МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

РЕЙНГОЛЬД АНДРІЙ ВАЛЕНТИНОВИЧ

УДК 343.98: 343.131

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ШАХРАЙСТВА В ІНТЕРНЕТ-КОМЕРЦІЇ

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

Автореферат
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Дніпро – 2023

Дисертацією є рукопис.

Робота виконана у Науково-дослідному інституті публічного права.

Науковий керівник –
доктор юридичних наук, професор
Чаплинський Костянтин Олександрович,
Дніпропетровський державний університет внутрішніх справ,
завідувач кафедри криміналістики та домедичної підготовки.

Офіційні опоненти:

доктор юридичних наук, професор
Дрозд Валентина Георгіївна,
Державний науково-дослідний інститут МВС України,
начальник 3-го науково-дослідного відділу науково-дослідної лабораторії проблем правового та організаційного забезпечення діяльності Міністерства;

кандидат юридичних наук, професор
Зарубей Вікторія Володимирівна,
Національна академія внутрішніх справ,
професор кафедри кримінального процесу.

Захист відбудеться 19 травня 2023 р. о 09.00 год. на засіданні спеціалізованої вченої ради Д 08.727.02 Дніпропетровського державного університету внутрішніх справ за адресою: 49005, м. Дніпро, просп. Гагаріна, 26.

Із дисертацією можна ознайомитись у загальній бібліотеці Дніпропетровського державного університету внутрішніх справ (м. Дніпро, просп. Гагаріна, 26).

Автореферат розіслано 18 квітня 2023 року.

Учений секретар
спеціалізованої вченої ради **В.С. Березняк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. В умовах розвитку глобалізаційних процесів та діджиталізації суспільства все частіше цифрові технології впроваджуються в усі сфери як державного устрою, так і людської діяльності зокрема. Цифровізація поступово змінює і механізми функціонування й розвитку торгівельно-комерційної сфери, що все частіше має свій прояв у виробництві, продажі та постачанні товарів і послуг через комп'ютерні мережі. Останнім часом більшість операцій побутового й комерційного призначення все частіше здійснюються у дистанційній формі, особливо у період пандемії, викликаною гострою респіраторною хворобою COVID-19, спричиненою коронавірусом SARS-CoV-2 (2020-2021 рр.), та повномасштабного збройного вторгнення рф на територію України (2022-2023 рр.), коли було зруйновано логістику, і більшість товарів й послуг стали недоступними для громадян. Попит формує пропозицію, і, як наслідок, предметом торгівельно-комерційних операцій стали медикаменти, косметичні засоби, одяг, речі побутового призначення та ін. Натомість, за часів воєнного стану в ТОП-продажів увійшли генератори та інше енергетичне обладнання, а також речі, необхідні для несення служби у зонах бойових дій (воєнний одяг, бронежилети, каски, військове обладнання, засоби освітлення). Маючи на меті отримати бажані товари й послуги, юридичні та фізичні особи активно вкладають гроші, на перший погляд, в «успішні комерційні угоди», і, вважаючи дистанційний варіант укладання таких угод більш зручним й безпечним, громадяни потрапляють у пастку інтернет-шахраїв. Нерідко негативні наслідки є результатом впливу низки форс-мажорних обставин. Між тим, здебільшого це є результатом заздалегідь спланованих та цілеспрямованих шахрайських дій. Спостерігається втягнення у злочинну діяльність, пов'язану з комерційним шахрайством у мережі інтернет, й представників кримінальних угруповань, що, використовуючи корупційні зв'язки в органах державної влади й управління, правоохоронних органах, активно протидіють розслідуванню.

За даними Офісу Генерального прокурора України, кількість таких посягань дедалі зростає. Так, у 2015 р. зафіксовано 45653 фактів учинення шахрайств, 2016 р. – 45764, 2017 р. – 36650, 2018 р. – 33136, 2019 р. – 32156, 2020 р. – 26595, 2021 р. – 23632, 2022 р. – 31937. Серед них кількість шахрайств в інтернет-комерції становить приблизно 8 %. У той час як шахраї, застосовуючи обман і зловживання довірою, отримують прибутки від укладання незаконних дистанційних правочинів, рівень розкриття шахрайства в інтернет-комерції залишається стабільно низьким. Проте, об'єктивно оцінити масштаби шахрайств досить складно через високу латентність і межу між цивільно-правовими та кримінально-правовими відносинами. Шахраї постійно удосконалюють свою злочинну діяльність, адаптуючись до реалій сьогодення. Правоохоронні органи наразі не завжди встигають так швидко адаптуватися під реальні потреби сучасності та застосовувати дієві засоби щодо запобігання шахрайствам у мережі інтернет. Зазначене свідчить про наявність низки

проблемних питань у сфері виявлення, розкриття й розслідування шахрайства в інтернет-комерції.

