинної групи та їх близьких.

4. За особливостями забезпечення злочинної діяльності:

- наявність корумпованих зв'язків із представниками державної влади та правоохоронних органів;

- цілеспрямована розробка заходів протидії правоохоронним органам;

- наявність системи нейтралізації форм соціального контролю [207, с. 35-36].

В контексті даної проблематики слід зауважити, що іноді вчені вважають, що для доведення ознак організованості слід застосовувати

декілька тактичних операцій. Наприклад, В. М. Варцаба для встановлення ознак організованості пропонує їх аж п’ять, зокрема: «Організований характер злочину»; «Склад і структура організованої групи»; «Корумповані зв’язки організованої групи»; «Взаємодія організованої групи з іншими злочинними формуваннями»; «Причетність організованої групи до злочинів» [22, с. 14].

Натомість, слід зауважити, що зміст вказаних тактичних операцій полягає у єдиному завданні – встановлення ознак організованості. Тому на нашу думку, при необхідності доведення факту вчинення шахрайства у сфері е-комерції організованою групою, не потрібно використовувати низку тактичних операцій, спрямованих на вирішення однакових завдань, оскільки це зумовить зайву витрату часу. В рамках однієї тактичної операції «встановлення ознак організованості» слідчий, шляхом проведення комплексу заходів, одночасно вирішить питання й щодо складу групи, ролі кожного із співучасників у вчиненні шахрайства, наявності корумпованих зв’язків тощо.

Вказана тактична операція здійснюється в тісній взаємодії органу досудового розслідування з оперативними підрозділами. Зокрема, працівники оперативних підрозділів за дорученнями слідчого, вказівками прокурора проводять оперативно-розшукові заходи, спрямовані на пошук і перевірку осіб на причетність до вчиненого кримінального правопорушення; негласні слідчі (розшукові) дії; перевірки за інтегрованими інформаційно-пошуковими системами Національної поліції України, Єдиними та Державними реєстрами, іншими пошуковими системами з метою отримання інформації про причетних до вчинення протиправних дій осіб. Також встановлення співучасників здійснюється шляхом проведення низки допитів підозрюваного (-их), свідків, у тому числі одночасних допитів [156, с. 292].

У свою чергу, найбільш поширеними заходами, що входять до тактичної операції «встановлення ознак організованості», можна віднести: допити свідків, потерпілих, співучасників; пред’явлення для впізнання

предметів, документів, осіб; проведення НСРД, спрямованих на спостереження за особою, річчю або місцем, зняття інформації з електронних комунікаційних мереж та електронних інформаційних систем (спостерігання за членами групи, які знаходяться на волі та прослуховування їхніх розмов); виконання спеціального завдання щодо участі в ЗУ особи, яка на конфіденційній основі співпрацює з органами досудового розслідування (впровадження в групу); контроль за вчиненням злочину; тимчасовий доступ до речей та документів та провадження одночасних обшуків; огляд предметів та документів; призначення судових експертиз (почеркознавчої, технічної експертизи документів, комп'ютерної техніки та програмних продуктів, економічної, судово-психологічної тощо); проведення ОРЗ, спрямованих на отримання інформації про співучасників та осіб, які могли сприяти вчиненню злочину; ОРЗ, спрямовані на встановлення місцезнаходження осіб, які переховуються від слідства та суду; проведення СРД, ОРЗ, спрямованих на розшук активів та накладення на них арешту тощо [210, с. 141].

При цьому, тактика допиту підозрюваних у розслідуванні кримінальних правопорушень, що вчиняють організовані групи, відрізняється і особливостями, і використанням специфічних тактичних прийомів. Важливим тактичним прийомом є пошук у ланцюзі підозрюваних «слабкої ланки». У криміналістичній літературі зазначено, що це можуть бути особи, які мають у групі незначне, підпорядковане становище, потрапили в групу через безвольність, матеріальну залежність від лідера, компромат. Цих осіб необхідно допитувати якнайперше, бо від них можна одержати правдиві показання. Якщо на цих осіб мають вплив лідери групи або вони бояться, потрібно спробувати роз'яснити непорядну роль лідера щодо втягування допитуваного у групу, прагненням лідера уникнути покарання через перекладення вини, використовувати наявні внутрішньогрупові конфлікти [31, с. 178]. Доцільно приділити увагу й особам, які схильні до співпраці зі слідством, проте бояться помсти, переслідувань з боку керівництва, інших зацікавлених осіб, розголосу їх свідомої громадянської позиції. За таких

обставин слідчий зобов'язаний забезпечити оптимальні умови безпеки для такого свідка [33].

Деякі вчені, з метою викриття організатора злочинного угруповання, пропонують досліджувати фонозапис розмов з віданням злочинних наказів та розпоряджень, з подальшим порівняльним дослідженням зразків голосу особи, яка перевіряється, з фонограмою, отриманою під час проведення оперативно-розшукових заходів [227; 52].

Загалом, до типових обставин, що мають надзвичайно важливе значення при встановленні ознак організованості, можуть бути віднесені: 1) організований характер злочину: яким чином вчинялися злочини, їхня тривалість, поширеність; наявність злочинної діяльності постійного характеру; плановий характер злочинної діяльності; прагнення до розширення сфер діяльності; використання вогнепальної зброї і засобів зв'язку; наявність контактів із співробітниками правоохоронних та інших державних органів та ін.; 2) наявність і склад організованого формування: кількість учасників злочинної діяльності; ієрархічна структура злочинної групи; наявність розподілу ролей; форми взаємодії в злочинному угрупованні; стабільність складу групи, правила поведінки в групі та ін.; 3) базовий елемент злочинної діяльності ОЗГ: господарсько-економічна діяльність членів угруповання; участь у тіньовому бізнесі; місця зосередження ядра і членів злочинного формування; незаконна діяльність групи; зв'язки злочинної групи з підприємцями і злочинним світом; місце угруповання в кримінальному середовищі; прикриття злочинної діяльності легальними структурами; участь членів злочинної групи в політичній діяльності тощо [22, с. 10]. Разом з тим, В. П. Корж додає, що окрім вказаних обставин, у разі використання комп'ютерних технологій при вчиненні кримінальних правопорушень, слід звернути увагу на ознаки, що можуть свідчити про організовану злочинну діяльність, зокрема: спотворення комп'ютерної інформації, що відображає виробничо-господарську операцію, суб'єкта підприємницької діяльності, кредитно-фінансову діяльність банку;

спотворення бухгалтерського обліку в електронному варіанті; протиріччя у змісті бухгалтерського обліку в електронному варіанті та у традиційному, тобто в головній книзі; знищення комп'ютерного запису в самому комп'ютері; знищення комп'ютерного запису, що зберігається на магнітних носіях інформації; збійні ситуації, що спричинили нібито через помилки у програмі збій комп'ютера, тощо [84, с. 225].

Наведемо приклад вчинення шахрайства у сфері е-комерції організованим угрупованням. Досудовим розслідуванням встановлено, що будучи раніше судимим за майнові злочини, маючи не зняту та непогашену судимість, ОСОБА 1 вирішив збагатитися шляхом незаконного заволодіння майном громадян шляхом шахрайства. Перебуваючи в Державній установі «Хмельницький слідчий ізолятор» (далі СІЗО), за підозрою у вчиненні майнових злочинів, останній на шлях виправлення не став та вирішив продовжити злочинну діяльність і визначив вчинення злочинів, пов`язаних із заволодінням чужим майном, як основне джерело свого збагачення та існування. Переслідуючи прямий умисел, направлений на здійснення протиправних дій в сфері злочинів проти власності, в вересні 2016 року організував злочинну групу у складі ОСОБИ 2, ОСОБИ 3, ОСОБИ 4, а в подальшому, у жовтні 2016 року, до складу групи на добровільних засадах увійшла ОСОБА_6. Так, ОСОБА 1 перебуваючи з лютого 2016 році в СІЗО, познайомився там з ОСОБОЮ 3 та ОСОБОЮ 2, які також раніше були судимі за майнові злочини та відповідно з липня 2016 та квітня 2015 перебували в СІЗО. Для реалізації своїх злочинних намірів ОСОБА 1 розробив злочинний план, який полягав у заволодінні майном громадян шляхом шахрайства, для чого вирішив створити стійку злочинну організовану групу. До складу вказаної групи, на початку вересня 2016 року, як співучасників залучив на добровільних засадах своїх нових знайомих ОСОБУ 2 та ОСОБУ 3, яким довів розроблений єдиний план злочинної діяльності щодо вчинення шахрайств, розподіливши при цьому їх функції, спрямовані на досягнення цього плану, шляхи прикриття своєї злочинної діяльності, отримання та

розподілу незаконних матеріальних благ між членами організованої групи. Розуміючи, що перебуваючи в СІЗО ОСОБА 1, ОСОБА 2 та ОСОБА 3, не зможуть в повній мірі реалізувати свої злочинні наміри у зв`язку з чим, як співвиконавців, в вересні 2016 року, залучили до складу групи ОСОБУ 4 та в подальшому, з жовтня 2016 року, ОСОБА_6, які перебували на волі. Згідно розробленого плану, ОСОБА 1 взяв на себе роль організатора та виконавця злочинів ОСОБА 2, ОСОБА 3, ОСОБА 4 та ОСОБА_6 виступили співвиконавцями вчинення злочинів. Дані особи підтримували між собою відносини та перебували у дружніх і близьких стосунках, а саме ОСОБА 1, ОСОБА 3 та ОСОБА 2 на час вчинення злочинів перебували в СІЗО м. Хмельницького. Стійкість організованої групи виражалася в стабільних, міцних внутрішніх зв`язках між її учасниками, існуванні певних правил поведінки, спільної мети, яка базувалася на бажанні кожного з них отримувати стабільні незаконні прибутки для задоволення власних потреб у виді грошових коштів, а також в обізнаності кожного учасника організованої групи у плані вчинення злочинів, розробленого ОСОБОЮ 1 і узгодженого з іншими учасниками організованої групи, який полягав у поетапному його виконанні [182]. Вказане свідчить про реальність вчинення шахрайських дій, у тому числі у сфері е-комерції із місць позбавлення волі. Як свідчить судово-слідча практика, кількість таких фактів складає приблизно 14 %.

Виходячи з цього, актуальною є проведення тактичної операції «Злочинець – в’язень», метою якої є встановлення факту, що шахрайство у сфері е-комерції вчинялося із місць позбавлення волі.

Реалізація цієї тактичної операції здійснюється у тісній взаємодії слідчого, оперативних підрозділів Департаменту кіберполіції НПУ та співробітниками місць позбавлення волі (СІЗО, УВП). При цьому, важливими заходами для викриття шахрая, який дії в місцях позбавлення волі є: проведення комплексу оперативних заходів, спрямованих на документування шахрайських дій; прослуховування телефонних переговорів шахрая із іншими особами та потерпілими в рамках НСРД; допит потерпілих; допити

свідків; проведення особистих обшуків, а також в камерах в'язня, з метою вилучення мобільних телефонів, планшетів, сім-карток мобільного зв'язку, чорнових записів, інформації щодо банківських карток, аккаунтів потерпілих тощо; проведення обшуків за місцем проживання співучасників, які проживають на волі та надавали допомогу у вчиненні шахрайства; затримання організатора та учасників злочинного угрупування та їх допити тощо.

Як ми вже раніше зазначали, важливим тактичним завданням при розслідувані шахрайства у сфері е-комерції є визначення комп'ютера користувача мережі, з якого були здійснені протиправні дії.

Як правило, для встановлення особи, яка розмістила пост чи іншу інформацію на веб-сторінці у мережі Інтернет, необхідно встановити власника веб-сайту (веб-сторінки). Відповідно до ст. 1 Закону України «Про авторське право і суміжні права» від 23.12.1993 р. № 3792-XII власник веб-сайту – особа, яка є володільцем облікового запису та встановлює порядок і умови використання веб-сайту. За відсутності доказів іншого власником веб-сайту вважається реєстрант відповідного доменного імені, за яким здійснюється доступ до веб-сайту, і (або) отримувач послуг хостингу. Власник веб-сторінки – особа, яка є володільцем облікового запису, що використовується для розміщення веб-сторінки на веб-сайті, та яка управляє і (або) розміщує електронну (цифрову) інформацію в межах такої веб-сторінки. Власник веб-сайту не є власником веб-сторінки, якщо останній володіє обліковим записом, що дозволяє йому самостійно, незалежно від власника веб-сайту, розміщувати інформацію на веб-сторінці та управляти нею [208].

Для ідентифікації особи, яка здійснювала протиправні дії з певної точки доступу, стають в нагоді тактичні операції «Встановлення IP-адреси» та «Ідентифікація особи у віртуальному просторі», що передбачають такі поступові слідчі (розшукові) дії, оперативно-розшукові й організаційні заходи: зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або

утримувачем чи непов’язаний з подоланням системи логічного захисту; встановлення місцезнаходження радіоелектронного засобу; оформлення та відправлення запитів про витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових осіб відомостей, що становлять інтерес для кримінального провадження та/або здійснення запитів щодо обміну інформацією між компетентними підрозділами правоохоронних органів іноземних держав з питань реагування на кіберзлочини каналами сектору Національного контактного пункту реагування на кіберзлочини (НПК ДКП НП України); допити потерпілих та свідків;обшуки у підозрюваних;огляд комп’ютерної техніки; призначення експертиз тощо[161, с. 179; 169, с. 35].

У цьому розрізі слід зазначити, що завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів таких як MAC або IP-адрес в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь на питання те ж цей пристрій або ні, але не повідомляє точний тип пристрою і спосіб його використання конкретним користувачем. Окрім ідентифікаторів, можливе використання додаткової інформації, яка затребувана у разі обробки непрямих ознак, на підставі інформації отримуваної з датчиків пристрою і в результаті роботи програмного забезпечення на пристрої. Особливе місце серед програмного забезпечення з точки зору завдання ідентифікації пристрою займає браузер, як програма, за допомогою якої користувач дістає доступ до більшості інтернет-ресурсів. Для ідентифікації використовується інформація cookies-файлів та інформація про встановлені шрифти і плагінах. Вирішуючи задачу ідентифікації з використанням непрямих ознак, слід враховувати швидкість зміни конфігурацій апаратного і версій програмного забезпечення вживаного користувачем [172, с. 151].

Натомість, В. А. Світличний та К. Е. Петров наголошують на погрішності ідентифікації, заснованої на IP-адресі (до недавнього часу облік був основним методом ідентифікації), складається з погрішностей передачі і

погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через proxy-сервер уся підмережа, яка за ним ховається, у більшості випадків матиме єдиний IP-адрес. З іншого боку, працюючи через комутоване з'єднання, користувач при кожному підключенні отримуватиме від провайдера новий IP-адрес і т. д. [172, с. 151]. З цього приводу В. О. Тімашов та Д. Ш. Діденко додають, що типові веб-браузери розкривають свої унікальні IP-адреси (інтернет-протоколи), що дає змогу відстежувати їх дії правоохоронними органами. Але веббраузер у «Даркнеті» видає помилкові IP-адреси, щоб замаскувати особистість користувача. Анонімність програмного забезпечення створює додаткові труднощі для збору та розшифрування доказів. З цією метою з'являється пріоритетна задача використання найкращих та найновіших стандартів та інструментів [193, с. 168].

Переходячи до тактичної операції «Фіктивний комерсант», слід сказати, що шахраї створюють в мережі Інтернет фейковий сайт популярних сервісів (інтернет-банкінгу, «olx» (наприклад olx-доставка), «Нової Пошти», популярних сервісів з миттєвого поповнення рахунку мобільних телефонів, тощо) який на вигляд не відрізняється від справжнього. Єдина відмінність у URL-адресі (посилання), на яку потерпілий зазвичай не звертає уваги. Проводячи оплату на фейковому сайті або заповнюючи форму зворотного зв'язку, потерпілий вводить данні своєї банківської карти (номер/строк дії/CVV-код), після введення яких – зловмисники в режимі реального часу можуть виводити кошти з банківської картки шляхом проведення несанкціонованих транзакцій, використовуючи отримані дані карткового рахунку, які сам же потерпілий і ввів.

Під час реалізації тактичної операції «Фіктивний комерсант», слід вирішити такі завдання: наявність у особи, яка здійснювала комерційні операції в Інтернеті, відповідних реєстраційних документів, ліцензій; встановлення відповідності реквізитів у документах назві суб'єкта підприємницької діяльності; наявність умислу на невиконання зобов'язань

згідно договору комерційного призначення; з'ясування, чи не є фальшивим сайт, з якого здійснювалися комерційні операції тощо.

Для встановлення належності сайту за допомогою сервісу Whois визначається провайдер, який надає послугу хостингу. Далі для встановлення належності сайта необхідно звернутися до провайдера із запитом про: реєстраційні дані (logs) та абонентську інформацію про особу, якій надаються послуги хостингу для сайта; адреси, телефонні номери та інші реквізити власника сайта; IP-адреси, використані для створення сайта; IP-адреси, використані для поповнення сайта; інформація про зміст сайта; інформація про користування сайтом. Разом з тим, тактична операція «Фальшивий сайт», окрім окреслених заходів, включає ще й: зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту; встановлення місцезнаходження радіоелектронного засобу; допити потерпілих та свідків; огляд комп'ютерної техніки; призначення експертиз тощо [169, с. 24; 161, с. 182].

На нашу думку, ознаками, що підтверджують фіктивність особи, яка здійснює комерційні операції шляхом використання комп'ютерних технологій, можуть бути:

- компанія, що здійснює комерційні операції, або приватна особа-підприємець, не мають відповідного підтвердження про реєстрацію;

- компанія, що здійснює комерційні операції, або приватна особа-підприємець, зареєстровані на підставну особу;

- відсутність ідентифікації електронної сторінки з самою фірмою (присутність ідентифікаційних характеристик компанії, логотипу і марки фірми);

- компанія, що здійснює комерційні операції, або приватна особа-підприємець, здійснюють продаж інших товарів та послуг, а не тих, щодо яких здійснено домовленість;

- компанія, що здійснює комерційні операції, або приватна особа-підприємець, завищують або занижують обсяги угод;

- комерційні операції не виконувалися особою, яка зазначена їх виконавцем або замовником;

- відсутність на сайті всього набору необхідної контактної інформації (адреса фірми, контактні телефони, електронна адреса і тому подібне), а також відомостей про діяльність фірми і її товари (послуги);

- відсутність інформації про успішну реалізацію комерційних проектів проєктів тощо.

3.2. Профілактична діяльність уповноважених осіб у провадженнях за фактами шахрайства у сфері е-комерції

У процесі досудового розслідування слідчий зобов'язаний виявити обставини, причини та умови, що сприяли вчиненню злочину, адже без цього неможливо встановити коло інших обставин, які підлягають доказуванню у кримінальному провадженні. Найголовніше, слідчий вправі поінформувати про виявлені обставини зацікавлених суб'єктів [111, с. 348; 233, с.33]. С. М. Смоков і А. А. Десятник також наголошують на необхідності закріплення процесуального обов'язку сторони обвинувачення встановлювати вказані обставини для активізації профілактичної діяльності [174, с. 115].

Не дивлячись на увагу з боку науковців до проблем криміналістичної профілактики, слід наголосити, що після набуття чинності КПК України 2012 р. у нормативному закріпленні профілактичних функцій слідчих Національної поліції склалася суперечлива ситуація. З одного боку, положення чинного кодексу не визначають обов'язки слідчих, пов'язані з виконанням загально-кримінологічної чи спеціальної профілактики. З іншого боку, у Законі України «Про Національну поліцію» запобігання злочинам та

іншим правопорушенням було віднесено до основних обов’язків поліції, які традиційно поширювалися на усі підрозділи та служби МВС України, в тому числі – на підрозділи Головного слідчого управління. Окрім того, профілактична складова роботи слідчого знайшла відображення у положеннях відомчого нормативного акту – наказу МВС України від 06.07.2017 № 570 «Про організацію діяльності слідчих підрозділів Національної поліції України» та закріплених ним Положеннях, згідно яких слідча профілактична діяльність зводиться до виявлення причин і умов, які сприяють учиненню кримінальних правопорушень, і вжиття через відповідні органи заходів щодо їх усунення [211, с. 185].

З цього вбачається суперечність між законодавчим та відомчим рівнями регулювання діяльності слідчих у сфері запобігання кримінальним правопорушенням, що потребує внесення в чинний КПК України положень, які б висвітлювали процедуру здійснення профілактичних заходів. Адже профілактична діяльність слідчого повинна бути необхідною складовою досудового розслідування кримінальних правопорушень [77, с. 54].

Традиційно вчені вважають, що фактори, які впливають на злочинність, вивчаються кримінологією, в той же час багато аспектів у проблемі запобігання кримінальним правопорушенням не належить ні до кримінології, ні до будь-якої іншої науки кримінально-правового циклу, а знаходиться на перетині різних галузей знань. Втім, складовою частиною методики розслідування окремих видів кримінальних правопорушень, на думку низки вчених, є методи з'ясування причин конкретного кримінального правопорушення [234, с. 57].

З цього приводу можна погодитися з думкою А. В. Рейнгольда, який влучно наголошує, що всі причини та умови, які сприяють вчиненню таких шахрайств, носять як суб’єктивний, так і об’єктивний характер. Зокрема, до об’єктивних причин та умов вчений відносить наступні:

- наявність законодавчих колізій щодо здійснення комерційних інтернет-угод. Так, згідно з роз’ясненням Міністерства економічного

розвитку і торгівлі України у листі № 3502-05/43517-14 від 19.11.2012 р. суб'єкти господарювання, які здійснюють торгівлю за допомогою мережі Інтернет, повинні керуватися вимогами Правил продажу товарів на замовлення та поза торговельними або офісними приміщеннями. Між тим, не дивлячись на існування цих Правил, законодавчо вимоги щодо порядку створення таких магазинів не достатньо визначені, що не заважає шахраям створювати інтернет-магазини, а потім їх ліквідовувати. Це створює підґрунтя для існування магазинів у мережі Інтернет, що діють за принципом фірм-одноденок;

- недостатня нормативна урегульованість питань пов'язаних із створенням, введенням/виведенням коштів, ліквідацією електронних гаманців, що полегшує використання їх у злочинній діяльності. Основні властивості віртуальних гаманців, якими зловживають злочинці, полягають у можливості: швидкого, дешевого проведення трансакцій і легкості обходу обмежень, зокрема за сумами платежів; організації та проведення нелегальної діяльності за допомогою мережі Інтернет, доходи від якої надходять за допомогою платежів в електронних грошах; ухилення від сплати податків; приховування слідів трансакції (послідовного ряду трансакцій); використання третіх осіб; де-персоніфікованого введення/виведення готівки; «обходу» банківської системи, яку жорстко регулюють з питань легалізації коштів, отриманих злочинним шляхом;

- зростання випадків переведення грошей через платіжні системи WebMoney, PayPaЬ, QIWI, які позбавляють можливості ідентифікувати особу, яка знімає кошти з рахунку;

- зростання випадків оплати товарів та послуг криптовалютою, статус якої дотепер не визначений;

- недостатня сформованість єдиного понятійного апарату щодо середовища, в якому вчиняються кримінальні правопорушення, пов'язані із використанням комп'ютерних технологій;

- низький рівень розкриття кримінальних правопорушень, пов’язаних із купівлею-продажем товарів через мережу Інтернет, в той час, як латентність є дуже високою;

- складність доведення факту вчинення обману в мережі Інтернет, що породжує нові випадку з боку одних і тих самих осіб;

– розповсюдженість недостовірних пропозицій у ЗМІ та мережі Internet;

- зниження рівня життя населення, що змушує шукати пропозиції в Інтернеті за більш вигідними цінами, аніж у торгівельних центрах;

- недостатній контроль з боку суб’єктів, які повинні здійснювати функції з контролю за діяльністю суб’єктів підприємницької діяльності сфери;

- неоднозначність судової практики щодо шахрайств у мережі Інтернет тощо [163, с. 192].

Водночас, суб’єктивними причинами та умовами, що сприяють вчиненню комерційних інтернет-шахрайств є:

- надання громадянами переваги укладанню дистанційного варіанта угод щодо купівлі-продажу товарів та послуг, що виключає прямий фізичний контакт продавця та покупця;

- халатне відношення до перевірки репутації підприємця, який пропонує об’єкти комерційного призначення і Інтернеті та покупця, який такі об’єкти (послуги) бажає отримати;

- халатне відношення до вивчення інформації, що міститься в електронній формі щодо умов купівлі-продажу товарів та послуг;

- халатне відношення до вивчення змісту документів, в яких зафіксовано укладання дистанційної угоди;

- надто велика довірливість, безпечність та необачність громадян;

- професійно-моральна деформація суб’єктів підприємницької діяльності, та схильність їх до обману з метою наживи [163, с. 192].

Є й думки щодо виокремлення причин та умов, що впливають на рівень вчинення кібершахрайств, через призму певних загроз, зокрема:

- відкритість суспільства та держави. Створена на основі комп'ютерних мереж та інформаційних технологій зручна інфраструктура для міжнародних постачань товарів, надання послуг, переказу коштів між фізичними і юридичними особами, зберігання інформації у мережі Інтернет та під'єднання до неї кожного комп'ютера, надає одночасно широкі можливості як власне кіберзлочинів за допомогою комп'ютерних технологій;

- висока технологічність. Надзвичайно швидкий розвиток інформаційних технологій та складність цієї сфери поряд з відносно тривалим та бюрократичним підходом до розвитку нормативно-правових баз призводить до значного відставання заходів щодо упередження та боротьби з кібершахрайством;

- складний характер злочину. Інтернет-шахраї використовують комп'ютерні технології, інформаційні мережі з соціально-психологічних міркувань, зокрема дискредитації урядів і держав, розміщення сайтів терористичної спрямованості, псування і руйнування ключових систем, виведення цих систем з робочого стану (що є свого роду доповненням до традиційного виду тероризму);

- анонімність злочину. Шахраїв приваблює відсутність фізичного контакту з жертвою та, безперечно, складність виявлення, фіксування та вилучення криміналістично-значущої інформації у віртуальному просторі;

- транснаціональний та популярний характер шахрайства. Особливістю даного виду злочинності є те, що підготовка та скоєння злочину, за наявності доступу до мережі Інтернет, може здійснюватись практично з будь-якого місця. А враховуючи, що комп'ютерна техніка та інтернет-послуги стають доступнішими для все ширшого кола осіб, кіберзлочинність стає все більш популярною [67, с. 130].

Не применшуючи значення встановлення причин та умов, які сприяють вчиненню кримінальних правопорушень, вчинених шляхом шахрайства, слід зауважити, що не менш важливим завданням є й розробка та застосування спеціальних заходів криміналістичної профілактики [131, с. 288].

Натомість, є певна розбіжність думок й щодо профілактичних заходів, за допомогою яких здійснюється запобігання, припинення та з'ясування причин та умов, що сприяли вчиненню злочину [52]. Наприклад, О. А. Борідько, розглядаючи теорію профілактики злочинності як системну розробку наукових засад діяльності щодо її попередження на всіх напрямах і рівнях різними державними інституціями, наголошує на необхідності комплексної розробки заходів планомірного впливу на причини та умови вчинення злочинів. У такій системі кримінологія дає лише загальні рекомендації, визначаючи основні напрями та заходи запобігання злочинів, а криміналістична теорія має розробляти конкретні запобіжні засоби та прийоми впливу на конкретні види злочинів. Тому вчений, застосовуючи системний аналіз, досліджує та узагальнює сучасні рівні та форми організації профілактичної діяльності різних суб'єктів профілактичної діяльності, зокрема, у соціологічному плані - суспільство в цілому, колективи, групи, індивіди; у соціально-політичному плані - держава в цілому, державні органи та громадські організації, громадяни [17, с. 11].

О. В. Александренко до профілактичних заходів, за допомогою яких здійснюється запобігання, припинення та з'ясування причин та умов, що сприяли вчиненню злочину,відносить: збереження таємниці слідства; запобігання витоку оперативної та службової інформації; заходи по забезпеченню захисту доказів від фальсифікації, знищення; спілкування суб'єктів розслідування з учасниками кримінального процесу, яке виключає виникнення чи розвиток з їх боку конфліктних ситуацій; своєчасне проведення слідчих і оперативних заходів для забезпечення збереження слідів, доказів, попередження здійснення протиправного впливу на учасників розслідування; використання з цією метою даних щодо способів протидії, які використовувалися конкретними особами та ін. [2, с. 13].

Слушною є думка про припинення та запобігання комерційних інтернет-шахрайств саме технічними засобами. Зокрема, дослідження технічних можливостей електронно-обчислювальної техніки та особливостей

функціонування мережі Інтернет дозволяє виявити певні факти, що можуть свідчити про шахрайські дії та запобігти подальшій їх реалізації. Деякі автори, з метою профілактики шахрайства, навіть розробили концептуальну модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу. Зокрема, виходячи з аналізу статистичних даних можна виділити показники, що можуть вказувати на можливе виникнення кіберзагрози в процесі виконання банківської операції:

- транзакція має ознаки кіберзагрози, якщо її ініційовано на території іншої країни. В більшості банків прийнята практика необхідності повідомлення банка клієнтом про його виїзд за кордон та зазначення країн, які будуть відвідані. В іншому випадку служба безпеки банку може заблокувати карту, якщо по ній будуть ініційовано транзакції з іншої країні. Це пов’язано з тим, що хакери, зламуючи доступ до мобільного або інтернет-банкінгу та привласнюючи чужі кошти, застосовують спеціальні програми для шифрування їх місцеположення;

- на ймовірність виникнення кіберзагрози впливає тип пристрою, з якого виконувалась транзакція. Існують різні способи злому мобільних пристроїв та комп’ютерів, завдяки яким зловмисники з легкістю отримують доступ до мобільного та інтернет-банкінгу користувачів банківських послуг. Також банк не в змозі контролювати, хто є користувачем та де він користується пристроєм. Частіше за все такі операції можуть містити ознаки кіберзагроз;

- тип проведеної транзакції впливає на ймовірність виникнення ознак кіберзагрози. Широке коло типів банківських транзакцій сприяє впровадженню нових заходів з боку зловмисників, направлених на заволодіння чужими коштами та порушення безпеки інформації в банку;

- обнуління рахунків клієнтів банку вказує на ймовірні ознаки кіберзагроз. Сьогодні досить розповсюдженими є безготівкові розрахунки, коли платежі відбуваються без використання готівкових коштів. Тому, в більшості випадків на банківському рахунку людини завжди присутня певна

сума коштів. Якщо під час транзакції зі зняття всієї суми можливо має місце ознака порушення користування рахунком або несанкціоноване зняття коштів [236; 161].

Серед різноманітних підсистем криміналістичної профілактики та різноманіття суб'єктів, що реалізують окремі напрямки превентивної діяльності, слід виділити й експертну профілактику, під якою розуміється складне системне утворення, основою якого складає діяльність експертів на базі своїх спеціальних знань, які виявлятимуть обставини, що сприяли вчиненню злочинів. Виявлення подібних обставин може здійснюватися як основне експертне завдання, для вирішення якого і була призначена експертиза, або це може бути супутній «продукт» експертної діяльності, що «з'являється» при вирішенні інших експертних завдань, які не ставили за мету виявлення криміногенних факторів. Допустимим є також виявлення криміногенних факторів та обставин, що сприяють вчиненню злочинів, у процесі узагальнення експертної практики в окремій судово-експертній установі у ході її накопичення, або в разі підготовки відповідних оглядів, звітів, аналітичних довідок [199, с. 155]. При чому, експертна профілактика полягає не лише у виявленні експертом на основі спеціальних знань обставин, які сприяють вчиненню злочину, а й у прогнозуванні виникнення можливих способів здійснення протизаконної діяльності у сучасних умовах та розробці заходів щодо покращення захисту об'єктів [32, с. 236].

Так, як показав аналіз кримінальних проваджень щодо шахрайства у сфері е-комерції, саме висновки експертів істотною мірою впливали на рівень запобігання подальшим спробам вчиняти шахрайські дії окремими особами (групою осіб). До того ж, у 67 % проваджень завдяки ідентифікаційним експертним дослідженням було встановлено аналогічні факти, які, як наслідок, складали один ланцюг шахрайських операцій у сфері е-комерції [74, с. 293].

У своєму монографічному дослідженні Н. Є. Філіпенко навіть наголошує, що у випадках, коли встановлені причини скоєння злочину

можуть сприяти вчиненню аналогічних правопорушень в інших підприємствах установах чи організаціях, у тому числі в інших сферах життєдіяльності людини, керівник експертної служби повинен безпосередньо повідомити відповідні правоохоронні органи для попередження вчинення цих правопорушень. При цьому, вчений зазначає, що проблему експертної ініціативи пов'язано не лише з межами кримінального провадження, але ще й із тим, що праву експерта фактично не відповідає нічий обов'язок реалізувати ту додаткову інформацію, яку за власною ініціативою отримує експерт. Складається досить складна ситуація: ініціатива експерта може залишитися не реалізованою, а його висновки – не використаними. Найчастіше доводиться зустрічатися з такою ситуацією, коли за ініціативою експерта розробляються ті чи інші профілактичні рекомендації [198, с. 225].

Якщо вести мову про профілактичні заходи, що здійснюються безпосередньо слідчим, то шляхами їх реалізації є застосування заходів забезпечення кримінального провадження (затримання особи, арешт майна, тримання під вартою), проведення окремих слідчих (розшукових) дій (огляду, допиту та інших), а також тактичних операцій. Так, застосування слідчим запобіжних заходів спрямоване не тільки на забезпечення виконання підозрюваним покладених на нього обов'язків, а й на запобігання спробам підозрюваного вчинити інше кримінальне правопорушення чи продовжувати кримінальне правопорушення, у якому він підозрюється. Крім того, саме під час ознайомлення з матеріалами кримінального провадження слідчий може виявити обставини криміногенного характеру, які вже попередньо зафіксовані у документах (актах ревізій, висновках експертів, довідках, поясненнях та показаннях інших осіб, тощо) [196, с. 323; 69, с.76; 8].

Слід сказати, що запобіганню шахрайствам у сфері е-комерції сприяє рівень інформаційно-аналітичного забезпечення та використання можливостей різноманітних обліків, баз даних тощо.

З цього приводу Д. М. Цехан і П. С. Луцюк стверджують, що нині основними джерелами інформації профілактики є: автоматизовані

інформаційні системи, автоматизовані робочі місця, оперативні обліки, алфавітні картотеки, мережа Інтернет тощо [204].

До того ж, що профілактична функція насамперед стосується й оперативних підрозділів кіберполіції. Зокрема, Департамент кіберполіції відповідно до покладених на нього завдань:

- визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;

- у межах своїх повноважень уживає необхідних оперативнорозшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;

- уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об’єктів, у тому числі об’єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень; організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;

- проводить серед населення роз’яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;

- вивчає позитивний вітчизняний і зарубіжний досвід боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та вносить пропозиції керівництву Національної поліції України щодо його впровадження;

- відповідно до чинного законодавства збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими

показниками службової діяльності, надає, відповідно до законодавства України, звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань попередження та протидії кіберзлочинам [6, с. 92; 161].

Натомість, слід погодитися з А. Ф. Волобуєвим, що профілактична діяльність правоохоронних органів при розслідуванні злочинів дає максимальний ефект тільки тоді, коли вона органічно поєднується з економічними, соціальними, правовими й організаційними заходами запобігання злочинності в масштабах країни [154, с. 12]. Крім того, стан захищеності знаходиться у прямій залежності від обізнаності, підготовленості, ресурсної та технічної забезпеченості, нормативно-правової урегульованості діяльності правоохоронних, контролюючих та інших органів державної влади й управління, які діють у взаємодії з юридичними та фізичними особами у питаннях забезпечення інформаційної безпеки і боротьби зі злочинністю з використанням мережі Інтернет [217, с. 91].

Разом з тим, профілактичні заходи у правовому полі спрямовані на розв’язання проблеми вдосконалення нормативно-правових актів, які є підґрунтям єдиної державної політики забезпечення інформаційної безпеки та її реалізації. На думку К. С. Качашвілі, першим кроком до здійснення цієї мети є визначення кібернетичної безпеки як самостійної сфери національної безпеки. Це дасть змогу формувати засади державної політики у сфері забезпечення кібернетичної безпеки України шляхом визначення основних реальних загроз національній безпеці, основних напрямів державної політики та основних функцій суб’єктів щодо забезпечення національної безпеки в цій сфері. Крім того, попередження кіберзлочинності базується на заходах, спрямованих на зниження ризику здійснення таких кримінальних правопорушень та нейтралізацію шкідливих наслідків для суспільства [67, с. 130].

У свою чергу, в організаційному аспекті основною проблемою профілактики шахрайств є відсутність необхідної спеціалізації підрозділів

МВС при організації та здійсненні профілактики таких кримінальних правопорушень та слабка взаємодія між суб'єктами профілактики, а також відсутність єдиного координуючого органу та ефективної системи контролю за виявленням та розслідуванням організованих кримінальних правопорушень. У цьому розрізі Г. В. Недзельська, серед заходів запобігання комп'ютерного шахрайства виділяє:

– створення спеціалізованих центрів збору та аналізу інформації про факти шахрайства в Інтернеті. Діяльність подібних організацій повинна бути орієнтована не стільки на констатацію злочинних посягань, скільки на вироблення дієвих профілактичних заходів. Одним із напрямків діяльності цих центрів мають стати збір інформації про потенційно небезпечні об'єкти та їх блокування;

– організація підбору, навчання та інструктажу працівників служб комп'ютерної (інформаційної) безпеки суб'єктів господарювання;

– впровадження програми навчання громадян основам комп'ютерної безпеки під час виробництва фінансових операцій через інформаційні мережі, спілкування у соціальних мережах та ін., інформування через ЗМІ про нові види комп'ютерного шахрайства;

– розробка та використання спеціального програмного забезпечення, у тому числі антивірусних програм або програм ідентифікації користувача;

– розширення системи спеціалізованих відділів, що займаються комп'ютерними злочинами, та формування єдиної державної бази інтернет-шахраїв [120, с. 212].

Оскільки у нашому дослідженні йдеться не просто про кібершахрайство, а шахрайство, пов'язане із комерційною діяльністю в онлайн-режимі, слід розглянути також заходи профілактики шахрайства саме у цій сфері.

Зокрема, є нагальна необхідність створення механізму оперативного реагування на шахрайство у сфері комерційної діяльності через блокування активів шахрайських компаній та зупинення їх діяльності. До того ж, є

необхідність ведення податковими органами інформаційної бази про підприємців, раніше судимих за шахрайство, та зазначення таких відомостей у виписці з ЄДРЮО, а також розвивати системи громадських порталів, що ведуть реєстр неблагонадійних суб'єктів комерційної діяльності [120, с. 212], у тому числі і в онлайн-режимі.

До того ж, важливими є профілактичні заходи інформаційного-виховного і віктимологічного характеру. Зокрема, шляхом задіяння засобів масової інформації (газети, журнали, телебачення, Інтернет, інформаційні ресурси, офіційні веб-сторінки державних органів влади та підприємств) здійснюється реалізація методу розповсюдження інформаційного контенту. Правоохоронні органи також можуть приймати участь у подібних заходах через спеціалізовані підрозділи та прес-центри Національної поліції [104, с. 97].

Що стосується юридичних осіб, то вони повинні також вживати комплекс ефективних заходів у протидії інтернет-шахрайству. Наприклад, із метою забезпечення безпеки банківських операцій компанії необхідно виокремити комп'ютери, що міститимуть фінансові дані та реквізити юридичної особи, а для вирішення решти питань, зокрема здійснення небанківських операцій, виділити іншу комп'ютерну техніку, з доступом до мережі Інтернет, тобто комп'ютери загального користування. Крім цього, за умови виведення комп'ютера з матеріально-технічної бази юридичної особи, слід пам'ятати про необхідність створення резервної копії наявної інформації та очищення жорсткого диску тощо [7, с. 191; 238].

Також до заходів криміналістичної профілактики можна ще віднести заборону інтернет-торгівлі суб'єктам, які не розкривають реєстраційної інформації та гармонізацію законодавчої бази України до міжнародно-правових стандартів, щоб не виникало непорозумінь під час здійснення е-комерції.

Таким чином, з урахуванням тенденції до суттєвого збільшення кількості зареєстрованих фактів онлайн-шахрайств під час дії воєнного стану

вважається доцільним рекомендувати Національній поліції України, слідчі (дізнавачі) якої відповідно до положень ст. 216 КПК України уповноважені на здійснення досудового розслідування кримінальних правопорушень, передбачених ст. 190 КК України, розгорнути «агресивну» інформаційну-роз'яснювальну кампанію серед населення.

Сутність вище згаданої кампанії полягає у активній взаємодії Національної поліції України та її територіальних підрозділів з органами місцевого самоврядування, громадськими організаціями, державними та не державними ЗМІ, закладами вищої та середньої освіти, представниками бізнесу щодо виготовлення та доведення до відома якомога більшої кількості громадян інформаційних матеріалів профілактичного характеру. З метою охоплення максимальної кількості населення виглядає доцільним розміщення інформаційно-роз'яснювальної інформації на білбордах та сітілайтах. Виготовлені постери, плакати та листівки мають бути присутні у громадському транспорті, на вокзалах, в торгово-розважальних центрах, АЗК.

Не мають бути залишені поза увагою місця масового перебування громадян: медичні заклади, поштові відділення, учбові заклади, магазини, приміщення органів влади та місцевого самоврядування.

Окремої уваги заслуговує використання можливостей інформаційних ресурсів самих правоохоронних органів, насамперед Національної поліції України, в якій створена та тривалий час функціонує система відділів комунікації, які співпрацюють з регіональними та всеукраїнськими ЗМІ, мають власні сайти, сторінки в соціальних мережах, виробляють власний аудіовізуальний контент, а також проявляють високу активність в інших засобах масової комунікації, в т.ч. в соціальних мережах та електронних ЗМІ.

Як окрему складову концепції профілактики вчинення онлайн-шахрайств, найпоширенішою схемою яких залишається непостачання замовлених товарів, необхідно зазначити діяльність правоохоронців щодо моніторингу соціальних мереж та ЗМІ. Зокрема, аналізуючи аудіо-відео-цифровий контент на предмет наявності скарг громадян щодо дій

або бездіяльності посадових осіб під час прийняття та розгляду заяв про скоєні шахрайства, правоохоронці можуть запобігти подальшим фактам укриття злочинів від обліку, а їх органи досудового розслідування – реалізувати принцип невідворотності покарання, шляхом встановлення та притягнення шахраїв до кримінальної відповідальності за усі епізоди їх злочинної діяльності.

Варто відзначити діяльність кіберполіції, яка з метою протидії та попередження шахрайствам надає усім відвідувачам свого офіційного сайту можливість перевірити підозрілу інформацію за такими параметрами: номер банківської картки, телефон або посилання на сайт (доступ за посиланням https://cyberpolice.gov.ua/stopfraud/), а також надає корисні поради «Як не стати жертвою шахраїв». На тому ж сайті існує форма зворотнього зв'язку для тих, хто зазнав моральної чи матеріальної шкоди від дій шахраїв та бажає звернутись до правоохоронців з електронним зверненням, не виходячи з власної домівки. Зазначена послуга від кіберполіції має набути подальшого розвитку та бути інтегрована у сервіси «ДІЯ» - мобільного застосунку, веб-порталу і бренду цифрової держави в Україні, розробленого Міністерством цифрової трансформації. Адже «ДІЯ» це доступний для більшості українців портал, в якому громадяни можуть отримувати державні послуги онлайн. Сервіси «ДІЇ», якими до кінця 2023 року будуть користуватись близько 20 млн. користувачів, можуть включати ті самі розділи, які доступні користувачам сайту кіберполіції.

Слід також зазначити, що в січні 2023 року Департаментом кіберполіції Національної поліції України розроблено концепцію Національної системи обміну даних та блокування банківських карток (система «AntiFraud»), задіяних в шахрайських схемах.

За результатами робочої зустрічі з представниками юридичних та безпекових департаментів банківських установ та платіжних систем України досягнуто спільної позиції щодо необхідності запровадження такої системи

та заявлено про готовність приєднання до неї з боку провідних банків (що складають 80 відсотків банківського сектору України).

Як перспективний напрям планується розробка нормативно-правового акта, який забезпечить правову основу для функціонування Національної системи «AntiFraud» на період дії воєнного стану та 6 місяців після його закінчення.

Згідно цієї концепції вже зареєстрована інформація та відомості, зазначені потерпілим (номер карти, сума збитку, дата та час транзакції) надходить до системи «AntiFraud». Після чого вказана система автоматично направляє запит до банківських установ, де в свою чергу встановлюється факт транзакції та відстежується подальший рух коштів потерпілого до кінцевого рахунку/банківської картки, на яку були перераховані кошти правопорушником з одночасним блокуванням рахунку на вивід коштів. Отримавши зазначені відомості, банківська установа дає автоматичний припис через (API), іншим банкам отримувачам коштів, на блокування банківських рахунків шахраїв та грошових коштів, з яких здійснено обготівкування, терміном до 48 годин.

Враховуючи вище викладене, вважаємо за необхідне розробити в правоохоронних органах, насамперед в Національній поліції України, концепцію протидії онлайн-шахрайству через її профілактичну складову з використанням можливостей соціальних мереж, а також національних та регіональних ЗМІ, насамперед електронних, із залученням сервісів «ДІЯ» тощо.

Отже, заходи профілактики шахрайств у сфері е-комерції можуть здійснюватися різноманітними суб’єктами за різними напрямками, що найбільш ефективно сприятимуть виявленню причин та умов вчинення кримінальних правопорушень даної категорії, та впливатимуть на рівень запобігання ним.

3.3. Міжнародний досвід протидії шахрайствам у сфері е-комерції

Наразі кібершахрайство є глобальною міжконтинентальною проблемою, а розвиток світової електронної комерції зумовлює збільшення кількості шахрайств у даній сфері також у світовому масштабі.

Гармонізація кримінального законодавства про інтернет-шахрайства на міжнародному рівні, а також розробка і реалізація в національне законодавство міжнародних стандартів, що дозволяють ефективно розслідувати кримінальні правопорушення в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази, повинні входити до комплексної протидії інтернет-шахрайства [67, с. 131].

Саме тому важливий досвід зарубіжних країн, які мають великі успіхи у протидії шахрайствам у сфері е-комерції, та напрацювали успішну практику їх розслідування.

В контексті дослідження проблем протидії шахрайствам у сфері е-комерції, І. М. Пістунов також вважає, що варто вдатися до вивчення досвіду розвинутих зарубіжних країн у даній сфері [147, с. 33]. Натомість, О. І. Кривенко окремо відмічає, що однією із найбільших проблем протидії інтернет-шахрайствам є те, що дії по боротьбі з шахрайством мають певні відмінності в залежності від країни [91, с. 210].