Теоретичну основу дослідження становлять праці вчених, які вивчали питання методики розслідування кримінальних правопорушень, у тому числі й шахрайства, зокрема: Ю. Аленіна, Л. Аркуші, В. Бахіна, А. Волобуєва, В. Дрозд, В. Журавля, М. Єфімова, В. Коновалової, Є. Лук'янчикова, С. Мінченка, О. Мотляха, В. Ортинського, Н. Павлової, І. Пирога, О. Пчеліної, М. Салтевського, Р. Степанюка, К. Чаплинського, С. Чернявського, Ю. Чорноус, В. Шевчука, В. Шепітька та ін.

Загальні проблеми розслідування і попередження шахрайства, вчиненого в мережі інтернет, розробляли такі вчені, як: С. Самойлова «Розслідування шахрайств, учинених із використанням мережі «Інтернет» (м. Донецьк, 2014 р.), С. Чучко «Розслідування шахрайства при купівлі-продажу товарів через мережу Інтернет» (м. Дніпро, 2021 р.), Т. Коршикова «Розслідування шахрайств, учинених з використанням електронно-обчислювальної техніки» (м. Київ, 2021 р.), І. Коваленко «Розслідування шахрайства у сфері використання банківських електронних платежів» (м. Дніпро, 2023 р.) та ін. Утім, способи шахрайств дедалі удосконалюються, що значно ускладнює процес доказування і впливає на організаційно-тактичне забезпечення їх розслідування. Зазначені обставини й зумовили вибір даної теми дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до Закону України «Про національну безпеку України» від 21.06.2018 № 2469-VIII, положень Стратегії національної безпеки України (Указ Президента України від 14.09.2020 № 392/2020), Стратегії боротьби з організованою злочинністю (розпорядження Кабінету Міністрів України від 16.09.2020 № 1126-р), Стратегії розвитку системи правосуддя та конституційного судочинства на 2021-2023 роки (Указ Президента України від 11.06.2021 № 231/2021), тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022-2026 роки (наказ МОН України від 03.02.2022 № 109), Порядку взаємодії Генеральної прокуратури України та МВС України щодо обміну інформацією з ЄРДР та інформаційних систем органів внутрішніх справ (спільний наказ ГПУ та МВС України від 17.11.2012 № 115/1046), Порядку електронної інформаційної взаємодії Офісу Генерального прокурора та МВС України (спільний наказ Офісу ГПУ та МВС України від 22.11.2021 № 371/846), 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 в інтернет-комерції.

Відповідно до обраної мети в дисертації поставлено та вирішуються такі основні взаємопов'язані *задачі*:

– визначити стан наукового дослідження питань розслідування

шахрайства в інтернет-комерції;

– узагальнити сучасні наукові підходи до розуміння криміналістичної характеристики шахрайства в інтернет-комерції та підкреслити наявність вагомих кореляційних зв'язків між усіма її елементами;

– з'ясувати специфіку початкового етапу розслідування шахрайства в інтернет-комерції;

– розглянути основні елементи організації й планування розслідування шахрайства та визначити коло обставин, що підлягають встановленню;

– виокремити типові слідчі ситуації, що складаються при розслідуванні шахрайства в інтернет-комерції;

– з'ясувати організаційно-тактичні особливості проведення окремих слідчих (розшукових), негласних слідчих (розшукових) та процесуальних дій;

– визначити особливості профілактичної діяльності уповноважених осіб у кримінальних провадженнях за фактами шахрайства в інтернет-комерції;

– сформувати типові тактичні операції, спрямовані на вирішення завдань розслідування шахрайства в інтернет-комерції.

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

Предмет дослідження – основи методики розслідування шахрайства в інтернет-комерції.