Особливий інтерес викликає досвід США щодо запобігання шахрайства в е-комерції з метою розроблення універсальних механізмів ефективного запобігання кримінальним правопорушенням у даній сфері, вироблення яких надалі дозволить напрацювати концептуальні заходи державної політики щодо протидії шахрайствам, та створити програму дій для правоохоронних органів [83, с. 221]. У цій державі протидія досліджуваному виду злочинності покладена на Федеральне бюро розслідування, в складі якого створено Центр скарг на інтернет-злочинність. Вказаний Центр приймає інтернет-скарги про злочини від фактичної жертви або від третьої сторони в онлайн-режимі. Для подання скарги необхідно надати наступну інформацію: ім’я жертви, адреса,

телефон та електронна пошта; інформація про фінансові операції (наприклад, інформація про обліковий запис, дата здійснення операції та сума, що надійшли гроші); ім’я суб’єкта, адреса, телефон, електронна адреса, веб-сайт та IP-адреса; конкретні подробиці про те, як громадянин став жертвою злочину; заголовки електронної пошти; будь-яка інша важлива інформація, яку громадяни вважають необхідною для розгляду скарги. У той же час, на сайті ФБР постійно оновлюються списки найбільш розповсюджених видів інтернет-шахрайств, фізичних та юридичних осіб, які підозрюються або підозрювались у вказаних шахрайствах, способи убезпечення від інтернет-шахраїв, списки шкідливого програмного забезпечення на комп’ютерну та мобільну техніку [91, с. 210].

У результаті спільної роботи правоохоронних органів, представників електронного бізнесу, громадськості та науковців у США були формально створені усталені правила захисту інтернет-магазинів від різних видів шахрайств, які полягають у вживанні превентивних заходів та знижують ризик шахрайства у сфері електронної торгівлі, зокрема:

- регулярний аудит безпеки сайту;

- перевірка відповідності онлайн-магазину стандарту PCI DSS;

- регулярна перевірка сайту щодо підозрілої активності (у зарубіжних країнах склалася практика, що онлайн-магазини наймають співробітників для запобігання шахрайству. Захистити інтернет-магазин від шахрайських транзакцій можна завдяки активному відстежуванню підозрілої активності, а саме: крадіжки персональних даних або зламу аканту);

- використання служби перевірки адрес (AVS). AVS перевіряє: чи вказана клієнтом адреса виставлення рахунку відповідає самій адресі рахунку власника кредитної картки. Зазвичай автентифікація AVS використовується як частина багатошарової системи захисту від шахрайства, з метою гарантування затвердження дійсних транзакцій та відхилення тих, які вважаються підозрілими;

- використання кодів CVV2, CVC2 - захисного коду платіжних карток, який закодований у магнітній смузі. Цей код потрібний для того, щоб банк міг ідентифікувати клієнта при оплаті товарів та послуг карткою онлайн та офлайн;

- використання безпечного протоколу передачі гіпертексту (HTTPS) - протоколу, який забезпечує цілісність та конфіденційність даних при їх передачі між сайтом та пристроєм користувача, який передбачає три основні рівні захисту: 1) шифрування переданих даних; 2) цілісність даних; та 3) аутентифікацію, яка гарантує, що відвідувачі потраплять саме на сайт, який їм потрібен, окрім цього, захищає від атаки посередника;

- зберігання обмеженої кількості інформації;

- встановлення обмеження на кількість покупок та їх загальну вартість, які онлайн-магазин приймає з одного облікового запису протягом одного дня;

- перевірки, чи збігаються IP-адреса та адреса кредитної картки;

- використання програм для боротьби з шахрайством. Зазвичай, вони інтегровані в онлайн-кошики та платформи електронної комерції. Ці інструменти використовують алгоритми машинного навчання для виявлення шахрайських транзакцій за допомогою геолокації IP, перевірки адрес електронної пошти, проведення відбитків пальців пристрою та перевірки адрес. З даного питання, журнал Merchant Fraud склали список кращих платформ для запобігання шахрайству. Серед них: Kount, Riskified, Forter, Signifyd, ClearSale, CyberSource, Feedzai, Ravelin, Sift, Fraud.net, Nethone, Precognitive, SEON, FraudLabs Pro. Відповідні програми при оплаті автоматизують перевірки на шахрайство, здійснюють блокування підозрілих пристроїв, скасування шахрайських замовлень та багато іншого [83, с. 222].

Можна вважати позитивним досвідом й боротьбу з фішингом в США. У цьому розрізі слід зазначити, що Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків Safe Card, запустила проект із ліквідації

шахрайських сайтів [128; 38, с. 94; 165]. США на переконання ряду дослідників є державою, яка потерпіла чимало атак від кібершахраїв і є чи не найпершою в історії, що розробляла відповідні норми для регулювання злодіянь даного типу. Головними нормами Національної стратегії національної безпеки США, прийнятої у 2015 році, є ті, що встановлюють необхідність захисту від кібератак у кіберпросторі. США, що проголосили себе батьківщиною Інтернету, взяли на себе відповідальність забезпечення кібербезпеки у всьому інтернет-світі [145, с. 45].

В контексті даної проблематики слід зауважити, що досліджуючи досвід запобігання шахрайству у сфері е-комерції в США, ряд вчених вже виділяє першочергові завдання запобігання електронному комерційному шахрайству в Україні, серед них наступні:

- створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції та торгівлі, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв;

- запровадження політики належного корпоративного управління;

- упровадження дієвих законодавчих ініціатив щодо належного регулювання комерційної реклами та просування комерційних продуктів або послуг; встановлення кримінальної відповідальності за злом та крадіжку в мережі, знищення приватної та / або секретної інформації;

- реформування інституту кримінальної відповідальності за електронне торговельно-комерційне шахрайство;

- використання новітніх електронних систем та досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства;

- популяризації електронної комерції через он-лайн та оф-лайн магазини;

- посилення міжнародного співробітництва та залучення громадськості до соціально-виховної роботи з профілактики шахрайства в сфері електронної торгівлі [83, с. 222].

Серед європейських держав, згідно з даними статистики фінансового шахрайства, лідерами є Велика Британія і Франція, що несуть найбільші збитки від шахрайства [41]. Тому, досвід цих та інших європейських держав, які стикнулися з проблемами кібершахрайства, у тому числі й у сфері е-комерції, та віднайшли ефективні шляхи боротьби із ним, можна взяти за основу.

Слід зазначити, що для протидії кіберзлочинності ряд зарубіжних країн створили спеціальні органи, завданням яких є формування і реалізація політики у сфері кібербезпеки. Формування національної політики щодо забезпечення кібербезпеки здійснюють органи загальної компетенції або ж спеціально створені органи. Так, органами загальної компетенції є Комітет з питань безпеки Фінляндії, Центр захисту національної інфраструктури Великобританії, Управління національної безпеки Чехії, Національне управління з питань безпеки та контр тероризму, Міністерство адміністрації та впровадження цифрових технологій Польщі. У Франції діє Національна служба безпеки інформаційних технологій, у Великобританії функціонує Управління кібербезпеки та інформаційного забезпечення, у Австрії – Керівна група з кібербезпеки [146, с. 56].

Як показав аналіз міжнародного досвіду, в цілому, У ЄС значна увага приділяється проблематиці раннього виявлення й оперативного реагування на кіберінциденти та кібератаки проти електронних інформаційних ресурсів. Так, Стратегія кібербезпеки Європейського Союзу у поняття «кіберзахист» додає виявлення і блокування кібератак, локалізацію їх наслідків незалежно від походження стосовно цивільних об’єктів усіх форм власності, а також встановлення і розслідування кіберзлочинів. Водночас, Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA) забезпечує виконання функції виявлення і блокування кібератак, а також локалізації їх наслідків незалежно від походження стосовно цивільних об’єктів усіх форм власності. CERT-EU (Computer Emergency Response Team) – це структура, яка виявляє кібератаки

за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається CERT-EU. Якщо CERT-EU виявляє кібератаки з ознаками злочинних дій, то відповідна інформація передається до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, ECC), який, у свою чергу, може поінформувати про них Європейську агенцію оборони (European Defence Agency) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) [239; 167, с. 388].

Серед основних викликів ЄС в протидії кіберзлочинності також стало і поширення криптовалюти. Зловживання біткоїном досі є одним з основних факторів, що допомагають кіберзлочинності в Інтернеті (до прикладу, для покупки чи оренди інструментів для кібершахрайств), проте є і інші валюти, що орієнтовані на анонімність (Monero), і які від 2017 року все частіше використовуються в цифровому андеграунді. Зараз для вирішення цієї проблеми ЄС зокрема встановлює партнерські стосунки з біржами криптовалюти та платіжними системами та проводить щорічну конференцію з віртуальних валют. Одним з кроків на шляху вирішення цього виклику також став законопроект про регулювання криптовалют MiCA (Markets in Crypto Assets). Законопроект отримав підтримку багатьох країн ЄС, у тому числі і Франції. 5 жовтня 2022 року члени Ради ЄС підписали текст законопроекту, який зобов’язує всіх постачальників послуг криптоактивів дотримуватись чітких норм та вимог, що будуть спрямовані на захист споживачів [35, с. 113].

Франція орієнтується на те, щоб інформаційні системи були здатні протистояти подіям в кіберпросторі, які можуть негативно вплинути на доступність, цілісність і конфіденційність інформації. Франція робить ставку на технічні засоби захисту інформації, боротьбу з кіберзлочинністю і встановлення кіберзахисту [146, с. 56].

У Німеччині проглядається висока зацікавленість держави у стабільності бізнесу. Так, уряд Німеччини створив національні спецслужби для контролю за ситуацією на економічно важливих об'єктах країни. Як протидію впливам іноземних спецслужб, німці створюють на національному рівні контррозвідувальні підрозділі, які у взаємодії з приватними охоронно-детективними агентствами виконують функції безпеки як щодо фірми, так и щодо її керівництва, і окремо, щодо працівників та клієнтів. У зв'язку з цим на приватні агентства інколи покладають обов'язки здійснення окремих заходів оперативно-розшукової діяльності, що в умовах законодавства України категорично заборонено. Головним чином це отримання оперативно-значущої інформації про вчинені чи ті, що плануються, правопорушення як на фірмі, так и на загальнодержавному рівні. Причому населення Німеччині своїм громадянським обов'язком вважає поінформувати відповідні органи про правопорушення, що стали їм відомі, і отримують за це винагороду, сума якої може перевищувати сто тисяч євро [147, с. 38].

Ще одним напрямом транснаціональної злочинної діяльності є встановлення все більш тісних зв’язків з представниками корпоративного сектору в деяких країнах ЄС. Така взаємодія будується за трьома напрямами. По-перше, бізнес-структури, іноді навіть найбільші корпорації замовляють послуги у кіберзлочинців. Найбільшою мірою це стосується кіберзлочинності і пов’язане з крадіжкою інтелектуальної власності та компрометуючої конкурентів документації. По-друге, ОЗУ намагаються інвестувати злочинні прибутки в легальний бізнес. Особливий інтерес ОЗУ проявляють до: будівництва, прибирання міського сміття та проблем екології. Також злочинність інвестує в ІТ-індустрію, особливо у фінансові технології, виготовлення відеоігор і різного роду мобільних додатків, які передбачають отримання від клієнтів персональних даних [28, с. 300].

Усталеною практикою реагування на випадки шахрайства у міжнародних організаціях є залучення зовнішніх форензік експертів для

аналізу та розслідування таких випадків, а також розробки практичних рішень, що сприяють запобіганню, виявленню і ліквідації наслідків шахрайства. В Україні ж лише 3% респондентів за останні два роки мали такий досвід, порівняно з 20% респондентів у світі. Незважаючи на збільшення витрат на боротьбу з шахрайством, багато українських організацій все ще не займаються профілактикою шахрайства, а лише реагують або захищаються, коли факт шахрайства вже скоєний [43].

Отже, головною відмінністю процесу протидії шахрайствам, що вчиняються через мережу Інтернет між вітчизняною практикою та практикою Європейського Союзу й США є те, що у вказаних зарубіжних країнах діяльність досліджуваного виду, головним чином, спрямована на превенцію зазначених злочинів та роботу із населенням, а не на розслідування вже вчинених злочинів [91, с. 210].

Втім, як справедливо наголошують Н. А. Лугіна і А. М. Лучук, для того, аби мати змогу ефективно розслідувати кримінальні правопорушення пов’язані з віртуальним простором, необхідною є не тільки гармонізація законодавства, а й розробка відповідних механізмів міжнародної співпраці [106, с. 239].

На необхідності постійної міжнародної співпраці для боротьби із загрозою інтернет-шахрайства наголошує й К. С. Качашвілі. На його думку, контролювати кібершахрайство і боротися з ним на рівні окремої держави практично неможливо. Прийняття міжнародних норм і стандартів повинне супроводжуватись внесенням змін до національного законодавства держав. Головне ж завдання полягає в тому, щоб на міжнародному рівні, наприклад, в рамках ООН, розробити комплексну програму, що включатиме в себе всі можливі форми та методи боротьби з інтернет-шахрайством. Ці дії матимуть успіх лише в тому випадку, якщо будуть спиратися на систему постійного моніторингу інтернет-простору на міжнародному та національному рівнях. Відповідно, правоохоронні органи всіх держав повинні паралельно

здійснювати заходи по припиненню і попередженню таких шахрайств [67, с. 131].

Необхідним є поглиблення практичної складової міжнародного співробітництва з питань боротьби з кіберзлочинністю взагалі та кібершахрайством зокрема в частині оперативного обміну інформацією. Разом з тим, міжнародна співпраця повинна містити угоди про видачу кібершахраїв, надання взаємної правової допомоги та консультацій із роз'ясненнями змісту норм та кваліфікуючих ознак кримінальних правопорушень за національним законодавством. Необхідно активізувати процеси імплементації та гармонізації міжнародного законодавства та законодавчої бази України в інформаційній сфері. Важливим, як справедливо зауважує С. В. Шапочка, є обмін інформацією між оперативними підрозділами різних країн про багатоепізодні кібершахрайства, що вже вчинені чи готуються [218, с. 189].

Слід зазначити, що порядок міжнародного співробітництва щодо боротьби із шахрайствами, у тому числі у сфері е-комерції, ґрунтується на національних законодавчих та підзаконних актах, а також міжнародних угодах, обов'язковість яких підтверджено Верховною Радою України. При цьому, Конвенція про кіберзлочинність є первинною міжнародною угодою у сфері протидії кібершахрайствам.

Більше 50 країн, включаючи США, підписали Конвенцію ЄС про кіберзлочинність. Безліч країн визнали необхідність співпраці з іноземними державами для боротьби зі зростаючою небезпекою кіберзлочинності. Однією з кінцевих цілей Конвенції ЄС є «проведення в першочерговому порядку спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, зокрема, шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву». Україна також ратифікувала цю Конвенцію [193, с. 170].

Серед універсальних міжнародно-правових документів, окрім згаданої Конвенції, слід зазначити Довідник ООН із запобігання і контролю

злочинності, пов’язаної з комп’ютерами, 1995 рік; Конвенцію ООН проти транснаціональної організованої злочинності, 2000 рік. Одним із перших міжнародних документів у боротьбі з кіберзлочинністю є «Мінімальний список» правопорушень у цій сфері, прийнятий Європейським комітетом з проблем злочинності Ради Європи у 1990 році, який передбачав наступні злочини: комп’ютерне шахрайство, комп’ютерний підлог, пошкодження комп’ютерної інформації чи програм, комп’ютерний саботаж, несанкціонований доступ до комп’ютерних систем, несанкціоноване перехоплення інформації, несанкціоноване копіювання захищених комп’ютерних програм, незаконне виготовлення топографічних копій. Згодом ця класифікація злочинних посягань була скорегована Конвенцією 2001 року. З метою протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів країн світу такі злочини класифікуються за кодифікатором міжнародної кримінальної поліції Генерального Секретаріату Інтерполу, який з 1991 року інтегровано в автоматизовану систему пошуку, і сьогодні він доступний підрозділам Національних центральних бюро Інтерполу більшості країн світу, зокрема, й НЦБ Інтерполу МВС України [167, с. 388].

Міжнародне співробітництво України в європейському регіоні здійснюється також в рамках проектів і програм, реалізованих РЄ та ЄС. Наприклад, CyberCrime@EAP з проблем кіберзлочинності в рамках Програми Східного партнерства. Крім цього, Україна тісно співпрацює з іншими міжнародними організаціями, а саме Інтерполом і НАТО та ЄС. Особливо важливо гармонізувати законодавство України з актами ЄС в контексті сучасних євроінтеграційних процесів [237, с. 129].

Важливим є включення до Закону України «Про основні засади кібернетичної безпеки України» дозволу на здійснення транскордонної передачі інформації: «Інформацію з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, дотримуючись вимог законодавства України та її

міжнародно-правових зобов'язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може допомогти компетентним органам іноземної держави припинити кібератаку, своєчасно виявити і припинити кримінальне правопорушення з використанням кіберпростору» [237, с. 129].

Слід зазначити, що, відповідно до Закону України № 1906-V від 29.06.2004 року «Про міжнародні договори України», згода на обов'язковість яких надана Верховною Радою України, міжнародні договори є частиною національного законодавства і застосовуються у порядку, передбаченому для норм національного законодавства. Якщо міжнародним договором України, який набрав чинності в установленому порядку, встановлено інші правила, ніж ті, що передбачені у відповідному акті законодавства України, то застосовуються правила міжнародного договору (ст.19 Закону) [152].

Як зауважують В. О. Тімашов і Д. Ш. Діденко, виявити та затримати кіберзлочинців у країнах, де існує міжнародний договір чи угода, не є проблемою. Натомість, проблема полягає в тому, що деякі найпоширеніші кіберзлочини нині походять з країн, в яких немає взаємних домовленостей, таких як Північна Корея. Однак, якщо Сполучені Штати навмисно намагаються відслідковувати та знищувати відомих північнокорейських хакерів, дії Сполучених Штатів можуть бути виправдані принципом, що Сполучені Штати можуть здійснювати кримінальну юрисдикцію на основі наслідків у межах нації та захищати інтереси нації [193, с. 171].

Інтереси України, як члена Міжнародної організації кримінальної поліції представляють Департамент Інтерполу та Європолу Національної поліції України. Останні, в межах наданих їм повноважень реалізовують державну політику України по боротьбі зі злочинністю, яка має транснаціональні ознаки. Крім того, в своїй діяльності Департаменти здійснюють координацію, організацію та забезпечення співробітництва правоохоронних та інших органів державної влади України з компетентними

органами іноземних держав у сфері боротьби зі злочинністю з використанням можливостей Інтерполу та Європолу [45; 134; 138].

В контексті даної проблематики слід зазначити, що важливим елементом системи міжнародного співробітництва України у сфері боротьби з кібершахрайством є участь у двосторонніх договорах про взаємну правову допомогу з кримінальних питань.

Часто так трапляється, коли під час кримінального провадження суб'єкти цього кримінального правопорушення перебувають на території декількох держав [139]. А тому, ряд важливих аспектів з питань їх розслідування можливо з'ясувати, реалізувати лише за сприяння уповноважених посадових осіб компетентних органів держав-учасниць. Вказана взаємодія передбачає вжиття необхідних заходів з метою надання міжнародної правової допомоги шляхом вручення документів, виконання окремих процесуальних дій (допит свідка, потерпілого, експерта, повідомлення про підозру, проведення обшуку, огляду, вилучення речей, документів, арешту чи конфіскації майна, проведення інших процесуальних дій), видачі осіб, які вчинили кримінальне правопорушення, тимчасової передачі осіб, перейняття кримінального переслідування, передачі засуджених осіб та виконання вироків, але міжнародним договором України можуть бути передбачені й інші, ніж у КПК України форми співробітництва під час кримінального провадження (ст. 542 КПК). Вказане співробітництво, як правило ґрунтується на відповідних міжнародних актах з питань надання правової допомоги у кримінальних провадженнях ратифікованих державами-учасницями. А за відсутності таких правових актів, здійснюється на засадах взаємності, за якою одна держава, в рамках необхідності отримання правової допомоги у кримінальному провадженні, звертаючись до іншої держави та направляючи відповідний запит про це, письмово гарантує запитуваній стороні, що якщо у неї в майбутньому виникне така ж потреба розглянути її запит з надання правової допомоги. Згідно норм чинного КПК України вирішувати питання щодо надання дозволу з ініціювання, чи дозволу

з виконання запиту про міжнародну правову допомогу на засадах взаємності може лише Уповноважений (центральний) орган України, якого законодавець поділяє на трьох уповноважених суб'єктів, офіс Генерального прокурора та Міністерство юстиції України, і Національне антикорупційне бюро України (ст. 545 КПК) [129; 96].

Як показали матеріали судово-слідчої практики щодо шахрайства у сфері е-комерції, при розслідуванні таких кримінальних правопорушень у 29 % випадках також виникає потреба у зверненні до компетентних органів іншої держави з питань виконання окремих процесуальних дій, видачі осіб, які вчинили шахрайства у сфері е-комерції, тимчасової передачі таких осіб, перейняття кримінального переслідування тощо.

При цьому, у клопотанні про правову допомогу зазначається:

- компетентний орган іноземної держави та установи, допомога якого потрібна;

- кваліфікація та короткий виклад обставин справи;

- докладна інформація про підозрюваних осіб, які переховуються на території іншої держави;

- докладна інформація про свідків та потерпілих, які проживають на території держави, куди направляється запит, з якими необхідно провести процесуальні дії;

- що необхідно виконати і в чому полягає запит (зміст доручення).

Висновки до розділу 3

Констатуючи зазначене у розділі, підсумуємо викладений матеріал таким чином.

1. Тактичні операції є дієвим засобом оптимізації діяльності слідчого, що використовується для вирішення комплексу тактичних завдань.

Враховуючи поширеність вчинення таких шахрайств з місць позбавлення волі, особливу увагу приділено тактичній операції «злочинець – в'язень». Реалізація цієї тактичної операції здійснюється у тісній взаємодії слідчого, оперативних підрозділів Департаменту кіберполіції НПУ та співробітниками місць позбавлення волі (СІЗО, УВП). Важливими заходами для викриття шахрая, який діє в місцях позбавлення волі, є: проведення комплексу оперативних заходів, спрямованих на документування шахрайських дій оперативними підрозділами пенітенціарної служби; прослуховування телефонних переговорів шахрая із іншими особами та потерпілими в рамках НСРД; допит потерпілих; допити свідків; проведення особистих обшуків, у тому числі в камерах в'язня, з метою вилучення мобільних телефонів, планшетів, сім-карток мобільного зв'язку, чорнових записів, Wi-Fi–роутерів, інформації щодо банківських карток, аккаунтів потерпілих тощо; проведення обшуків за місцем проживання співучасників, які проживають на волі та надавали допомогу у вчиненні шахрайства; затримання організатора та учасників ЗУ та їх допити тощо.

Висвітлено тактичні заходи, що сприяють виявленню ознак, які свідчать про злочинну діяльність організованого угрупування у сфері е-комерції.

Виокремлено тактичні помилки, яких припускаються слідчі при проведенні тактичних операцій.

2. Об'єктивні та суб'єктивні фактори характеризують рівень протидії розслідуванню шахрайств у сфері е-комерції. Наголошено на суперечності між законодавчим та відомчим рівнями регулювання діяльності слідчих у сфері запобігання кримінальним правопорушенням, що потребує внесення в чинний КПК України положень, які б висвітлювали процедуру здійснення профілактичних заходів. Профілактична діяльність слідчого повинна бути необхідною складовою досудового розслідування кримінальних правопорушень, у тому числі й шахрайств у сфері е-комерції.

Виокремлено ряд причин та умов, що сприяють учиненню шахрайств у сфері е-комерції та запропоновано спеціальні заходи криміналістичної профілактики. Наголошено, що окремої уваги заслуговує використання можливостей інформаційних ресурсів самих правоохоронних органів, насамперед Національної поліції України, в якій створена та тривалий час функціонує система відділів комунікації, які співпрацюють з регіональними та всеукраїнськими ЗМІ, мають власні сайти, сторінки в соціальних мережах, виробляють власний аудіовізуальний контент, а також проявляють високу активність в інших засобах масової комунікації, в т.ч. в соціальних мережах та електронних ЗМІ. Як окрема складова концепції профілактики вчинення онлайн-шахрайств зазначено діяльність правоохоронців щодо моніторингу соціальних мереж та ЗМІ.

3. Кібершахрайство є глобальною міжконтинентальною проблемою, а розвиток світової електронної комерції зумовлює збільшення кількості шахрайств у даній сфері також у світовому масштабі. Підтримується думка провідних світових вчених щодо створення Єдиної інформаційної системи профілактики шахрайства у сфері електронної комерції, яка б поєднувала різноманітні інформаційні ресурси та бази даних про шахраїв у всьому світі тощо.

Є необхідною постійна міжнародна співпраця у боротьбі із шахрайством у сфері е-комерції, що ґрунтується на національних законодавчих та підзаконних актах, а також міжнародних угодах, обов’язковість яких підтверджено Верховною Радою України.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що виявляється в розробленні теоретико-прикладних засад методики розслідування шахрайства у сфері е-комерції, а також формулювання науково обґрунтованих практичних рекомендацій і пропозицій щодо їх розвитку й удосконалення з урахуванням міжнародного досвіду США і країн ЄС. В результаті дослідження сформовано низку теоретичних положень, висновків і практичних рекомендацій, основними з яких є такі:

1. Здійснено криміналістичний аналіз функціонування сфери е-комерції та визначено фактори, що зумовлюють учинення шахрайських дій. Динаміка звернень за фактами шахрайських дій у мережі Інтернет має стійку тенденцію до зростання, злочинна діяльність набуває все більш організованого й латентного характеру, а заходи протидії таким явищам не відповідають сучасним загрозам.

Комерційна діяльність із застосуванням комп'ютерних мереж й інтернет-технологій стрімко розвивається та приносить значні прибутки. Висока прибутковість комерційної діяльності є спонукальною основою для значної кількості зловживань і обернення чужих коштів на свій власний рахунок. Способи протиправного заволодіння коштами громадян з використанням автоматизованих систем банківських установ, соціальних мереж, електронної пошти дедалі змінюються й удосконалюються, набувають все більш прихованого характеру. Не без уваги сфера е-комерції залишилася й для ОГ, які, маючи корупційні зв'язки в органах державної влади й управління та правоохоронних органах, постійно удосконалюють схеми злочинної діяльності. Процеси діджиталізації економічних відносин «переводять» комерційну діяльність у віртуальний простір, де використовуються, поряд із традиційними технологіями, технології blockchain та інші інноваційні способи проведення фінансових операцій. Звідси шахрайства набувають міжрегіональний характер та характеризуються

високим рівнем анонімізації злочинців.

Однією з головних причин неефективності заходів з протидії шахрайствам залишається низький рівень обізнаності слідчих/дізнавачів та оперативних працівників щодо типових шахрайських схем та шляхів встановлення злочинців за цифровою слідовою картиною, особливостей доказування кіберзлочинів та ін.

Виокремлено основні фактори, що зумовлюють учинення шахрайств: недосконаліть законодавства у сфері е-комерції; відсутність контролюючого органу із захисту споживачів; невизначеність порядку здійснення електронних правочинів із застосуванням інформаційно-телекомунікаційних систем; недосконалий механізм збереження конфіденційності персональних даних; послаблення правоохоронних функцій в умовах запровадженого воєнного стану; набуття незаконної електронної комерційної діяльності організованого характеру.

2. Визначено сучасні наукові підходи до розуміння криміналістичної характеристики шахрайства у сфері е-комерції та основних її елементів, на підставі чого окреслено кореляційні зв'язки між ними. Система криміналістичної характеристики шахрайства складається з таких елементів: спосіб і слідова картина шахрайства, обстановка і умови, предмет посягання, особа злочинця і потерпілого.

Способи шахрайства у сфері е-комерції мають широкі межі та проявляються у системі взаємопов'язаних дій з підготовки, безпосереднього вчинення й приховування протиправних дій, які пов'язані між собою єдиним мотивом і метою. Охарактеризовано типові способи шахрайства і розподілено їх за групами: 1) здійснення електронних комерційних угод від імені фіктивного суб'єкта підприємницької діяльності або з використанням вкрадених кредитних карток чи проведення транзакцій з викраденими персональними даними; 2) шахрайські операції під час е-банкінгу; 3) шахрайське заволодіння персональними даними суб'єктів комерційної діяльності з подальшим переказом грошей на електронний гаманець;

4) шахрайські операції шляхом перенаправлення клієнтів у браузері на web-сайт шахраїв для здійснення комерційних угод; 5) шахрайські операції з обміном і обготівкування електронних грошових коштів між користувачами різноманітних платіжних систем; 6) шахрайські операції із встановленням мобільного додатку з обіцянкою виконання певних послуг (оформлення кредиту); 7) шахрайства у сфері волонтерської діяльності та благодійної допомоги, здійснюваної через мережу Інтернет; 8) шахрайські дії під приводом прийняття внесків як інвестицій у криптовалюту, управління фінансовими активами, надання інших фінансових послуг у мережі Інтернет; 9) шахрайства з цінними паперами; 10) шахрайські дії шляхом залучення коштів у віртуальні комерційні проекти з використанням технологій блокчейн; 11) фішингові атаки на комп'ютерні системи суб'єктів комерційної діяльності з подальшим вчиненням шахрайських дій та ін.

Визначено обстановку та слідову картину шахрайства**.** Обстановка здійснення шахрайських дій визначається умовами часу і місця, які переважно є «розмитими» та охоплюють значну кількість об'єктів, які можуть виступати місцями події. До обстановки шахрайства віднесено такі складові: 1) особливості нормативно-правового регулювання сфери е-комерції, що зумовили можливість здійснення шахрайських операцій; 2) час, протягом якого здійснювалися комерційні операції між суб'єктами; 3) час, коли наступили наслідки від протиправних дій внаслідок здійснення комерційних операцій в онлайн-просторі; 4) місце здійснення шахрайських дій (віртуальне середовище, в якому вчиняються шахрайства, і місця, де знаходяться точки доступу – IP-адреси), з яких здійснювався контакт між суб'єктами комерційних операцій) та ін.

З'ясовано, що крім матеріальних та ідеальних слідів, визначеній категорії шахрайств притаманна така група як віртуальні сліди (цифрові, електронні, комп'ютерні). Віртуальні (цифрові, електронні) сліди переважно містяться на таких носіях: електронні поштові скриньки, сайти, пам'ять комп'ютера або телефону, профілі соціальних мереж, криптовалютні пабліки,

бази даних операторів зв’язку та інтернет-провайдерів, флеш-носії, SIM-картки тощо.

Надано характеристику предмета злочинного посягання – товари, послуги, цінності, цінні папери (корпоративні акції, облігації, векселі, у тому числі електронні), гроші (у готівковій і безготівковій формах, криптовалюта), право на майно, інформація комерційного призначення та ін. Узагальнено криміналістично вагомі ознаки особи злочинця, на підставі чого сформовано ймовірний «портрет» шахрая. Визначено структуру ОГ та надано характеристику її учасникам. Виокремлено віктимогенні групи потерпілих.

3. Визначено основні напрями організації розслідування шахрайства у сфері е-комерції. **З**’ясовано особливості криміналістичного аналізу первісної інформації та визначення основних напрямів розслідування шахрайських дій. При внесенні інформації до інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» та ЄРДР потрібно максимально деталізувати обставини і способи вчинення правопорушень в сфері онлайн-шахрайств (місце вчинення, сайти, ресурси, фізичні об’єкти), зазначати дані про заявників, потерпілих, причетних чи підозрюваних осіб, ідентифікатори (номери телефонів, банківських карток, рахунків) та суми завданих збитків.

Залежно від слідчої ситуації, що склалася, запропоновано відповідні тактичні завдання: 1) встановлення механізму шахрайських дій; 2) підтвердження факту заволодіння майном чи правом на майно; 3) встановлення точок доступу, з яких здійснювалися шахрайські дії; 4) ідентифікація осіб, які здійснювали незаконні комерційні операції через електронні інформаційні системи і електроннікомунікаційні мережі; 5) встановлення усіх епізодів злочинної діяльності; 6) пошук свідків шахрайських дій; 7) відпрацювання електронних слідів, залишених під час розміщення об’яви на сайті, користування електронною скринькою; 8) відпрацювання мобільних контактів і зв’язків підозрюваного; 9) відпрацювання поштових і банківських переказів підозрюваного;

10) пошук документів (електронних) щодо комерційної діяльності суб'єктів господарювання; 11) вжиття заходів щодо запобігання протидії розслідуванню.

В межах тактичних завдань охарактеризовано особливості взаємодії слідчих з оперативними службами Департаменту кіберполіції (97 %), оперативними підрозділами Національної поліції (96 %), підрозділами Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ (7 %), підрозділами Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ (4 %), підрозділами у складі Департаменту оперативно-технічних заходів (92 %), оперативними підрозділами установ виконання покарань (37 %), суб'єктами, що забезпечують передачу і зберігання інформації з використанням інформаційно-комунікаційних систем(17 %), операторами мобільного зв'язку (51 %), банківськими працівниками (12 %) та ін.

4. Конкретизовано організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій.

Визначено тактику огляду. Виокремлено вузлові ділянки, де можуть бути зосереджені сліди шахрайських дій: 1) місце розташування call-центру; 2) локації розташування програмно-технічних засобів, що зазнали злочинного впливу; 3) місцезнаходження банкоматів, відділення банку, зони вільного підключення до мережі Інтернет з використанням технології Wi-Fi (кафе, інтернет-клуби) та ін.

Розкрито тактику обшуку. Наголошено на складнощах, що пов'язані з: 1) вилученням низки паперових і електронних документів; 2) предметів, які використовувалися для досягнення злочинного задуму; 3) комп'ютерної техніки і електронних носіїв інформації у приміщеннях підприємств, установ і організацій, а також комп'ютерних клубів, інтернет-кафе, банківських установах та ін. Охарактеризовано роль спеціаліста під час вилучення комп'ютерної техніки та її носіїв, а також необхідності подолання системи захисту, роботи з пристроями електроживлення, правильного копіювання

електронної інформації.

Особливу увагу приділено огляду електронної інформації, яка розміщена у відкритому доступі у мережі Інтернет або знаходиться на матеріальних носіях інформації чи хмарних сервісах зберігання електронної інформації.

Якщо є підстави вважати, що речі та документи будуть надані сторонами, у володінні яких вони знаходяться, у добровільному порядку, здійснюється тимчасовий доступ до речей та документів: 1) з банківських установ про власників банківських карток/рахунків, на які здійснювався переказ грошей потерпілих, місце зняття коштів та записи з камер відеоспостереження, встановлених у відділеннях банку або банкоматах. Якщо гроші перераховувались на інші рахунки, то IP-адреси користування web-банкінгом; 2) у операторів мобільного зв'язку щодо абонентських номерів мобільних телефонів та банківських установ (належність банківського рахунку, IP-адреси користування web-банкінгом, відеозапис зняття коштів у банкоматах, відділеннях банку). При особистому спілкуванні потерпілого з шахраєм засобами мобільного зв'язку, ініціюється звернення слідчого з клопотанням про тимчасовий доступ до інформації, що перебуває у володінні мобільного оператора, з метою встановлення IMEI мобільних терміналів, в яких працювала дана SIM-карта, місце виходу її на зв'язок та коло її інших абонентів.

Значну увагу приділено організації проведення НСРД: зняття інформації з електронних комунікаційних мереж (49 %) та електронних інформаційних систем (34 %), накладення арешту на кореспонденцію, її огляд та виїмка (25 %).

Зосереджено увагу на допиті потерпілого та окреслено основні його завдання: 1) отримання інформації для встановлення аккаунту (облікового запису) шахрая; 2) відображення URL-адреси на оголошенні (зробити скріншот або фотознімок); 3) з'ясування механізму спілкування потерпілого з шахраєм (особисте спілкування, за телефоном, у соціальних мережах або

мессенджерах); 4) встановлення контактної інформації про шахрая (номер карткового рахунку, електронного гаманця, телефону або електронної адреси). Рекомендовано до допиту потерпілого долучати: 1) зображення (скріншоти) переписки; 2) зображення безпосереднього змісту самого оголошення; 3) скріншоти сторінки, облікового запису шахрая у мессенджері, документу, що підтверджує сплату коштів; 4) виписку по банківському рахунку постраждалого із зазначенням платіжних систем, за допомогою яких здійснювалась транзакція. Такі виписки потерпілий може сформувати через системи онлайн-доступу (web-банкінг) до карткового чи електронного рахунку або отримати у відділенні банку роздруківку за своїм рахунком; 5) у разі, якщо потерпілий зробив аудіозапис розмови з шахраєм, долучити копію такого запису для отримання зразків голосу злочинця.

Виокремлено обставини, що підлягають з'ясуванню під час допиту потерпілого та свідка. Предмет допиту свідків формується, виходячи з наявної інформації, якою він володіє, та його відношення до розслідуваної події.

Розроблено найбільш ефективні тактичні прийоми допиту підозрюваного. Визначено безконфліктні й конфліктні ситуації допиту. Висвітлено специфіку допиту, що полягає в участі спеціалістів у галузі комп'ютерних технологій, комерційної та банківської діяльності, які допомагають слідчому сформулювати питання, виходячи з особливостей здійснення електронних комерційних проектів, сприяють вчасному виявленню хибної інформації. Розкрито тактику проведення одночасного допиту двох або більше раніше допитаних осіб.

5. Окреслено сучасні можливості використання спеціальних знань при розслідуванні шахрайства у сфері е-комерції. Виокремлено найбільш поширені форми використання спеціальних знань: використання консультативної допомоги спеціаліста (87 %), призначення і проведення судових експертиз (100 %), участь спеціаліста при проведенні СРД та інших процесуальних (98 %). Спеціаліст переважно залучається до проведення

таких процесуальних дій: допит, обшук, огляд, пред'явлення для впізнання у режимі відеоконференції, зняття інформації з електронних мунікаційних мереж та електронних систем, тимчасовий доступ до речей та документів, відібрання зразків для експертного дослідження.

Визначено коло осіб, яких доцільно залучати у якості спеціаліста при проведенні окремих СРД: 1) бухгалтери, економісти та інші особи, обізнані у комерційній діяльності; 2) дистриб'ютори, дилери та інші посередники, які допомагають доставити товар до споживача; 3) працівники банківських установ; 4) виробники товарів і послуг; 5) оператори послуг платіжної інфраструктури; 6) реєстратори, що присвоюють мережеві ідентифікатори; 6) постачальники електронних комунікаційних послуг;7) інші суб'єкти, що забезпечують передачу та зберігання інформації з використанням інформаційно-комунікаційних систем.

Акцентовано увагу на призначенні судових експертиз при розслідуванні шахрайства, де особливого значення набувають наступні їх види: технічна експертиза документів, почеркознавча експертиза, економічна експертиза, телекомунікаційна експертиза, трасологічна експертиза, комп'ютерно-технічна експертиза, експертиза відеозвукозапису, портретна експертиза та ін.

6. Сформовано типові тактичні операції при розслідуванні шахрайства у сфері е-комерції та розроблено оптимальний комплекс дій для їх проведення. Для збирання первинної інформації про обставини події, встановлення ознак шахрайства та відмежування його від інших правопорушень розроблено тактичні операції: «Незаконна транзакція», «Фіктивний комерсант», «Збирання вихідної інформації про шахрайство», «Встановлення ознак організованості», «Епізод».

Для встановлення осіб, які мають відношення до шахрайства, сформовано тактичні операції: «Ідентифікація особи у віртуальному просторі», «Встановлення IP-адреси», «Пошук та викриття шахрая», «Затримання», «Нейтралізація протидії розслідуванню», «Забезпечення

відшкодування матеріальних збитків». Для визначення структури ОГ і виявлення її лідера запропоновано тактичні операції – «Виявлення співучасників», «Встановлення корумпованих зв'язків» та ін.

З урахуванням слідчої практики надано перелік СРД, НСРД та інших процесуальних й розшукових заходів, необхідних для ефективного здійснення наведених тактичних операцій. Виокремлено тактичні помилки й прорахунки, яких припускаються слідчі під час проведення тактичних операцій.

7. Запропоновано перелік заходів профілактичної діяльності уповноважених осіб щодо виявлення й усунення причин та умов учинення шахрайства, зокрема: а) взаємодія Національної поліції з органами місцевого самоврядування, громадськими організаціями, закладами освіти, представниками бізнесу щодо виявлення осіб, схильних до антисуспільної поведінки у сфері використання комп'ютерних технологій та подальша їх постановка на облік кіберполіції; б) використання можливостей інформаційних ресурсів Національної поліції, де створена і функціонує система відділів комунікації, які співпрацюють з ЗМІ, мають власні сайти, сторінки у соціальних мережах, виробляють власний аудіовізуальний контент, проявляють високу активність в інших засобах масової комунікації, в т.ч. у соціальних мережах; в) діяльність правоохоронних органів щодо моніторингу соціальних мереж та ЗМІ; г) розміщення на сайті кіберполіції інформації, що надає можливість громадянам перевірити підозрілу інформації за такими параметрами: номер банківської картки, телефон або посилання на сайт. Зазначений напрям роботи кіберполіції має набути подальшого розвитку та інтегруватися у сервіси «ДІЯ» – мобільного застосунку, web-порталу; д) створення механізму оперативного реагування на шахрайські прояви через блокування активів комерційних об'єктів; е) використання можливостей різноманітних обліків та інформаційних баз даних щодо шахрайства в Інтернеті.

Наголошено на необхідності підвищення ефективності профілактичної діяльності уповноважених осіб у кримінальних провадженнях за фактами шахрайства, які полягають у внесенні змін до КПК України шляхом визначення їх обов'язку виявляти причини й умови, що сприяли учиненню кримінального правопорушення. Доведено необхідність обов'язкового внесення до відповідних державних органів, громадських організацій або посадових осіб подання стосовно вжиття заходів для усунення наведених умов та причин.

8. Охарактеризовано міжнародний досвід та особливості міжнародного співробітництва при розслідуванні шахрайства у сфері е-комерції. Враховуючи, що злочинна діяльність здебільшого має транснаціональний характер, проаналізовано досвід зарубіжних країн, зокрема США, Великої Британії та країн ЄС (Німеччина, Нідерланди, Франція, Іспанія), з протидії шахрайствам. Взаємодії правоохоронних органів України з іноземними компетентними органами при вирішенні задач міжнародного співробітництва у кримінальних провадженнях за фактами шахрайства властива низка факторів, що визначають ефективність такої взаємодії й впливають на кінцевий результат. Перебування суб'єктів шахрайських дій на території декількох держав зумовлює необхідність міжнародного співробітництва з правоохоронними органами та іншими компетентними особами інших країн з питань виконання окремих процесуальних дій (допитів, затримань, вилучення документів), видачі осіб, які вчинили шахрайства, тимчасової передачі таких осіб, перейняття кримінального переслідування. Порядок міжнародного співробітництва щодо протидії шахрайствам ґрунтується на національних законодавчих і підзаконних актах, а також міжнародних угодах, обов'язковість яких підтверджено Верховною Радою України. При цьому, Конвенція про кіберзлочинність є первинною міжнародною угодою у сфері протидії кібершахрайствам. Використання міжнародного досвіду є необхідним заходом, якого доцільно вживати з урахуванням національних особливостей, діючих надзвичайних правових режимів та економічного

потенціалу держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александренко О. В. Криміналістичні проблеми подолання протидії розслідуванню: дис. … канд. юрид. наук: спец. 12.00.09 / О. В. Александренко. Київ, 2004. 250 с.

2. Александренко О. В. Криміналістичні проблеми подолання протидії розслідуванню: автореф. дис. на здоб. наук. ст. к.ю.н. за спец. 12.00.09. Національна академія внутрішніх справ. Київ, 2004. 20 с.

3. Андронік О. Л., Воронін А. В. Можливості та загрози електронної комерції в Україні. *Економіка і організація управління.* № 4 (44). 2021. С. 118-130.

4. Антонюк О. А. Проблемні аспекти призначення експертиз при розслідуванні кримінальних правопорушень протии громадського порядку. *Науковий вісник публічного та приватного права*. 2017. Вип. 2. Т. 2. С. 231-236.

5. Ахтирська Н. М. Актуальні проблеми розслідування кіберзлочинів : навчальний посібник. Київ, 2018. 229 с.

6. Бакаянова Н. М., Кубаєнко А. В., Свида О. Г. Організація діяльності Національної поліції України та оперативних підрозділів: навчально-методичний посібник (для здобувачів вищої освіти денної форми навчання) Одеса : Фенікс, 2020. 251 с. URL: http://dspace.onua.edu.ua/ (дата звернення 21.08.2020 р.).

7. Березняк В. С. Запобігання шахрайству в Інтернеті. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2023. № 1. С. 190-196.

8. Березняк В.С. Основні напрями криміналістичної профілактики під час розслідування кримінальних правопорушень у сфері нерухомості. *Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики:*матер. Всеукр. наук.-практ. конф. (м. Дніпро, 17 жовт. 2020 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. С. 5-8.

9. Березняк В. С. Основні напрями використання спеціальних знань під час розслідування кримінальних правопорушень у сфері нерухомості. *Юридична наука*. 2020. № 6. С. 183-188.

10. Бишевець О. В. Використання спеціальних знань у доказуванні в кримінальних провадженнях. *Вісник кримінального судочинства*. № 2. 2015. С. 187-191.

11. Бишовець О. В., Романенко Т. В. Особа злочинця як елемент криміналістичної характеристики шахрайств, що вчиняються в мережі Інтернет. *Вісник кримінального судочинства.* 2016. № 1. С. 81–87.

12. Бідняк Г. С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

13. Бідняк Г. С. Використання спеціальних знань при розслідуванні шахрайств. дис. … канд. юрид. наук: 12.00.09 / Дніпропетровський державний університет внутрішніх справ, Дніпро, 2018. 254 с

14. Білоусов Ю. В., Черняк О. Ю. Цивільно-правовий статус споживача: у контексті адаптації національного законодавства до законодавства Європейського Союзу: монографія. Київ: Науково-дослідний інститут приватного права і підприємництва НАПрН України. 2010. 190 с.

15. Близько 75 % випадків світового шахрайства й витоків даних стосується електронної комерції: URL:https://tech.liga.net/ua (дата звернення 21.12.22 р.).

16. Борисова Л. В. Транснаціональні комп’ютерні злочини як об’єкт криміналістичного дослідження: дис. ... канд. юрид. наук: 12.00.09. Київ, 2007. 217 с.

17. Борідько О. А. Криміналістична профілактика як структурний елемент методики розслідування злочинів. автореф. дис. на здобуття наук. ступеня канд. юрид. наук / 12.00.09. Національний університет внутрішніх справ. Харків, 2005. 20 с.

18. Бородин В. С. Системный подход к организации взаимодействия органов досудебного следствия и дознания. *Ученые записки Таврического национального университета им. В. И. Вернадского*. 2011. Т. 24 (63). № 2. С. 237–245.

19. Бортник Н. П., Коваль М. М. Криміналістичні завдання початкового етапу розслідування катувань, що вчиняються співробітниками Національної поліції. *Порівняльно-аналітичне право*. 2018. № 1. С. 301–303.

20. Брисковська О. М., Пустовіт В. А. Організовані форми інтернет-шахрайства на сучасному етапі. *Вісник Запорізького національного університету*. *Юридичні науки.* № 4. Том 1. 2020. С. 219-225.

21. Бутузов В. М. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки: науково-практичний посібник. Київ, 2010. 245 с.

22. Варцаба В. М. Розслідування злочинів організованих злочинних груп. автореф. … дис. к.ю.н. 12.00.09 Національна юридична академія ім. Ярослава Мудрого. Харків. 2003. 20 с.

23. Волобуєв А. Ф. Проблеми методики розслідування розкрадань майна в сфері підприємництва. Харків : Вид-во ун-ту внутр. справ, 2000. 336 с.

24. Галаган В. І., Шум В. В Процесуальний порядок накладення арешту на кореспонденцію у кримінальному провадженні України: монографія, Київ, 2017. 168 с.

25. Глинська Н. В., Лобойко Л.М., Марочкін О. І. Концептуальні основи побудови сучасного кримінального процесу України: монографія: за заг. ред. О. Г. Шило. Харків: НДІ ВПЗ імені акад. В. В. Сташиса НАПрНУ, 2016. 264 с.

26. Головкін Б. М. Види злочинності. Журнал східноєвропейського права. 2015. № 18. С. 14–21. URL:

http://easternlaw.com.ua/wp-content/uploads/2015/08/golovkin_18.pdf (дата звернення: 11.11.2020).

27. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: монографія. Запоріжжя, 2003. 250 с.

28. Гребенюк М., Черняк А. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємство, господарство і право*. № 3. 2019. С. 297-303.

29. Гринько Л. П. Криміналістична алгоритмізація: окремі проблеми теорії та практики. *Правова позиція*. № 4 (25), 2019. С. 145-150.

30. Гукова І. А. Криміналістична характеристика та особливості розслідування шахрайства у сфері надання послуг із працевлаштування: дис. док-ра філос. (081 – Право). Дніпропетровський державний університет внутрішніх справ, Дніпро, 2021. 253 с.

31. Гула Л. Ф. Особливості розслідування злочинів, учинених організованими злочинними групами. *Науковий вісник Львівського державного університету внутрішніх справ*. Львів, ЛДУВС, 2015. Вип. 3. 170–180.

32. Гуріна Д. П. Завдання експертної профілактики. *Актуальні проблеми держави і права*. 2008. Вип. 44. С. 233.

33. Давиденко В. Тактика викриття неправдивих показань при розслідуванні економічних злочинів. *Зовнішня торгівля: економіка, фінанси, право.* 2019. № 1. С. 45-57.

34. Дараган В. В., Постулов Т. А. Щодо деяких проблем правового забезпечення взаємодії органів досудового розслідування та оперативних підрозділів кіберполіції під час протидії злочинам у сфері інтелектуальної власності. *Міжнародна та національна безпека: теоретичні та прикладні аспекти*: матеріали VII Міжнародної науково-практичної конференції (ДДУВС, 17.03.2023). С. 355-358.

35. 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.

36. Джевага С. В. Використання спеціальних знань органами досудового розслідування у протидії кіберзлочинності. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*: матеріали науково-практичної конференції. Харків, 2014. С. 105-107.

37. Довженко О. Ю. Основи методики розслідування кіберзлочинів: автореф. дис. … на здобуття наук. ступеня канд. юрид. наук / 12.00.09. Одеський державний університет внутрішніх справ, Одеса, 2019. 20 с.

38. Домінова І. В. Ризик шахрайства в умовах функціонування електронного банкінгу. *Науково-виробничий журнал «Бізнес-навігатор»*. Випуск 4-2 (43) 2017. С. 92-98.

39. Дрозд В. Окремі питання регламентації початку досудового розслідування в умовах проведення правової реформи. *Підприємство, господарство і право.* № 12. 2017. С. 268-272.

40. Дрозд В. Г. Організаційні і тактичні аспекти розслідування умисних тяжких тілесних ушкоджень: дис. … канд.. юрид. наук за спец. 12.00.09. Київ, 2009. 234 с.

41. Дубина М. В., Садчикова І. В., Середюк І. О. Концептуальні підходи до підвищення рівня безпечності банківського платіжного середовища України. URL: https://www.business-inform.net/export_pdf/business-inform-2020-3_0-pages-349_359.pdf.

42. Думчиков С. А., Лукічов В. В. Статистика фітингових інцидентів в Україні за 2021 рік. https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/34523/91970.pdf?sequence=2&isAllowed=y (дата звернення 21.09.22 р.).

43. Економічні злочини та шахрайство: досвід українських організацій. URL: https://www.epravda.com.ua/columns/2020/12/17/669308/ (дата звернення 02.02.3023 р.).

44. Електронна комерція в Україні. URL: http://dspace.nlu.edu.ua/bitstream/123456789/12748/1/Ivanova_134-155.pdf. (дата звернення: 25.03.2023 р.).

45. 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. (дата звернення 21.03.2023 р.).

46. Єфімов М. М., Павлова Н. В., Чучко С. В. Павлова Н.В. Методика розслідування шахрайств, пов'язаних із купівлею-продажем товарів через мережу Інтернет: теоретичні та праксеологічні засади: монографія: Київ : Видавничий дім «Гельветика», 2022. 202 с.

47. Жилін А., Шевчук О. Метод аналізу фітингових повідомлень. *Information Technology and Security.* January-June 2022. Vol. 10. Iss. 1 (18). С. 72-82.

48. Жилін А. Е. Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері використання банківських електронних платежів: дис. … канд. юрид. наук (доктора філософії) / 12.00.09. Науково-дослідний інститут публічного права; Дніпропетровський державний університет внутрішніх справ, Київ, 2023. 227.

49. Журавель В. А. Тактичні завдання та механізм їх вирішення. *Теорія та практика судової експертизи і криміналістики.* Випуск 17. 2017. С. 11-18.

50. Завидняк В. І., Пушина Н. Л. Особливості початкового етапу досудового розслідування кримінальних правопорушень, вчинених у сфері господарської діяльності з використанням комп'ютерних технологій. *Порівняльно-аналітичне право*. № 2. 2020. С. 198-201.

51. Завидняк І. О. Планування і взаємодія слідчого з оперативними підрозділами під час розслідування злочинів, пов'язаних з незаконним обігом підакцизних товарів. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 3-4. С. 205–212.

52. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою: дис. док-ра філос. 081 – Право. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом, Київ, 2021. 246 с.

53. Захарова Г. В. Теоретичні засади методики розслідування шахрайства у сфері туризму, вчиненого організованою групою: автореф. дис. на здобуття наук. ступеня канд.юрид. наук / 12.00.09. ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», Київ, 2021. 20 с.

54. Захарова Г. В. Провадження обшуку та тимчасового доступу до речей та документів при розслідуванні кримінальних правопорушень у сфері нерухомості. URL: https://nvppp.in.ua/vip/2019/2/tom_3/13.pdf. (дата звернення 21.03.2023 р.).

55. Заяць К. Д. Особливості сучасних форм вчинення шахрайства та їх криміналістичне значення. *Підприємство, господарство і право*. № 11. 2017. С. 207-210.

56. Заяць К. Д. Про особливості окремих елементів механізму чинення шахрайств. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка*. 2017. № 4 (80). С. 233-239.

57. Здоровко С. Ф. Тактичні операції при розслідуванні вбивств, що вчиняються організованими групами і злочинними організаціями: автореф. автореф. дис… канд. юрид. наук.: 12.00.09 / НЮА ім. Ярослава Мудрого. Харків, 2002.18 с.

58. Івакін Е. О. Теоретичні та методичні питання не ідентифікаційних досліджень в судовому почеркознавстві дис. … канд. юрид. наук: 12.00.09 / Національна академія внутрішніх справ, Київ, 2002. 188 с.

59. Іванчишин І. І. Наукові підходи щодо визначення поняття та ознак організованого злочинного угруповання. *Право і суспільство*: Науковий журнал. 2015, № 5-2. С. 171-175.

60. Казаренко М. С. Про тактичні операції у структурі розслідування економічних злочинів. *Право і безпека*. 2005. С. 73-75.

61. Как распознавать различные виды фишинговых атак // vps.ua : сайт. 13.11.2017. URL: https://vps.ua/blog/how-to-identify-phishing-attacks/ (дата звернення: 27.10.2021).

62. Калюга Т. О. Розслідування шахрайства у сфері надання туристичних послуг: дис ... канд. юрид. наук, спец.: 12.00.09. Київ : МАУП, 2019. 264 с.

63. Калюга Т. О. Особливості участі спеціаліста в огляді документів під час розслідування шахрайства у сфері надання туристичних послуг. *Актуальні питання теорії та практики криміналістичної науки*: матеріали наук.-практ. семінару (м. Дніпро, 16 трав. 2018 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. С. 182–186.

64. Калюга Т.О. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайства, пов'язаного з наданням туристичних послуг. *Науковий вісник Ужгородського національного університету.* Серія «Право». 2017. Випуск 43. Т. 4. С. 184–189.

65. Карпенко М. Ю. Електронна комерція: конспект лекцій для студентів усіх форм навчання першого (бакалаврського) рівня вищої освіти спеціальності 073 – Менеджмент /; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2021. 146 с.

66. Каткова Т. В. Проблеми реалізації принципу безпосередності дослідження доказів на досудовому слідстві: автореф. дис... канд. юрид. наук: 12.00.09 / НЮА ім. Я. Мудрого. Харків, 1997. 18 с.

67. Качашвілі К. С. Проблема інтернет-шахрайства в Україні та способи боротьби із ним. URL: http://dspace.puet.edu.ua/bitstream/123456789/9520/1/%D0%9A%D0%B0%D1%87%D0%B0%D1%88%D0%B2%D1%96%D0%BB%D1%96%20%D0%9A.%D0%A1..pdf (дата звернення 10.03.2022 р.).

68. Кіберполіція викрила шахрайський call-центр, працівники якого спустошували рахунки іноземних громадян: URL: https://www.npu.gov.ua/news/kiberpolitsiya-vikrila-shakhrayskiy-call-tsentr-pratsivniki-yakogo-spustoshuvali-rakhunki-inozemnikh-gromadyan (дата звернення 12.04.2023 р.).

69. Книженко С. Криміналістична профілактика злочинів проти правосуддя. *Вісник Національної академії прокуратури України.* № 1 (39). 2015. С. 74-78.

70. Коба В. Б.Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право*. 2020. № 2 (68). С. 303–307.

71. Коба В. Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

72. Коба В. Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

73. Коба В. Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

74. Коба В. Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

75. Коба В. Б. Е-комерція – як об’єкт криміналістичного дослідження: ґенеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

76. Коба В. Б. Значення тактичних завдань для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

77. Коба В. Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56

78. Коба В. Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі :матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

79. Коба В. Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування :матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36

80. Коваленко А. В. Особливості тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров’я журналіста. *Вісник Національної академії правових наук України.* № 1 (88) 2017. С. 182-191.

81. Колеснікова І. А., Демидова Є. Є., Домашенко О. М., Латиш К. В. Профілактика експертних помилок під час дослідження цифрових фотозображень. *Юридичний науковий електронний журнал*. № 6/2022. С. 427-429.

82. Коновалова В. Е. Организационные и психологические основы деятельности следователя. Київ: РИО МВД УССР, 1973. 122 с.

83. Коновалова І. О. Досвід запобігання шахрайству в сфері електронної торгівлі в США. *Науковий вісник Ужгородського Національного Університету*. 2021. С. 220-224.

84. Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности : монография. Харьков: Изд-во Нац. ун-та внутр. дел, 2002. 412 с.

85. Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи: автореф. дис. … на здобуття наук. ступеня канд. юрид. наук / 12.00.09. Харківський національний університет внутрішніх справ. Харків, 2017. 20 с.

86. Коршикова Т. В. Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки: дис. док-ра філософії. 081 (Право). Національна академія внутрішніх справ, Київ, 2021. 255 с.

87. Костецька Т. А. Актуальні проблеми державно-правового регулювання інформаційних відносин. *Часопис Київського університету права*. 2006. № 4. С. 63–68.

88. Кравченко В.С., Руденко О.В., Доманов І.О., Казначей С.М. Аналіз фішинг – атак. Дослідження методів запобігання та захисту. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2022. Вип. № 1(11). С. 85-95.

89. Краморенко Н. Правові аспекти електронної комерції в контексті світового досвіду. *Наука молода*. № 10, 2008 р. С. 77-81.

90. Краус К. М., Краус Н. М., Манжура О. В. Електронна комерція та Інтернет-торгівля: навчально-методичнийпосібник. Київ. АграрМедіаГруп, 2021. 454 с.

91. 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 (дата звернення 21.03.2023 р.).

92. Кривопуск О. Г. Слідова картина як елемент криміналістичної характеристик злісного невиконання обов'язків по догляду за дитиною або за особою, щодо якої встановлена опіка та піклування. *Юридичний науковий електронний журнал*. № 12/2022. С. 450-453.

93. Криміналістика: підручник / за заг. ред. Є.В. Пряхіна. Львів, 2016. 948 с.

94. Криміналістичне документознавство: Практичний посібник / В. В. Бірюков, В. В. Коваленко, Т. П. Бірюкова, К. М. Ковальов; за заг. ред. В. В. Бірюкова. Київ: Вид. ПАЛИВОДА А.В., 2007. 332 с.

95. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/4651-17. (дата звернення 14.05.2023 р.).

96. Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 14.05.2023 р.).

97. Криушенко Л. І. Особливості виявлення обставин, що підлягають з'ясуванню під час розслідування шахрайства в банківській сфері. *Науковий вісник Ужгородського національного університету*. 2016. Вип. № 39 (2). С. 94–99.

98. Кузьменко О. В. Особливості криміналістичної характеристики кіберзлочинів. *Актуальні проблеми вітчизняної юриспруденції.* № 4. 2022. С. 162-166.

99. Кузьменко С. С. Розслідування шахрайства, пов'язаного з інвестуванням коштів у будівництво об'єктів нерухомості: дис. ... канд. юрид. наук. 12.00.09 / Дніпр. держ. ун-т. внутр. справ. Дніпро, 2019. 270 с.

100. Кун Д. Е. Особенности обеспечения прав участников следственных действий. *Общество: политика, экономика, право*. 2017. № 4. С. 101–103. DOI: https://doi.org/10.24158/pep.2017.6.19. (дата звернення 21.03.2023 р.).

101. Курман О. В. Криміналістична характеристика несанкціонованого втручання у роботу електронно-обчислюваних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'зку. *Наук. вісн. Херсон. держ. ун-ту. Серія «Юрид. науки»*. Вип. 4. Т. 2. 2017. С. 127–130.

102. Курман О. В. Тактичні та організаційні особливості початку досудового розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. № 4. 2019. С. 303-308.

103. Ларин В. В., Лебедев А. Н., Соловяненко Н.И. Правовое регулирование заключения сделок на современном этапе. URL: www.vlarin.chat.ru/larin/diplom.htm (дата звернення: 25.02.2023 р.).

104. Лефтеров Л. В. Загальносоціальні заходи запобігання шахрайству,що вчиняється шляхом застосування засобів електронних комунікацій. *Публічно-правовий дискурс у контексті глобалізації*. № 1. (15). 2019. С. 89-101.

105. Лисиченко В. К. Криминалистическая техника. Криминалистика / под ред. В. П. Колмакова. Киев: «Вища школа», 1973. 512 с.

106. 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.

107. Лукашевич В. Г. Криминалистическая теория общения: постановка проблемы, методика исследования, перспективы использования. Киев: Украинская академия внутренних дел, 1993. 194 с.

108. Луцик В. В. Зняття інформації з електронних інформаційних систем.URL:file:///C:/Documents%20and%20Settings/User/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/vchfo_2014_4_25.pdf (дата звернення16.07.2020 р.).

109. Маковоз О. С., Передерій Т. С. Шляхи вирішення забезпечення безпеки у сфері електронної комерції Україні: URL: https://univd.edu.ua/general/publishing/konf/24-25_05_2019/pdf/80.pdf (дата звернення 21.02.23 р.).

110. Малютин А. А. Електронна комерція та її роль у сучасній економіці. *Економіка та суспільство*. 2016. № 12. С. 177-181. URL: https://readera.org/jelektronnaja-kommercija-i-ee-rol-v-sovremennoj-jekonomike140117509 (дата звернення: 26.06.2022).

111. Малярова В.О. Розслідування злочинів проти моральності у сфері статевих стосунків: теорія та практика: монографія / за ред. д-ра юрид. наук, чл.-кор. НАПрН України С.М. Гусарова. Харків: Диса плюс, 2013. 422 с.

112. Матеріали кримінального провадження ВПК в Херсонській області за 2021 рік.

113. Матеріали кримінального провадження ВПК у Вінницькій області за 2021 рік.

114. Мельник О. В. Електронна комерція як складова частина електронного бізнесу. Рубрика: Сучасні інформаційні технології URL: http://intkonf.org/melnik-ov-elektronnakomertsiya-yak-skladova-chastina-elektronnogo-biznesu/ (дата звернення: 27.02.2023 р.).

115. Міжнародний досвід правового регулювання електронної комерції. URL: https://ru.osvita.ua/. (дата звернення: 26.04.2023 р.).

116. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій: дис… канд. юрид. наук: 12.00.09 / Академія праці і соціальних відносин Федерації профспілок України. Київ, 2005. 221 с.

117. Мусієнко О. Л. Теоретичні засади розслідування шахрайства в сучаснихумовах: монографія / О. Л. Мусієнко ; за ред. проф. В. Ю. Шепітька. Харків: Право, 2009. 168 с.

118. Навроцький В. О. Основи кримінально-правової кваліфікації. 2-ге вид. Київ: Юрінком Інтер, 2009. 511 с.

119. Найдьон Я. Поняття та характеристика віртуальних слідів кіберзлочинів. *Підприємство, господарство і право*. № 5. 2019. С. 304-307.

120. Недзельська Г. В. Спеціально-кримінологічні заходи запобігання шахрайства, що вчиняється організованою групою. *Юридичний науковий електронний журнал*. № 3. 2022. С. 211-213.

121. Неділько Я. В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право. Юридичні і політичні науки*. 2020. Вип. 88. С. 202-211.

122. Неділько Я. Обстановка та «слідові картина» як елементи криміналістичної характеристики розслідування кіберзлочинів. *Підприємство, господарство і право*. № 7. 2020. С. 359-364.

123. Олішевський О. В. Організація розслідування злочинів та її місце у структурі криміналістики : автореф. дис. на здобуття наук. ступ. канд. юрид. наук / 12.00.09. Харківський націон. ун-т внутр. справ. Харків, 2010. 20 с.

124. Омельян О. С. Поняття та ознаки цифрових слідів, що утворюються під час вчинення кіберзлочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 457-466.

125. Опанасенко Н. О. Криміналістична характеристика та основні положення розслідування шахрайства, вчиненого організованими злочинними групами у сфері житлового будівництва: автореф. дис. ... канд. юрид. наук. 12.00.09. Академія адвокатури України. Київ, 2018. 20 с.

126. Організація розслідування фактів несанкціонованого переказу коштів з рахунків клієнтів банку, які обслуговуються за допомогою систем дистанційного обслуговування: Методичні рекомендації / В. В. Корнієнко, В. І. Стреляний. Харків, 2015. 71 с.

127. Орехова Т. В., Дубель М. В. Вплив процесу діджиталізації на розвиток електронної комерції в Україні. *Економіка і організація управління*. № 4 (32). 2018. С. 17-25.

128. Офіційний сайт Української міжбанківської асоціації платіжної системи ЄМА. URL: https://ema.com.ua/fraud-digest-25-07-2017/ (дата звернення 21.03.2023 р.).

129. 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.

130. Павлова Н. В. Важливість дотримання прав і свобод особи під час проведення обшуку при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2021. № 1. С. 278-282.

131. Павлова Н. В. Основні профілактичні заходи при розслідуванні кримінальних правопорушень, вчинених шляхом шахрайства. *Науковий вісник Луганського державного університету внутрішніх справ*. 2023. № 1. С. 288-298.

132. Павлова Н. В. Особливості розслідування шахрайства, пов'язаного з відчуженням приватного житла: дис. … канд. юрид. наук: 12.00.09 / Дніпроп. держ. ун-т внутр. справ. Дніпро, 2007. 223 с.

133. Павлова Н. В. Роль спеціаліста у технічному забезпеченні проведення слідчих (розшукових) дій. *Кібербезпека в Україні: правові та організаційні питання*: матеріали міжнар. наук.-практ. конф., (м. Одеса, 22 листоп. 2019 р.). Одеса : ОДУВС, 2019. С. 64-65.

134. Павлова Н. В., Федченко В. М. Генеральная прокуратура Украины как субъект международного сотрудничества: особенности полномочий в сфере уголовного судопроизводства. *Legeasi Viata: международный научно-практический правовой журнал.* 2016. № 7. С. 86-93.

135. Павлова Н. В. Приводи та підстави для відкриття кримінального провадження щодо шахрайства / матеріали круглого столу. *Актуальні питання досудового розслідування*. (м. Кривий Ріг, 28 квіт. 2023 р.). Кривий Ріг, Донецький державний університет внутрішніх справ. 2023. С.30-33.

136. Павлова Н. В., Птушкін Д. А., Чаплинський К. О. Теоретичні засади методики розслідування шахрайства, пов’язаного з відчуженням об’єктів нерухомого майна громадян : монографія. Дніпро : Дніпропетровський державний університет внутрішніх справ; Херсон: Видавничий дім «Гельветика», 2019. 190 с.

137. Павлова Н. В. Роль і місце юридичної освіти в професійній діяльності слідчих. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 3. С. 190-196.

138. Павлова Н. В., Федченко В. М. Особенности полномочий офиса Генерального прокурора Украины во время уголовного производства в рамках международного сотрудничества / *Профессиональная подготовка кадров для подразделений Министерства внутренних дел и других правоохранительных органов:* матер. Междунар. науч.-практ. конф. (04 декаб. 2020 г.) / Академия «Штефан чел Маре» МВД Республики Молдова, 2020.С. 304-310.

139. 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.

140. Пазинич Т. А. Криміналістична характеристика шахрайств та основні положення їх розслідування: дис... канд. юрид. наук: 12.00.09 / Харківський національний університет внутрішніх справ. Харків, 2007. 211 с.

141. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж: автореф. дис… на здобуття наук. ступ. канд.. юрид. наук. 12.00.09 / Академія прокуратури. Київ. 2005. 21 с.

142. Парфило І. В. Обстановка скоєння злочину як системоутворюючий елемент криміналістичної характеристики фальсифікації та обігу фальсифікованих лікарських засобів. *Національний юридичний журнал:теорія та практика*. 2018. С. 197-202.

143. Пахомов Ю. Н. та ін. Національні економіки в глобальному конкурентному середовищі / Київ, 1998. С. 120-122.

144. Пашнєв Д. В. Використання спеціальних знань при, розслідуванні злочинів вчинених із застосуванням комп'ютерних технологій. дис. … канд. юрид. наук: 12.00.09 / НАВС. Київ, 2007, 228 с.

145. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 45-46

146. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений*. № 12/1. 2019. С. 55-59.

147. Пістунов І. М. Безпека електронної комерції: навч. посібн. / І. М. Пістунов, Є. В. Кочура ; Нац. гірн. ун–т. Електрон. текст. дані. Д. : НГУ, 2014. 125 с.

148. Погорецький М. А. Початок досудового розслідування: окремі проблемні питання. *Вісник кримінального судочинства*. № 1. 2015. С. 93-103.

149. Полуніна Л. Особливості проведення тактичних операцій при розслідуванні злочинів, пов'язаних із посяганням на відомості, що становлять комерційну або банківську таємницю. *Національний юридичний журнал: теорія і практика.* 2019. С. 161-165.

150. Правила продажу товарів на замовлення та поза торговельними або офісними приміщеннями: затв. наказом Міністерства економіки України від 19.04.2007 № 103: http://zakon. rada.gov.ua/laws/show/z1181-07. (дата звернення 21.03.2023 р.).

151. Про електронну комерцію: Закон України від 03.09.2015 № 675-VIII. URL: https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення: 25.06.2022 р.).

152. Про міжнародні договори України: Закон України від 29 червня 2004 року № 1906-IV URL: https://zakon.rada.gov.ua/laws/show/1906-15 (дата звернення 16.11.2018 р.).

153. Про призначення та проведення судових експертиз та експертних досліджень: Інструкція, затв. наказом М-ва юстиції від 08.10.1998 №53/5 (у ред. наказу М-ва юстиції України від 26.12.2012 №1950/5). URL: http://zakon5.rada.gov.ua/laws/show/z0705-98/ (дата звернення 21.03.2023 р.).

154. Профілактична діяльність слідчого при розслідуванні злочинів: Лекція для всіх форм навчання / уклад. А. Ф. Волобуєв. Харків: НУВС, 2003. 24 с.

155. Птушкін Д. А. Розслідування шахрайства, вчиненого щодо об'єктів нерухомого майна громадян: дис. ... канд. юрид. наук: 12.00.09 / МВС України, Дніпр. держ. ун-т. внутр. справ. Дніпро, 2018. 240 с.

156. Пчеліна О. В. Тактичні операції під час розслідування злочинів у сфері службової діяльності. *Підприємство,господарство і право*. № 3. 2017. С. 290-294.

157. Пчеліна О. В. Особливості предмета доказування у кримінальних справах про економічні злочини та їх вплив на методику розслідування: дис. ... канд. юрид. наук: спец. 12.00.09. Харків, 2010.

158. Пчеліна О. В. Використання спеціальних знань у галузі економіки під час розслідування злочинів у сфері службової діяльності. *Часопис Національного університету «Острозька академія». Серія «Право».* 2014. № 2 (10).

159. Ревака В. М. Форми використання спеціальних пізнань в досудовому провадженні: дис. ... канд. юрид. наук: 12.00.09 / Національна юридична академія України імені Ярослава Мудрого. Харків, 2006. 214 с.

160. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції: автореф. дис. … канд. юрид. наук / 12.00.09. Дніпропетровський державний університет внутрішніх справ, Дніпро, 2023. 20 с.

161. Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції: дис. … канд. юрид. наук / 12.00.09. Дніпропетровський державний університет внутрішніх справ, Дніпро, 2023. 253 с.

162. Рейнгольд А. В. Проблемні питання організації взаємодії органів і підрозділів Національної поліції України при розслідуванні шахрайства в інтернет-комерції. *Актуальні питання теорії та практики криміналістичної науки :* матер. наук.-практ. семінару (м. Дніпро, 16 трав. 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. С. 211–214.

163. РейнгольдА. В. Криміналістична профілактика у провадженнях за фактами вчинення шахрайства в інтернет-комерції. *Науковий вісник публічного та приватного права*. 2021. Випуск 2. Том 2. С. 188–193.

164. Романенко Т. В. Особливості слідової картини шахрайств, що вчиняються в мережі Інтернет. *Молодий вчений*. 2016. № 1 (28). Ч. 2. С. 51–54 (дата звернення 11.03.2023 р.).

165. Сабадаш В. П. Шахрайство в електронній комерції: реалії сьогодення. *Вісник Запорізького національного університету.* № 1. 2011. С. 216-220.

166. Савчук Т. І. Особливості планування допиту підозрюваних у вчиненні комп'ютерних злочинів. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*: матеріали науково-практичної конференції. Харків, 2014. С. 105-107.

167. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету*. № 64. 2021. С. 386-391.

168. Салтевський М.В. Криміналістика. Підручник: У 2 ч. Харків : Консум, 2001. Ч. 2. 478 с.

169. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 112 с.

170. Самойленко О. А. До питання оцінки слідчим матеріалів первинної перевірки оперативної інформації про злочин, вчинений у кіберпросторі. *Науковий юридичний журнал*. № 7. 2019. С. 145-151.

171. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет»: автореф. дис. канд. юрид. наук.: 12.00.09. Донецький юридичний інститут. 2014. 18 с.

172. Світличний В. А., Петров К. Е. Від ідентифікації комп'ютера до ідентифікації користувача в мережі Інтернет. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності*: матеріали науково-практичної конференції. Харків, 2014. С. 105-107.

173. Сіренко О. В. Обстановка вчинення крадіжок, грабежів і розбійних нападів неповнолітніми як елемент криміналістичної характеристики. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2012. № 4 (59). С. 223-228.

174. Смоков С. М., Десятник А. А. Окремі питання запровадження профілактичної діяльності під час досудового розслідування. *Вісник кримінального судочинства.* 2015. № 1. С. 111–118.

175. Смушкин А. Б. Виртуальные следы в криминалистике. *Законность.* 2012. № 8. С. 43–45.

176. Соколов О. В. Виконання оперативними підрозділами доручень слідчого, прокурора про проведення негласних слідчих (розшукових) дій : дис. ... канд. юрид. наук: 12.00.09. Харків, 2019. 231 с.

177. Сорочан А. В. Організація та планування розслідування шахрайства, що вчиняється на первинному ринку нерухомості. *Юридична наука*. № 2(104)/2020. С. 454-461.

178. Способи шахрайства в електронній комерції : URL:https://fondy.ua/uk/blog/ways-of-fraud-in-e-commerce (дата звернення 12.02.2023 р.).

179. Справа № 344/15443/21: Вирок Івано-Франківського міський суду Івано-Франківської області. URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 11.03.2023 р.).

180. Справа № 405/945/19: Ухвала Ленінського районного суду м. Кіровограда. URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 11.03.2023 р.).

181. Справа № 554/12566/15-к: Ухвала Октябрського районного суду м. Полтави . URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 12.02.2023 р.).

182. Справа № 686/7672/18: вирок Хмельницького міськрайонного суду Хмельницької області 19» листопада 2018 року: URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 12.02.2023 р.).

183. Справа № 686/7672/1819»: Вирок Хмельницького міськрайонного суду Хмельницької області від листопада 2018 року: URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 12.02.2023 р.).

184. Справа № 760/6919/16-к: Ухвала Солом`янського районного суду м. Києва. URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 12.02.2023 р.).

185. Справа № 363/1435/16-к: Ухвала Вишгородського районного суду Київської області. URL: https://reyestr.court.gov.ua/Review/57206134 (дата звернення 12.02.2023 р.).

186. Степанюк Р. Л. Теоретичні засади методики розслідування злочинів, вчинених у бюджетній сфері : дис. ... д-ра юрид. наук; спец. 12.00.09 / Р. Л. Степанюк. Х. :Харк. нац. ун-т внутр. справ, 2012. 491 с.

187. Судові рішення у сфері електронної комерції. URL: https://id-legalgroup.com/ (дата звернення 08.02.2023 р.).

188. Сучасні інструменти боротьби з кібершахрайствами у банках: Монографія / О. В. Кузьменко, Г. М. Яровенко, С. В. Лєонов та ін.; за заг. ред. О. В. Кузьменко, Г. М. Яровенко. Суми: видавництво «Ярославна», 2018. 144 с.

189. Таран О. В. Особливості отримання криміналістично значимої інформації на початковому етапі розслідування злочинів, пов’язаних з

порушенням вимог законодавства про охорону праці. *Правова інформатика*. № 3-4 (31). 2011. С. 156-160.

190. Таранова А. М. Участь спеціаліста в проведенні допиту під час розслідування неналежного виконання професійних обов'язків медичним або фармацевтичним працівником. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 1. С. 312-324.

191. Тардаскіна Т. М., Стрельчук Є. М., Терешко Ю. В. Електронна комерція: навчальний посібник / Одеса: ОНАЗ ім. О. С. Попова, 2011. 244 с.

192. Тертичний Я. С. Сутність і природа електронної комерції. *Вісник Хмельницького національного університету*. 2018. № 3. Том 2. С. 277-284.

193. Тімашов В. О., Діденко Д. Ш. Міжнародний досвід протидії сучасній кіберзлочинності в мережі «Даркнет». *Південноукраїнський правничий часопис*. № 1. 2021. С. 167-171.

194. Тіщенко В. В. Щодо використання спеціальних знань у кримінальному провадженні. Матеріали Всеукраїнської науково-практичної Інтернет-конференції (27 листоп. 2013 року, м. Одеса). Одеса: «Юридична література», 2013. С. 349–353.

195. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса: Фенікс, 2007. 260 с.

196. Томин С. В. Використання тактичних прийомів допиту з метою профілактики кримінальних правопорушень. *Криміналістика і судова експертиза*. Випуск 64. 2019. С. 319-331.

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

198. Філіпенко Н. Є. Кримінологічна діяльність судово-експертних установ України: монографія. Харків: ХХХ, 2020. 392 с.

199. Філіпенко Н. Є., Угровецький О. П., Шарапова О. В. Теоретичні основи експертної профілактики. *Теорія та практика судової експертизи*. № 20. 2019. С. 151-162.

200. Фролов О. П. Спеціаліст як суб'єкт обшуку у формі спеціальної операції. *Право*, 2019. № 4 (66). С. 169-173.

201. Хакерський рух, як соціальне явище і база організованої злочинності. URL: https://polka-knig.com.ua/article.php?book=520&article=25590 (дата звернення 12.02.2023 р.).

202. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів. *Юридичний часопис Національної академії внутрішніх справ*. 2011. № 1(1). С. 89-93.

203. Царьов Р. Ю. Електронна комерція: навчальний посібник з підготовки бакалаврів. Одеса: ОНАЗ ім. О. С. Попова, 2010. 112 с.

204. Цехан Д. М., Луцюк П. С. Інформаційно-аналітичне забезпечення запобігання злочинам у сфері господарської діяльності оперативними підрозділами ОВС / URL: http://criminology.onua.edu.ua/?p=477 (дата звернення 21.03.2022 р.).

205. Чайковська В. П. Електронна комерція в Україні: сучасний стан та тенденції розвитку. *Національна економіка. Інтелект ХХ*І. № 3. 2016. С. 38-48.

206. Чаплинський К. О. Організація і тактика слідчих дій при розслідуванні злочинів, учинених організованими злочинним угрупуваннями : монограф. Дніпропетровськ : юрид. акад. м-ва внутр. справ, 2004. 192 с.

207. Чаплинський К. О. Тактичне забезпечення розслідування злочинів, вчинених злочинними угрупованнями. монографія. 2009. 325 с.

208. Чванкін С. А. Веб-сторінка як електронний доказ у цивільному судочинстві в Україні. *Науковий вісник Ужгородського Національного Університету*. 2020. № 62. С. 172-177.

209. Чергове викриття діяльності шахраїв під виглядом роботи легальних інтернет-магазинів :

https://www.facebook.com/cyberpoliceua/posts/483409595116542/?locale=uk_UA (дата звернення 21.02.2023 р.).

210. Чередник К. О. Розслідування шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями: дис. … канд. юрид. наук: 12.00.09 / Відкритий міжнародний університет розвитку людини «Україна». Київ. 2019. 271 с.

211. Черненко О. О. Роль слідчих підрозділів у профілактиці злочинності (зарубіжний досвід). *Інформація і право*. № 1(16). 2016. С. 180-187.

212. Чорненький Р. Фишинг в 2019 году: какие виды угроз будут преобладать и как от них защититься? // Delo.ua : сайт. 22.02.2019. URL: https://delo.ua/special/fishing-v-2019-godu-kakie-vidy-ugroz-budut-preob-350360/ (дата звернення: 17.09.2021 р.).

213. Чорноус Ю. М., Лісіцький А. В. Особливості організації розслідування кримінальних правопорушень, вчинених шляхом підпалу. *Науковий вісник Міжнародного гуманітарного університету*. Юриспруденція. 2022. № 59. С. 74-79.

214. Чучко С. В. Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет: дис. док-ра філософії. 081 – Право. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2021. 276 с.

215. Шаповал О. В. Особливості організаційно-тактичного забезпечення обшуку під час розслідування економічних злочинів. *Судова апеляція*. № 4 (45). 2016. С. 71-79.

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

217. Шапочка С. В. До питання запобігання окремим видам шахрайства, яке вчиняється з використанням можливостей мережі інтернет. *Правова інформатика*. № 3(43). 2014. С. 89-95.

218. 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.

219. Шапочка С. В. Класифікація шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). *Наука і правоохорона діяльність*. 2015. № 1. С. 159-165. URL:http://nbuv.gov.ua/UJRN/Nip_2015_1_26. (дата звернення 11.03.2023 р.).

220. Шахрайство в Інтернеті: яким буває, якими наслідками загрожує і як себе убезпечити? URL: https://advokat-zhuk.com.ua/ua/shahrajstvo-v-interneti-jakim-buvaie-jakiminaslidkami-zagrozhuie-i-jak-sebe-ubezpechiti/ (дата звернення 11.03.2023 р.).

221. Шевців В. М. Типові способи незаконного використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги. *Вісник пенітенціарної асоціації України*. 2022. № 2 (20). С. 49-58.

222. Шевченко Т. Б., Бортновська З. П., Солоткий С. А. До питання про докази у кримінальному судочинстві. *Вісник Верховного Суду України.* 2009. № 11. С. 26.

223. Шевчук В. Технологія тактичної операції як різновид криміналістичних технологій. *Вісник Національної академії правових наук України.* № 4 (75). 2013. С. 235-242.

224. Шевчук В. М. Проблеми криміналістичної класифікації тактичних операцій. *Питання боротьби зі злочинністю*. № 24. 2012. С. 180-192.

225. Шепитько В. Ю. Криминалистика: курс лекций / [Изд. 2-е, перераб. и доп.]. Харків: Одиссей, 2005. С. 153.

226. Шепітько В. Ю. Криміналістична тактика (системноструктурний аналіз): монографія. Харків: ХНУВС, 2007. 432 с.

227. Школьний В. Б. Тактика викриття організатора злочинного угруповання. автореф. … дис. к.ю.н. 12.00.09 / Національний університет внутрішніх справ. Київ. 2010. 20 с.

228. Шкригун Ю. О. «Електронний бізнес», «електронна комерція» та «електронна торгівля»: відмінності й особливості. *Управління економікою: теорія та практика: Зб. наук. праць.* Київ: ІЕП НАНУ, 2020. С. 312-325.

229. Щербаковський М. Г., Коршенко В. А. Тактичні та організаційні особливості зняття інформації із транспортних телекомунікаційних мереж. *Криміналістика і судова експертиза*. Випуск 63. С. 154-162.

230. Щербюк Х. В., Пядишев В. Г. Особливості виключення комп'ютерної техніки під час проведення обшуку. Актуальні задачі досягнення у галузі кібербезпеки: матеріали всеукраїнської науково-практичної конференції. Кропивницький. 2016. С. 64-65.

231. Що заважає українській електронній торгівлі стати цивілізованою. URL: https://www.pravda.com.ua/ (дата звернення 03.02.2023 р.).

232. Юдін В. Ю. Електронна комерція та її правове регулювання. *Юридичний науковий електронний журнал*. 2020. № 8. С. 213-216.

233. Юрчишин В.М. Класифікація функцій прокурора у досудовому розслідуванні. *Адвокат*. 2014. №2. С. 30-34.

234. Янковий М. О. Криміналістична профілактика як складова слідчої діяльності. *Актуальні проблеми держави і права*. 2008. С. 55-59.

235. Яременко О.І. Сучасне право розуміння відносин в інформаційній сфері та методологія їх систематизації. *Інформація і право.* № 3 (22). 2017. С. 30-42.

236. Яровенко Г. М., СковронськаА. І., Бояджян М. М. Моделювання виявлення ознак кіберзагроз в банках із використанням інтелектуального аналізу. *Ефективна економіка*. 2018. № 7. URL:

http://www.economy.nayka.com.ua/pdf/7_2018/39.pdf (дата звернення 11.03.2023 р.).

237. Яцишин М. Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю: дис. … канд. юрид. наук (12.00.11) Національний авіаційний університет, Київ, 2019. 220 с.

238. Avoid online fraud. Nidirect: government services. URL: https://www.nidirect.gov.uk/articles/avoid-online-fraud. (дата звернення 11.03.2023 р.).

239. 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. (дата звернення 20.02.2022 р.).

240. International Telecommunication Union of the United Nations: Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector: URL: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf (дата звернення 21.02.2023 р.).

241. Internet Fraud: How to Avoid Internet Investment Scams. Sec.gov. Retrieved 2012-02-18. URL: https://uk.wikipedia.org/wiki (дата звернення 11.03.2023 р.).

242. Nathaniel Popper (February 10, 2013). «Complex Investments Prove Risky as Savers Chase Bigger Payoff». The New York Times. Retrieved February 11, 2013. URL: https://uk.wikipedia.org/wiki/(дата звернення 12.02.2023 р.).

243. The World Price of Insider Trading by Utpal Bhattacharya and Hazem Daouk in the Journal of Finance, Vol. LVII, No. 1 (Feb. 2002).

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Коба В.Б.Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право*. 2020. № 2 (68). С. 303–307.

2. Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

3. Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

4. Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

5. Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

6. Коба В.Б. Е-комерція – як об’єкт криміналістичного дослідження: ґенеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Коба В.Б. Значення тактичних завданьдля побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

8. Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

9. Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі :матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

10. Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування :матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Додаток Б

Зведені результати
анкетування 245 слідчих, 137 працівників органів прокуратури, 56 працівників кіберполіції, 198 працівників оперативних підрозділів, 76 працівників експертних установ МВС України.

	З а п и т а н н я	
1	**Ваш вік:**	
	20-25 років	**23**
	25-30 років	**31**
	31-40 років	**38**
	41 рік і старше	**8**
2	**Який досвід практичної роботи:**	
	до 1 року	**8**
	від 1 до 3 років	**26**
	від 3 до 5 років	**19**
	від 5 до 10 років	**18**
	більше 10 років	**29**
3	**Яку посаду займаєте:**	
	слідчий	**18**
	старший слідчий	**34**
	працівник експертної установи	**7**
	керівник слідчого підрозділу	**8**
	працівник оперативного підрозділу	**13**
	процесуальний керівник (прокурор прокуратури)	**8**
	інше	**12**
4	**Ваша освіта:**	
	тільки вища юридична	**81**
	вища юридична та інша за іншим профілем	**9**
	вища освіта за іншим профілем	**7**
	середня освіта	**3**
5	**Чи можете Ви надати інформацію щодо розслідування шахрайства в е-комерції:**	
	Так	**100**
	Ні	**0**
	На Вашу думку, що найчастіше стає предметом злочинного	

6	**посягання:**	
	послуги	**43**
	гроші	**39**
	товари побутового прзначення	**12**
	товари військового призначення	**7**
	медикаменти	**8**
	криптовалюта	**2**
	інше	**15**
7	**Чи вважаєте Ви, що розслідування шахрайства в е-комерції потребує кваліфікації слідчого у цьому напряму:**	
	Так	**100**
	Ні	**0**
8	**Яким чином Ви підвищуєте свою кваліфікацію:**	
	шляхом спілкування з фахівцями у сфері е-комерції, (консультування)	**79**
	шляхом вивчення спеціальної літератури	**78**
	не підвищую, оскільки не маю часу	**8**
	проходження спеціальних курсів	**3**
	інше	**14**
9	**Чи є необхідність у використанні спеціальних знань при розслідуванні шахрайства в е-комерції:**	
	так	**100**
	ні	**0**
10	**Чи вважаєте Ви, що питання, які стосуються е-комерції, є достатньо складними для сприйняття слідчим без належної підготовки та консультацій:**	
	так	**98**
	ні	**2**
11	**Між якими органами (установами) здебільшого здійснюється взаємодія при розслідуванні шахрайства в е-комерції:**	
	між слідчим та оперативним працівником	**100**
	між слідчим та представникам державних та приватних установ, які мають відношення до е-комерції	**98**
	між слідчим та банківським установами	**19**
	інше	**39**
12	**Взаємодія між слідчим та оперативними підрозділами у справах щодо шахрайства в е-комерції, має місце у вигляді:**	
	взаємний обмін інформацією та спільний її аналіз	**98**
	спільне планування слідчих (розшукових) дій та оперативно-розшукових заходів	**98**
	надання допомоги при виконанні заходів забезпечення кримінального провадження (привід, затримання тощо)	**78**

	інше	**38**
13	**Вкажіть, які слідчі (розшукові) та процесуальні дії у провадженнях даної категорії звичайно проводяться:**	
	огляд місця події	**91**
	огляд комп'ютерної техніки	**100**
	допит	**100**
	обшук	**76**
	пред'явлення для впізнання	**33**
	слідчий експеримент	**4**
	призначення експертиз	**100**
	освідування	**8**
	тимчасовий доступ до речей та документів	**100**
	інші	**59**
14	**Участь спеціаліста в проведенні слідчих дій (інших процесуальних дій) у провадженнях даної категорії найбільш поширена при проведенні:**	
	обшуків	**54**
	тимчасового доступу до речей та документів	**39**
	допиту	**15**
	огляду електронних документів	**76**
	відібрання зразків підпису та почерку для почеркознавчого дослідження	**14**
	призначення експертиз	**100**
	інше	**38**
15	**Як Ви вважаєте, які можуть бути основні причини великої тривалості розслідування шахрайства в е-комерції:**	
	складність розмежування злочину від цивільно-правового делікту	**94**
	недостатність кваліфікації у слідчого в галузі е-комерції	**39**
	відсутність технічного оснащення	**14**
	інше	**37**
16	**Чи потребувалась додаткова консультація фахівця перед призначенням експертиз:**	
	так	**96**
	ні	**4**
17	**Вкажіть основні тактичні помилки, яких припускаються слідчі, які розслідуютьшахрайства у сфері е-комерції:**	
	неправильно підібраний або неповний тактичний комплекс дій	**81**
	порушення процесуального порядку проведення слідчих (розшукових) дій	**71**
	проведення деяких процесуальних дій без участі спеціаліста	**41**
	«поверхневий» характер процесуальних дій, ігнорування встановлення низки важливих обставин	**53**
	обрання неправильної послідовності процесуальних дій, зокрема	**51**

	тактичних операцій	
	інше	**41**
18	**Як Ви відноситесь до проведення тактичних операцій при розслідуванні шахрайства в е-комерції:**	
	позитивно	**100**
	негативно	**0**
19	**Чи вважаєте Ви планування у справах даної категорії обов'язковим:**	
	так	**100**
	ні	**0**
20	**Що є основними причинами рідкого застосування пред'явлення для впізнання у режимі відеоконференції**	
	складність підготовки й проведення впізнання в режимі відеоконференції	**37**
	відсутність необхідного технічного забезпечення слідчого підрозділу ГУНПУкраїни	**41**
	інші причини	**32**
21	**Як Ви вважаєте, чи є поширеними факти вчинення протидії розслідуванню кримінальним правопорушенням даної категорії:**	
	так	**96**
	ні	**4**

Додаток В

Результати вивчення
матеріалів 157 кримінальних проваджень за фактами шахрайств у сфері е-комерції (Вінницька, Волинська, Дніпропетровська, Донецька, Запорізька, Київська, Львівська, Миколаївська, Одеська, Полтавська, Сумська, Харківська, Хмельницька, Черкаська та Чернівецька області, м. Київ) за 2016-2023 рр.

№	Досліджувані питання	%
1	**Способи вчинення шахрайств включали**	
	підготовка, безпосереднє вчинення, приховування	**95**
	безпосереднє вчинення, приховування	**5**
	тільки вчинення	**0**
2	**Підготовка до вчинення шахрайства у сфері е-комерції включала**	
	планування злочину	**89**
	підбір та збирання інформації щодо об’єкта	**83**
	добір співучасників злочину	**43**
	розподіл ролей між співучасниками	**43**
	інше	**56**
3	**Способи приховування**	
	виготовлення та використання фіктивних документів	**44**
	використання у злочинній діяльності підроблених документів, що засвідчують особу	**25**
	маскування злочину під легальні цивільно-правові угоди	**76**
	інше (вказати спосіб)	**32**
4	**Способи вчинення шахрайства у сфері е-комерції**	
	здійснення електронних комерційних угод із використанням вкрадених кредитних карток	**16**
	здійснення електронних комерційних угод, проведення транзакцій із викраденими персональними даними	**31**
	здійснення електронних комерційних угод від імені фіктивного суб’єкта підприємницької (комерційної) діяльності	**13**
	шахрайські операції шляхом перенаправлення клієнтів в браузері на вебсайт шахраїв для здійснення комерційних угод	**7**
	інше	
5	**Сліди, які було виявлено при розслідуванні шахрайств у сфері е-комерції**	
	нотатки злочинця	**32**
	бланки документів	**31**
	печатки, штампи, за допомогою яких підроблялися документи	**42**
	зразки підписів та почерку певних осіб	**14**

	різноманітні документи, що засвідчують особу (підроблені, викрадені та загублені)	**12**
	комп'ютерна техніка	**72**
	інше	**44**
6	**Відомості про особу шахрая**	
	1) освіта: середня вища неповна середня освіта	 **50** **40** **10**
	2) місце проживання: сільська місцевість велике місто	 **13** **87**
	3) професія: юристи та адвокати держслужбовці банківські працівники безробітні інше	 **19** **27** **33** **11** **10**
	4) сімейний стан: є сім'я немає сім'ї	 **84** **16**
	5) наявність судимості: є судимість немає судимості	 **3** **97**
	6) склад осіб: шахрайство вчинено однією особою шахрайство вчинено групою осіб або організованою злочинною групою	 **30** **70**
	7) стать: жіноча чоловіча	 **31** **69**
7	**Відомості про потерпілого**	
	1) освіта: середня вища неповна середня освіта	 **25** **15** **60**
	2) чи мала місце віктимна поведінка потерпілого так ні	 **86** **14**
	3) чи належить потерпілий до соціально незахищених верств населення:	

	так ні	**5** **95**
	4) *чи зловживають спиртними напоями або наркотичними речовинами:* так ні	 **4** **96**
7	**Наявність у кримінальному провадженні плану розслідування**	
	план є	**93**
	плану немає	**17**
8	**Серед позицій, які є в аналізованих планах розслідування, здебільшого можна відзначити такі**	
	визначення завдань та цілей розслідування	**45**
	висунення версій	**88**
	обставини, що підлягають встановленню	**94**
	основні заходи	**100**
	визначення послідовності і строків	**100**
	визначення виконавців	**95**
	інше	**30**
9	**Які слідчі (розшукові), процесуальні дії проводились у справах щодо шахрайств у сфері е-комерції**	
	допит	**100**
	одночасний допит двох або більше осіб	**90**
	обшук	**56**
	огляд місця події	**78**
	огляд предметів та документів	**95**
	пред’явлення для впізнання осіб	**37**
	пред’явлення для впізнання предметів та документів	**32**
	призначення експертиз	**100**
	відібрання зразків для порівняльного дослідження	**94**
	інші	**85**
10	**Шляхом допиту вдалося:**	
	висунути слідчі версії	**73**
	отримати відомості про особу злочинця та його злочинну поведінку	**86**
	визначити послідовність, мету та характер проведення інших процесуальних дій	**89**
	обставини, що підлягають встановленню та доказуванню у кримінальному провадженні	**69**
	інше	**78**
11	**Свідками у справах щодо шахрайств у сфері е-комерції**	

	виступали:	
	знайомі та родичі потерпілого	**80**
	знайомі та родичі підозрюваного	**55**
	особи, які випадково стали свідками події (знаходилися у нотаріальній конторі, в банківській установі, чули розмову між шахраєм та потерпілим)	**44**
	інтернет-провайдери	**19**
	співробітники установ виконання покарань	**3**
	інші	**52**
12	**Одночасний допит проводився:**	
	між підозрюваними особами	**65**
	між підозрюваним та потерпілим	**52**
	між підозрюваним та свідками	**15**
	між свідками	**3**
13	**Результати одночасного допиту між підозрюваним і потерпілим:**	
	під час одночасного допиту між потерпілим та підозрюваним останній у ході проведення слідчої дії повністю або частково підтвердив факти, що раніше заперечував	**11**
	підозрюваний лише повторював ті показання, що раніше надавав (не на підтвердження своєї провини)	**88**
14	**Обшук проводився:**	
	в офісних приміщеннях	**22**
	у житлових приміщеннях	**73**
15	**Під час обшуків у справах щодо шахрайства у сфері е-комерції здебільшого вилучалися:**	
	записи, схеми і графіки про злочинні дії у записних книжках та на окремих аркушах	**11**
	роздруківки із криміналістично значимою інформацією	**6**
	взуття, одяг, аксесуари, засоби маскування (перуки, вуса, накладні носи та ін.)	**11**
	бланки документів, необхідних для здійснення шахрайських дій	**67**
	спеціальна література (на тему підробки документів, психології обману, правил укладання угод)	**11**
	газети із підкресленням номерів телефонів	**3**
	сім-картки	**4**
	документи, що посвідчують особистість (паспорти, посвідчення тощо як справжні, так і підроблені)	**54**
	комп’ютерна техніка	**78**
	інше	**47**
1	**До обшуку залучались**	

6		
	спеціалісти-криміналісти	**72**
	спеціалісти з інших галузей	**18**
	інші	**34**
17	**Помилки, яких припускаються слідчі під час проведення обшуку**	
	відсутність технічних засобів фіксації	**37**
	обмежене застосовування техніко-криміналістичних засобів для виявлення пошуку	**54**
	недотримання криміналістичних рекомендацій щодо правил проведення відео-, фотозйомки	**38**
	відсутність спеціаліста (спеціалістів)	**37**
18	**Призначення експертиз**	
	почеркознавчі	**95**
	технічні експертизи документів	**100**
	комп'ютерно-технічні	**8**
	дактилоскопічні	**4**
	трасологічні	**5,5**
	експертиза відео-, звукозапису	**2**
	фототехнічна експертиза	**1,5**
	судово-психіатрічна	**1**
	інші	**7**

Додаток Г

<u>АЛГОРИТМ</u>
<u>дій при документуванні найпоширеніших схем онлайн шахрайств</u>

Шахрайство у сфері електронної комерції	**Фішинг**
<u>Механізм скоєння злочину:</u> Потерпілий на легальних торгівельних Інтернет – майданчиках або в соціальних мережах віртуально (шляхом переписки у чаті, у месенджерах) або телефону домовляється з шахраєм про придбання товару, здійснює передплату/або повну оплату: 1) на банківський рахунок шахрая/карту дропа або 2) отримує фейкове посилання на olx-доставку, здійснює оплату. Товар потерпілий не отримує. Відповідно до залишеної слідової картини, необхідно здійснити наступні <u>першочергові слідчі та розшукові дії</u>: **<u>1.</u>**Провести якісний і ретельний допит потерпілого*(див. додаток до алгоритму № 1)*, під час якого встановити: -аккаунт злочинця (обліковий запис); -посилання на його оголошення, відобразити механізм спілкування потерпілого з шахраєм (чати, месенджери, електронна пошта, тощо);	**Телефонний:** <u>Механізм скоєння злочину:</u> Потерпілому на його фінансовий номер мобільного телефону телефонує шахрай, який представляється працівником банківської установи/або потерпілий отримує sms – повідомлення про зняття коштів/блокування банківського рахунку з пропозицією зателефонувати за номерами телефонів. У ході бесіди шахраї, використовуючи знання психології та соціальної інженерії заволодівають реквізитами банківської картки та sms – повідомленнями від банківських установ/або примушують потерпілого провести певні дії у банкоматі/терміналі. В результаті, з банківського рахунку потерпілого знімаються кошти, у тому числі кредитні. Наявний практичний досвід свідчить про походження такої шахрайської схеми із місць позбавлення волі, але останнім часом до вказаної схеми входять так звані «колл-центри», в яких працюють особи, що діють згідно наданих їм інструкцій під виглядом працівників банківських установ. Документування та розкриття таких видів злочинів доцільно проводити в межах кримінального провадження з проведенням НСРД. Відповідно до залишеної слідової картини, необхідно здійснити <u>наступні першочергові слідчо-розшукові дії</u>:

-наявну контактну інформацію злочинця, у тому числі номер карткового рахунку, номер електронного гаманця та телефону, тощо. *ВАЖЛИВО!* До допиту долучити зображення (скріншоти) переписки, змісту і стилістики самого оголошення, сторінки шахрая в соціальній мережі або мессенджері, документу, що підтверджує сплату коштів. Долучити виписку по банківському рахунку постраждалого із зазначенням платіжних систем, за допомогою яких здійснювалась транзакція (такі виписки потерпілий може сформувати через системи онлайн-доступудо карткового чи електронного рахунку). **2.**З метою отримання належних і допустимих доказів у кримінальному провадженні, відразу після внесення до ЄРДР,звернутисьіз клопотанням про тимчасовий доступ у порядку глави 15 КПК України(*див. додаток до алгоритму№ 2*): - до інформації банківських установ про власників банківських карток/рахунків, на які здійснювався переказ грошей потерпілих, місце зняття коштів та фото- і відеозаписи з камер, встановлених на банкоматах або у відділеннях банку. Якщо гроші перераховувались на інші рахунки, то також IP-адреси користування web-банкінгом; - до інформації операторів мобільного зв'язку. *ВАЖЛИВО!*Крім отримання доказової бази по справі, вказане в подальшому може сприяти передачі провадження (при визначенні	**1.**Допит потерпілого в якому відобразити механізм спілкування, обсяг інформації про потерпілого, яким володів шахрай, номери мобільних телефонів, з яких телефонували зловмисники*(див. додаток до алгоритму№ 1)*. *ВАЖЛИВО!*До допиту потерпілого долучити виписку по його банківському рахунку з зазначенням платіжних систем, за допомогою яких здійснювалась транзакція.(такі виписки потерпілий може сформувати через системи онлайн-доступу до карткового чи електронного рахунку). **2.** З метою отримання належних і допустимих доказів у кримінальному провадженні, відразу після внесення до ЄРДР, звернутись із клопотанням про тимчасовий доступ у порядку глави 15 КПК України (*див. додатокдо алгоритму № 2*): - до інформації банківських установ про власників банківських карток/рахунків, на які здійснювався переказ грошей потерпілих, місце зняття коштів та фото- і відеозаписи з камер, встановлених на банкоматах або у відділеннях банку. Якщо гроші перераховувались на інші рахунки, то також IP-адреси користування web-банкінгом; - до інформації операторів мобільного зв'язку, з метою встановлення IMEI мобільних терміналів, в яких працювала дана сім-карта, місце виходу її на зв'язок та коло її інших абонентів. Дана інформація дозволить встановити інших потерпілих, через коло зв'язків прив'язати сім-карту до шахрая, знайти під час обшуку мобільні термінали, в яких вона використовувалась та ідентифікувати їх із злочинцем.

прокурором підслідності) в порядку ст. 218 КПК України. **3.**Якщо мало місце реальне фізичне спілкування потерпілого і шахрая за телефоном, ініціювати звернення слідчого з клопотанням про тимчасовий доступ до інформації, що перебуває у володінні мобільного оператору, з метою встановлення IMEI мобільних терміналів, в яких працювала дана сім-карта, місце виходу її на зв'язок та коло її інших абонентів. Дана інформація дозволить встановити інших потерпілих, через коло зв'язків прив'язати сім-карту до шахрая, знайти під час обшуку мобільні термінали, в яких вона використовувалась та ідентифікувати їх із злочинцем. *ВАЖЛИВО!*У випадку, якщо під час шахрайських дій фізичних розмов з шахраєм не було, а мало місце лише листування у мессенджері, то скоріш за все використовувався віртуальний телефонний номер за технологією IP-телефонії, в таких випадках не потрібні мобільні термінали для фізичного розміщення сім-карти і вказана процесуальна дія не дасть очікуваного результату. **4.**Відпрацювати всі наявні електронні сліди злочину: - на адресу ВПК в Миколаївській області надати доручення (в порядку ст.ст. 40-1, 40 КПК України) з метою встановлення особи шахрая. В дорученні обов'язково відобразити розширену фабулу із зазначенням всієї інформації про контактні данні злочинця, встановлені у ході допиту	ВАЖЛИВО! Крім отримання доказової бази по справі, вказане в подальшому може сприяти передачі провадження (при визначенні прокурором підслідності) в порядку ст. 218 КПК України. **3.**Для відпрацювання всіх наявних електронних слідів злочину, на адресу ВПК в Миколаївській області надати доручення (в порядку ст.ст. 40-1, 40 КПК України) щодо отримання інформації з електронних платіжних систем з метою отримання білінгової інформації про автора оголошення, провайдерів телекомунікацій та СПД, які надають послуги хостингу, реєстраторів доменних імен з метою отримання фактичної адреси зловмисників.*(див. додаток до алгоритму № 3)* **4.** З метою отримання належних і допустимих доказів у кримінальному провадженні, відразу після внесення до ЄРДР, звернутись із клопотанням про тимчасовий доступ до інформації операторів мобільного зв'язку щодо абонентських номерів мобільних телефонів та банківських установ (належність банківського рахунку, IP-адреси користування web-банкінгом, фото-відео зняття коштів у банкоматах, у відділеннях банку) в порядку глави 15 КПК України. Крім отримання доказової бази по справі, вказане в подальшому може сприяти передачі провадження (при визначенні прокурором підслідності) в порядку ст. 218 КПК України. **5.**Після отримання інформації про причетних до вчинення злочинів осіб та за умови, що ці злочини територіально підслідні органам досудового розслідування Миколаївської області, готувати і проводити необхідні слідчі дії, в тому

потерпілого. Зазначена інформація сприятиме отриманню допустимих доказів у кримінальному провадженні та ідентифікації особи злочинця.*(див. додаток до алгоритму № 3)* -у разі, якщо оплата здійснювалась на електронні гаманці, або за допомогою електронних платіжних систем, надати доручення ВПК в Миколаївській області (в порядку ст. 40-1, 40 КПК України) з метою встановлення особи злочинця (автора оголошення). У дорученні зазначити всю інформацію, отриману в процесі допиту потерпілого. Вказане сприятиме отриманню білінгової інформації про автора оголошення. *ВАЖЛИВО!* Викладення у дорученні оперативному підрозділу повної інформації про спосіб скоєння правопорушення, наявні ідентифікатори злочинця дадуть змогу ВПК в Миколаївській області ДКП НПУ здійснити якісне та швидке її відпрацювання, встановити СПД, які надають телекомунікаційні та послуги хостингу, реєстраторів доменних імен та інш. з метою отримання білінгової інформації про клієнтів, способи оплати за хостинг, за доменне ім'я та інш. **5.**Після отримання інформації про причетних до вчинення злочинів осіб та за умови, що ці злочини територіально підслідні органам	числі НСРД(передбачені ст.ст. 264, 267, 268, 269, 270 КПК України), обшуки та інш., направлені на отримання доказів протиправних дій фігурантів. Провести інші необхідні слідчо-розшукові заходи **Інтернет-фішинг** Механізм скоєння злочину: Зловмисники створюють в мережі Інтернет фейковий сайт популярних сервісів (інтернет-банкінгу, «olx» (наприклад olx-доставка), «Нової Пошти», популярних сервісів з миттєвого поповнення рахунку мобільних телефонів, тощо) який на вигляд не відрізняється від справжнього. Єдина відмінність у URL-адресі (посилання), на яку потерпілий зазвичай не звертає уваги. Проводячи оплату на фейковому сайті або заповнюючи форму зворотного зв'язку, потерпілий вводить данні своєї банківської карти (номер/строк дії/CVV-код), після введення яких – зловмисники в режимі реального часу можуть виводити кошти з банківської картки шляхом проведення несанкціонованих транзакцій, використовуючи отримані дані карткового рахунку, які сам же потерпілий і ввів. Відповідно до залишеної слідової картини, необхідно здійснити аналогічні першочергові слідчо-розшукові дії, як і при розслідуванні фактів телефонного фішингу. Відмінність у способі заволодіння реквізитами банківської картки (використання Інтернет (URL-адреси).

досудового розслідування Миколаївської області, готувати і проводити необхідні слідчі дії, в тому числі НСРД, обшуки та інш., направлені на отримання доказів протиправних дій фігурантів. Провести інші необхідні слідчо-розшукові заходи.	

За матеріалами ВПК в Миколаївській області ДКП НПУ

Додаток Д

Пропозиції щодо
алгоритму
дій за системою «AntiFraud»

1. ПОТЕРПІЛИЙ ПОДАЄ ЗАЯВУ.

Громадянин України, який став жертвою шахрайських дій подає заяву до центрального чи територіального органу Національної поліції України (далі – НПУ) за допомогою лінії «102» чи форми зворотного зв'язку на веб-сайті Департаменту кіберполіції або повідомляє банківську установу клієнтом якої він є, про скоєні шахрайські дії відносно нього. При цьому зазначає повні відомості щодо:

- власного карткового рахунку;
- банківської картки отримувача;
- дати, часу та суми транзакції;
- інші значущі відомості.

Банк отримавши повідомлення про шахрайські дії, інформує клієнта, що дане повідомлення буде передано до НПУ, при отримані на це згоди, через автоматизовані алгоритми рішення для передачі даної інформації (API), якщо клієнт не дає згоди то отримує інформацію на рекомендацію звернутися до поліції самостійно.

Лінія «102».

Заява (повідомлення), що надходить телефоном за скороченим номером екстреного виклику поліції «102», реєструється в ІТС ІПНП де кожній електронній картці автоматично присвоюється власний номер − ID.

Також, кожному зверненню присвоюється порядковий номер – **ЄО.** 2

2. ОБМІН ІНФОРМАЦІЄЮ.

Вже зареєстрована інформація та відомості зазначені потерпілим (номер карти, сума збитку, дата та час транзакції) надходить до системи «AntiFraud». Після чого вказана система автоматично направляє запит до банківських установ, де в свою чергу встановлюється факт транзакції та відстежується подальший рух коштів потерпілого до кінцевого рахунку/банківської картки, на яку були перераховані кошти правопорушником з одночасним блокуванням рахунку на вивід коштів.

Отримавши зазначені відомості, банківська установа дає автоматичний припис через (API), іншим банкам отримувачам коштів, на блокування банківських рахунків шахраїв та грошових коштів, з яких здійснено обготівкування, терміном до 48 годин.

Для мінімізування часу визначення територіальності та реєстрації ЄРДР за місцем знаходження шахрая (на теперішній момент реєстрація матеріалів про шахрайські дії здійснюється за місцем мешкання потерпілого),

а також блокування грошових коштів на рахунках якими користується зловмисник та з метою недопущення їх подальшого привласнення НБУ передає інформацію у зворотному напрямку, не пізніше ніж за 12 годин, із зазначенням:

- фінансового номеру телефону шахрая;
- інформацію по територіальності де здійснювалось обготівкування коштів (адреса розташування банкомату);
- IP адреси, з яких здійснювалось керування підконтрольними рахунками.

Алгоритм взаємодії між НБУ та поліцією, НБУ та банками буде розроблений в період реалізації проекту, а саме: процес обміну інформації, порядок блокування та розблокування.

ЗАКОНОДАВЧА ЧАСТИНА.

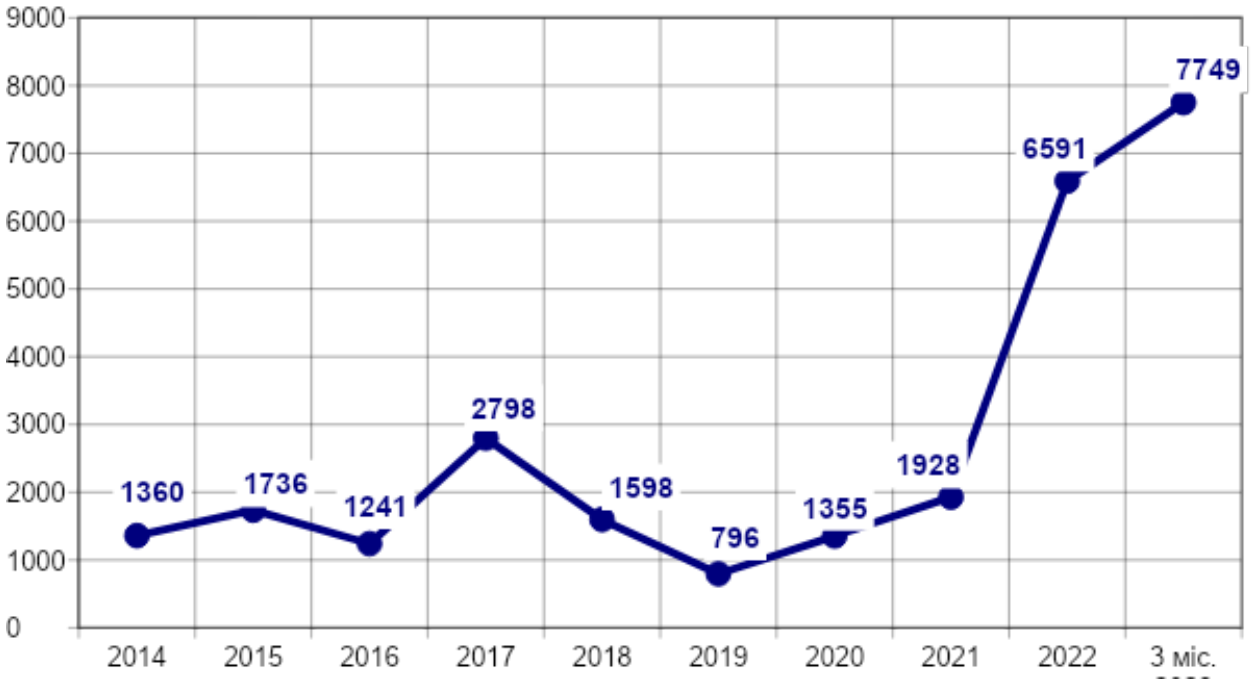
- Постанова НБУ «Щодо регулювання процесу обміну даними між банківськими установами та правоохоронними органами» (з урахуванням банківської таємниці)

зміни часткові:

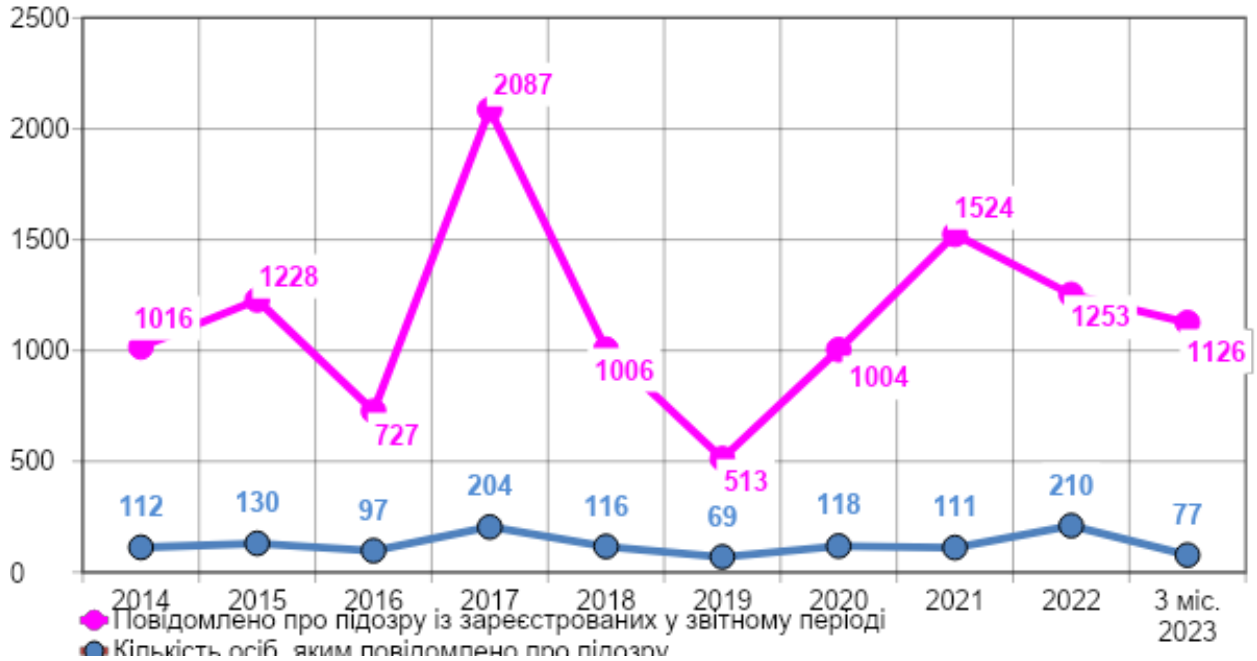
- до Закону про Банки і Банківську діяльність (порядок розкриття та передачі інформації);
- до Закону про захист персональних даних (порядок розкриття та передачі інформації);
- до Закону Про платіжні послуги (збільшення терміну блокування рахунків);
- до Закону Кримінального кодексу (за передачу даних карток).

Додаток Е

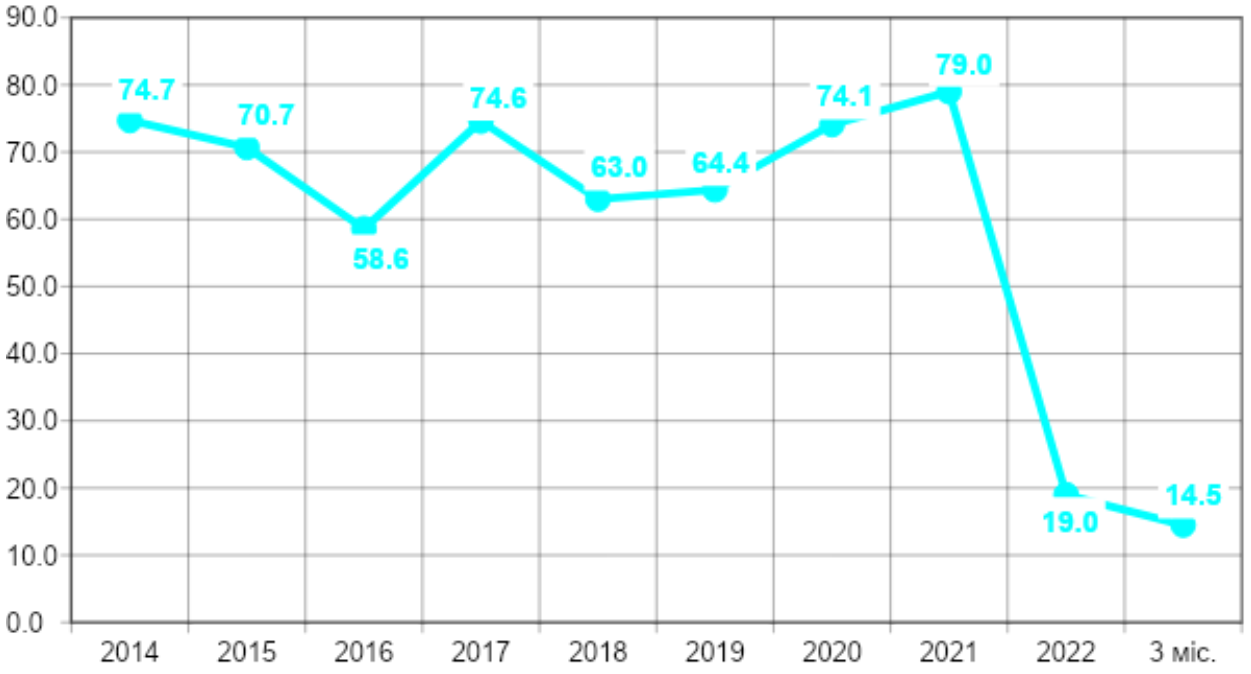
Статистичні дані
Департаменту інформаційно-аналітичної підтримки
Зареєстровані кримінальні правопорушення, передбачені ч. 3 ст. 190 КК України, що вчинені з використанням високих інформаційних технологій, за період з 2014 року по І квартал 2023 року



Кримінальні правопорушення, передбачені ч. 3 ст. 190 КК України, що вчинені з використанням високих інформаційних технологій, за якими особі повідомлено про підозру, із числа зареєстрованих у звітному періоді за період з 2014 року по I квартал 2023 року



Питома вага розкритих кримінальних правопорушень, передбачених ч. 3 ст. 190 КК України, що вчинені з використанням високих інформаційних технологій, із числа зареєстрованих у звітному періоді за період з 2014 року по І квартал 2023 року



Додаток Є

Звіт
про проведення інформаційної кампанії з протидії шахрайствам
(07.06. - 25.09.2023)

Управління комунікації забезпечило узагальнення інформації щодо результатів проведення інформаційно-роз'яснювальної кампанії з протидії шахрайствам.

Зокрема розміщено:
білбордів – 1 135
сітілайтів – 771
роздано листівок – 718 857
постерів і плакатів – 169 040, у тому числі:
- у громадському транспорті – 33 967
- на залізничних вокзалах – 2 822
- на автостанціях – 4 217
- у метрополітені – 111
- у ТРЦ – 7 944
- на АЗС – 6 897
- у поліцейських підрозділах – 4 331
- у приміщеннях органів влади – 11 245
- у ЦНАПах – 3 464
- у приміщеннях поштових відділень – 8 775
- у медичних закладах – 8 293
- у магазинах – 62 381
- інше – 14 593

У регіональні підрозділи надіслано по три відео- та аудіоролики – 1 275 083 виходи, у тому числі:
- в ефірах регіональних телеканалів – 24 262
- в ефірах радіостанцій – 41 731
- у торгових центрах – 161 730
- у громадському транспорті – 872 644
- АЗС – 65 885

(- інше – 108 831)

На відомчих інформаційних ресурсах Національної поліції України опубліковано 14 695 тематичних матеріалів, у тому числі:
- вебсайт – 1 595
- Фейсбук – 9 399
- Інстаграм – 1 565
- Ютуб-канал – 323
- Телеграм – 1 296
- Твітер – 505
- ТікТок – 12

Загальне охоплення аудиторії інформаційних ресурсів Нацполіції становить майже чотирнадцять мільйонів осіб (14 402 745).

У засобах масової інформації та засобах масової комунікації опубліковано 38 016 тематичних матеріалів, у тому числі:

- телебачення – 5 723
- радіо – 8 411
- друковані ЗМІ – 1 184
- електронні ЗМІ – 5 207
- соціальні мережі – 13 512
- телеграм-канали – 3 979

Окрім того, тематичні ролики виходять в ефірі телемарафону «Єдині новини» і транслюються на АЗК мережі «ОККО».

У регіональних ЗМІ вийшло 951 коментар поліцейських, у центральних ЗМІ – 44, тематичних програм за участю керівництва ГУНП – 55, профілактичних сюжетів – 579.

За данимимоніторинговоїсистемиSemantrum, у 2023 роцізагалом у ЗМІ булоопублікованопонад44,8 тис. тематичнихматеріалів у 3,2 тис. джерелах. Кількістьконтактів з аудиторієюстановить понад 190,2 млн.

Найбільшеконтактівзабезпечили - Марафон «Єдиніновини» - 97,1 млн, ТСН – 27,1 млн, Нацполіція – 14,4 млн, 5 канал – 9 млн, Київоперативний – 3,8 млн, РБК-Україна – 2,9 млн.

Додаток Ж

АКТИ ВПРОВАДЖЕННЯ

результатів дослідження у наукову діяльність, освітній процес та правохоронну практику

ЗАТВЕРДЖУЮ
Проректор
Харківського національного
університету внутрішніх справ
доктор юридичних наук, професор
заслужений юрист України
полковник поліції

Олександр МУЗИЧУК

«__» _____ 2023 року

АКТ

впровадження у науково-дослідну діяльність та освітній процес Харківського національного університету внутрішніх справ результатів дисертаційного дослідження Коби В.Б. «Теоретичні та праксеалогічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: професора кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктора юридичних наук, професора Юхна О.О.

членів комісії: професора кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, доктора юридичних наук, професора Степанюка Р.Л.

старшого викладача кафедри кримінального процесу та організації досудового слідства факультету № 1 Харківського національного університету внутрішніх справ, кандидата юридичних наук, доцента Чичі Р.П.

склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби Валерія Борисовича на тему: «Теоретичні та праксеалогічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза;

оперативно-розшукова діяльність.

Основні результати дисертаційного дослідження Коби Валерія Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» використовуються в освітньому процесі та науково-дослідницькій роботі Харківського національного університету внутрішніх справ з метою подальшої розробки проблемних питань протидії економічній злочинності, насамперед, у сфері інтернет-комерції, а також методики розслідування окремих видів кримінальних правопорушень.

Основні результати дисертації відображено у наступних наукових публікаціях здобувача, зокрема:

Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право :* Науково-виробничий журнал. 2020. № 2 (68). С. 303–307.

Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели :* Науковий юридичний журнал. 2020. № 11. С. 413–419.

Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство :* Науковий журнал. 2021. № 6. С. 369–374.

Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал :* Електронне наукове фахове видання. 2021. № 9. С. 418–420.

Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління :* Збірник наукових праць. 2022. № 3. С. 291–295.

Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування : матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Наукові публікації відповідають планам науково-дослідних та дослідно-конструкторських робіт профільних кафедр Харківського національного університету внутрішніх справ на 2022-2023 навчальний рік.

Члени комісії дійшли висновку, що надані матеріали свідчать про відповідність спеціальності 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність; належний науковий, теоретичний та практичний рівень розробки дисертаційного дослідження на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції»; актуальність, вчасність і практичну значущість

дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України. Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Харківського національного університету внутрішніх справ при проведенні наукових досліджень.

Голова комісії:
професор кафедри криміналістики
та судової експертології
Харківського національного
університету внутрішніх справ
доктор юридичних наук, професор **Олександр ЮХНО**

Члени комісії:
професор кафедри криміналістики
та судової експертології
Харківського національного
університету внутрішніх справ
доктор юридичних наук, професор **Руслан СТЕПАНЮК**

старший викладач кафедри кримінального
процесу та організації досудового слідства
Харківського національного
університету внутрішніх справ
кандидат юридичних наук, доцент **Руслан ЧИЧА**

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ
доктор юридичних наук, професор
заслужений діяч науки і техніки
України
полковник поліції

Сергій ЧЕРНЯВСЬКИЙ

«__» _____ 2023 року

АКТ
впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ результатів дисертаційного дослідження

Про впровадження у науково-дослідну діяльність та освітній процес Національної академії внутрішніх справ основних результатів дисертаційного дослідження Коби Валерія Борисовича «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: заступника начальника навчально-методичного відділу Національної академії внутрішніх справ, кандидата юридичних наук, капітана поліції Бистрицького Б.Ю.

членів комісії: професора кафедри криміналістики та судової медицини Національної академії внутрішніх справ, доктора юридичних наук, професора, підполковника поліції Чорноус Ю.М.

т.в.о. завідувача кафедри криміналістики та судової медицини Національної академії внутрішніх справ, кандидата юридичних наук, доцента, капітана поліції Антощука А.О.

відповідно до Пріоритетних напрямів наукових досліджень Національної академії внутрішніх справ на 2022-2023 навчальний рік склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби Валерія

Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність.

Основні результати дослідження використовуються у НДіДКР Національної академії внутрішніх справ для подальшої розробки проблемних питань методики розслідування злочинів у сфері економіки. Результати дисертації відображено у наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (статтях і тезах доповідей на конференціях):

Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право.* 2020. № 2 (68). С. 303–307.

Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матер. Міжнар. наук.-практ. конф.* (м. Київ, 14-15 червня 2022 р.). Київ : НДІПП, 2022. С. 21–23.

Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування : матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей В.Б. Кобн, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Національної академії внутрішніх справ при проведенні наукових досліджень.

Заступник начальника навчально-методичного відділу
Національної академії внутрішніх справ
кандидат юридичних наук,
капітан поліції **Богдан БИСТРИЦЬКИЙ**

Професор кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
доктор юридичних наук, професор
підполковник поліції **Юлія ЧОРНОУС**

Т.в.о. завідувача кафедри
криміналістики та судової медицини
Національної академії внутрішніх справ
кандидат юридичних наук, доцент
капітан поліції **Андрій АНТОЩУК**

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор
Заслужений юрист України
Лариса **НАЛИВАЙКО**
«05» 05 2023 року

АКТ
впровадження у науково-дослідну діяльність
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

12 травня 2023 року м. Дніпро

Про впровадження у науково-дослідну діяльність Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Кобн Валерія Борисовича «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голова: заступник директора Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Обшалов С.В.

члени комісії: завідувач кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Дараган В.В.

професор кафедри криміналістики та медичної підготовки Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Пиріг І.В.

завідувач кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук Санакоєв Д.Б.

відповідно до Пріоритетних напрямів наукових досліджень Дніпропетровського державного університету внутрішніх справ на 2020-2024

роки комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби Валерія Борисовича «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність. Основні результати дослідження використовуються у науково-дослідницькій роботі Дніпропетровського державного університету внутрішніх справ з метою подальшої розробки проблемних питань методики розслідування кримінальних правопорушень у сфері економіки, в тому числі і у сфері інтернет-комерції. Результати дисертаційного дослідження В.Б. Коби відображаються у наукових публікаціях здобувача наукового ступеня кандидата юридичних наук (фахових наукових статтях і тезах доповідей на міжнародних конференціях і семінарах), зокрема:

1. Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право.* 2020. № 2 (68). С. 303–307.

2. Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

3. Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

4. Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

5. Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

6. Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

7. Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

8. Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

9. Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Наукові публікації В.Б. Коби відповідають загальноуніверситетській темі наукових досліджень «Актуальні проблеми кримінально-правового, кримінального процесуального та криміналістичного забезпечення протидії злочинності в Україні (державний реєстраційний номер 0118U100431), напрямам досліджень наукової школи ДДУВС «Криміналістичне забезпечення досудового розслідування» та планам науково-дослідних та дослідно-конструкторських робіт профільних кафедр Дніпропетровського державного університету внутрішніх справ на 2022-2023 навчальний рік.

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, використовуються при підготовці науково-практичних рекомендацій та у системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також були враховані профільними кафедрами Дніпропетровського державного університету внутрішніх справ при проведенні наукових досліджень на замовлення Головного Управління Національної поліції в Дніпропетровській області.

Голова комісії: **Сергій ОБШАЛОВ**

Члени комісії: **Валерій ДАРАГАН**

Ігор ПИРІГ

Дмитро САНАКОЄВ

ЗАТВЕРДЖУЮ
Проректор
Дніпропетровського державного
університету внутрішніх справ
доктор юридичних наук, професор
Заслужений юрист України

Лариса НАЛИВАЙКО

«__» _____ 2023 року

АКТ
впровадження в освітній процес
Дніпропетровського державного університету внутрішніх справ
результатів дисертаційного дослідження

27 квітня 2023 року м. Дніпро

Про впровадження в освітній процес Дніпропетровського державного університету внутрішніх справ основних результатів дисертаційного дослідження Коби В.Б. «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голова: заступник директора Навчально-наукового інституту права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Обшалов С.В.

члени комісії: професор кафедри криміналістики та домедичної підготовки Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Плетенець В.М.

завідувач кафедри оперативно-розшукової діяльності Дніпропетровського державного університету внутрішніх справ, доктор юридичних наук, професор Дараган В.В.

завідувач кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент Санакоєв Д.Б.

відповідно до Положення про організацію освітнього процесу в

Дніпропетровському державному університеті внутрішніх справ, затвердженого наказом ДДУВС від 13.05.2020 № 352 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби Валерія Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право.* 2020. № 2 (68). С. 303–307.

Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матер. Міжнар. наук.-практ. конф.* (м. Київ, 14-15 червня 2022 р.). Київ : НДІПП, 2022. С. 21–23.

Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування : матер. Міжнарод. наук.-практ. конф.* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Члени комісії дійшли висновку, що надані матеріали (фахові наукові статті та тези доповідей) свідчать про належний науковий, методологічний та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, відображені у науково-методичних матеріалах навчальних дисциплін з кримінального процесу, криміналістики та оперативно-розшукової діяльності для здобувачів вищої освіти бакалавра і магістра, використовуються при підготовці методичних рекомендацій та в системі підвищення кваліфікації слідчих та інших категорій практичних працівників Національної поліції та Міністерства внутрішніх справ України.

Матеріали дисертації можуть бути використані при викладанні навчальних дисциплін «Кримінальне право», «Криміналістика», «Кримінальний процес», «Організація розслідування кримінальних правопорушень», «Тактичні особливості проведення слідчих (розшукових) дій», «Оперативно-розшукова діяльність», а також підготовці підручників, монографій, проведення практичних занять з кримінального процесу, криміналістики та оперативно-розшукової діяльності.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі Дніпропетровського державного університету внутрішніх справ при підготовці здобувачів вищої освіти ННІ права та підготовки фахівців для підрозділів Національної поліції, факультету підготовки фахівців для підрозділів кримінальної поліції, факультету підготовки фахівців для підрозділів превентивної діяльності, студентів ННІ права та інноваційної освіти та навчально-наукового інституту заочного навчання та підвищення кваліфікації.

Голова комісії: **Сергій ОБШАЛОВ**

Члени комісії: **Віктор ПЛЕТЕНЕЦЬ**

Валерій ДАРАГАН

Дмитро САНАКОЄВ

ЗАТВЕРДЖУЮ
Директор
Навчально-наукового інституту права
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
доктор юридичних наук, професор
заслужений юрист України

Анатолій КИСЛИЙ
«10» 03 2023 року

АКТ
впровадження в освітній процес і наукову діяльність
Навчально-наукового інституту права ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»
результатів дисертаційного дослідження

Про впровадження в освітній процес і наукову діяльність ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» дисертаційного дослідження Коби Валерія Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Комісія у складі:

голови: завідувача кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, професора Зароєнла В.О.

членів комісії: заступника директора Навчально-наукового інституту права ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», кандидата юридичних наук, доцента Тимошенка Ю.П.

професора кафедри правоохоронної та антикорупційної діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доктора юридичних наук, доцента Козаченка О.І.

відповідно до Положення про організацію освітнього процесу і наукової діяльності в ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія

управління персоналом» склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби Валерія Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність у вигляді наукових статей і тез доповідей на науково-практичних конференціях та семінарах, зокрема:

Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право*. 2020. № 2 (68). С. 303–307.

Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели*. 2020. № 11. С. 413–419.

Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство*. 2021. № 6. С. 369–374.

Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал*. 2021. № 9. С. 418–420.

Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління*. 2022. № 3. С. 291–295.

Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: ґенеза наукових підходів. *KELM (Knowledge, Education, Law, Management)*. 2022. № 7 (51). С. 223–227 (Республіка Польща).

Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування : матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Члени комісії дійшли висновку, що надані здобувачем Науково-дослідного інституту публічного права В.Б. Кобою матеріали (наукові статті та тези доповідей) свідчать про належний науковий, методологічний та практичний рівень розробки теми дисертаційного дослідження, ґрунтуються на достатній кількості опрацьованих законодавчих, наукових та емпіричних джерел, відображені у науково-методичних матеріалах навчальних дисциплін з

кримінального права, кримінального процесу та криміналістики для здобувачів вищої освіти бакалавра і магістра.

Комісія вважає, що представлені наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та можуть використовуватися в освітньому процесі та науковій діяльності ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» при підготовці здобувачів вищої освіти.

Голова комісії: **Володимир ЗАРОСИЛО**

Члени комісії: **Юрій ТИМОШЕНКО**

Олександр КОЗАЧЕНКО

ЗАТВЕРДЖУЮ
Директор
Дніпропетровського НДЕКЦ МВС
кандидат юридичних наук, доцент

Володимир КОРОТАЄВ

30 05 2023 р.

АКТ
впровадження результатів дисертаційного дослідження
у практичну діяльність Дніпропетровського НДЕКЦ МВС

Про впровадження у практичну діяльність Дніпропетровського НДЕКЦ МВС результатів дисертаційного дослідження Коби Валерія Борисовича «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність

Уклала комісія у складі:

Голови: т.в.о. заступника завідувача лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Геннадія Комизи

Членів комісії: завідувача сектору дактилоскопічного обліку лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Ольги Гейко

головного судового експерта лабораторії криміналістичних видів досліджень Дніпропетровського НДЕКЦ МВС Павла Кумця

Комісія відповідно до Положення про організацію проведення науково-дослідних та дослідно-конструкторських робіт у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15 травня 2007 року № 154 склала цей акт з приводу того, що комісією розглянуто результати дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Коби

Валерія Борисовича на тему: «Теоретичні та праксеологічні засади методики розслідування шахрайства у сфері е-комерції» на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 (кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність) у вигляді фахових наукових статей і тез доповідей на науково-практичних конференціях і семінарах, зокрема:

Коба В.Б. Наукові диспути щодо комплексів тактичних операцій при розслідуванні шахрайств у сфері е-комерції. *Держава та регіони. Серія: Право.* 2020. № 2 (68). С. 303–307.

Коба В.Б. Загальні напрями організації розслідування шахрайства у сфері е-комерції. *Правові новели.* 2020. № 11. С. 413–419.

Коба В.Б. Теоретичні та праксеологічні аспекти використання спеціальних знань під час розслідування шахрайств у сфері е-комерції. *Право і суспільство.* 2021. № 6. С. 369–374.

Коба В.Б. Організаційно-тактичні особливості проведення обшуку при розслідуванні шахрайств у сфері е-комерції. *Юридичний науковий електронний журнал.* 2021. № 9. С. 418–420.

Коба В.Б. Засоби криміналістичної профілактики, що застосовуються уповноваженими особами при розслідуванні шахрайства у сфері е-комерції. *Право та державне управління.* 2022. № 3. С. 291–295.

Коба В.Б. Е-комерція – як об'єкт криміналістичного дослідження: генеза наукових підходів. *KELM (Knowledge, Education, Law, Management).* 2022. № 7 (51). С. 223–227 (Республіка Польща).

Коба В.Б. Значення *тактичних завдань* для побудови алгоритму розслідування у кримінальних провадженнях щодо шахрайства у сфері е-комерції. *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. 32–34.

Коба В.Б. Криміналістичний аналіз причин та умов, що сприяють учиненню шахрайств у сфері е-комерції. *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. 53–56.

Коба В.Б. Взаємодія слідчого з іншими правоохоронними органами, а також представниками державних і приватних установ, як складова організації розслідування шахрайства в інтернет-комерції. *Перспективні напрямки розвитку юридичної науки у 21-му сторіччі : матеріали Міжнародної науково-практичної конференції* (м. Київ, 14-15 червня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 21–23.

Коба В.Б. Приводи і підстави для відкриття кримінального провадження щодо шахрайства у сфері е-комерції: проблеми теорії та практики. *Актуальні проблеми взаємодії правової науки та практики її застосування : матеріали Міжнародної науково-практичної конференції* (м. Київ, 16-17 березня 2022 р.). Київ : Науково-дослідний інститут публічного права, 2022. С. 33–36.

Комісія вважає, що представлені матеріали дисертаційного дослідження, фахові наукові статті та тези доповідей, отримані на основі проведеного наукового дослідження, мають необхідний теоретичний і методологічний рівень та практичну значимість, а також можуть бути впроваджені у діяльність Дніпропетровського НДЕКЦ МВС України.

Голова комісії: **Геннадій КОМИЗА**

Члени комісії: **Ольга ГЕЙКО**

Павло КУМЕЦЬ