Методи дослідження. Відповідно до поставленої мети реалізація задач дослідження відбувалася із застосовуванням низки загальнонаукових і спеціальних методів. Основою для використання методологічної бази став діалектичний метод дослідження, який дозволив системно здійснити аналіз методики розслідування шахрайства в інтернет-комерції. Використання *історико-правового методу* зумовлено вивченням особливостей законодавства щодо окремих домінант розслідування шахрайства в інтернет-комерції, його реформування (підрозділ 1.1, 2.1). *Формально-логічні методи* використано при опрацюванні кримінальних проваджень, нормативних актів, що становлять предмет дослідження (розділи 1–3). *Структурний метод* застосовано при визначенні структури криміналістичної характеристики шахрайства в інтернет-комерції; з'ясуванні окремих наукових категорій і положень (підрозділ 1.2). Використання *порівняльно-правового методу* відбувалося при дослідженні законодавства, що регулює питання дистанційної інтернет-торгівлі, а також при аналізі системи СРД і НСРД (підрозділи 1.1, 2.1, 2.2). *Функціональний метод* використано при формуванні особливостей проведення тактичних операцій (підрозділ 3.3). *Системний метод* застосовано при виокремленні віктимогенних груп потерпілих, класифікації способів шахрайства та типових слідчих ситуацій (підрозділ 1.2, 2.3). *Соціологічні методи* застосовано при анкетуванні працівників органів прокуратури, оперативних, слідчих та експертних підрозділів (розділи 1–3). *Статистичні методи* використано при узагальненні результатів анкетування респондентів й аналізу кримінальних проваджень (розділи 1–3). *Документальний метод*

застосовано при визначенні тактичних помилок у тактичному забезпеченні СРД і НСРД (підрозділи 3.1, 3.3). На основі *синтезу* визначено загальні висновки й практичні рекомендації за темою дослідження.

Емпіричну основу дослідження становлять матеріали Єдиного звіту про кримінальні правопорушення Офісу Генерального прокурора України за період 2018-2023 років та результати узагальнення оперативної, слідчої та судової практики протягом 2016-2023 рр. Проаналізовано матеріали 192 кримінальних проваджень з проблематики дослідження (Вінницька, Дніпропетровська, Запорізька, Івано-Франківська, Київська, Львівська, Миколаївська, Одеська, Черкаська та Чернівецька області, м. Київ); зведені результати анкетування 179 працівників оперативних підрозділів, 186 слідчих, 80 дізнавачів, 89 працівників органів прокуратури України та 113 обізнаних осіб. Під час дослідження використано власний досвід роботи в підрозділах Національної поліції України.

Наукова новизна одержаних результатів полягає у тому, що дисертаційна робота є першим у вітчизняній науці комплексним монографічним дослідженням методики розслідування шахрайства в інтернет-комерції, у якому сформульовано низку теоретичних узагальнень, наукових положень і практичних рекомендацій, спрямованих на підвищення ефективності діяльності органів досудового розслідування Національної поліції України, що вирізняються науковою новизною та мають важливе теоретичне і практичне значення, зокрема:

уперше:

– запропоновано криміналістичні засоби та методи криміналістичної профілактики шахрайства в інтернет-комерції на підставі виокремлення заходів правового, соціального, технічного, інформаційного та організаційного характеру, що є запорукою виявлення причин й умов, що сприяли вчиненню таких кримінальних правопорушень, та обрання заходів щодо їх усунення;

– визначено доктринальний підхід до інформативного наповнення структури криміналістичної характеристики шахрайства в інтернет-комерції, а саме, виокремлено такі її складові: спосіб шахрайства, слідова картина, особа шахрая і потерпілого, місце, час і обстановка в розрізі з позицій законодавчого регулювання комерційних правовідносин у мережі інтернет, предмет злочинного посягання;

– розглянуто особливості взаємодії уповноважених осіб правоохоронних органів між собою та з державними і приватними структурами, що стосуються супроводження комерційних правочинів у мережі інтернет (постачальники послуг проміжного характеру в інформаційній сфері, органи державної влади й управління та органи місцевого самоврядування в частині виконання ними функцій держави або місцевого самоврядування тощо);

– аргументовано підхід до розгляду методики розслідування шахрайства в інтернет-комерції через проведення тактичних операцій, на підставі чого розроблено низку тактичних операцій з оптимальним комплексом дій для кожної, зокрема: «Фальшивий сайт», «Незаконна транзакція», «Встановлення

IP-адреси», «Ідентифікація особи у віртуальному просторі», «Встановлення умислу», «Організація затримання шахрая, який діяв у мережі інтернет» тощо;

удосконалено:

– систему заходів із організації та планування розслідування шахрайства в інтернет-комерції, що включає комплекс необхідних заходів, що забезпечують діяльність органів досудового розслідування з виявлення, розслідування та попередження таких кримінальних правопорушень на різних етапах розслідування;

– типові слідчі ситуації початкового етапу розслідування шахрайства, у зміст яких покладено інформаційний критерій та типові джерела доказів, що враховуються при визначенні слідчих ситуацій та напрямів розслідування;

– теоретико-правове розуміння систематизації типових способів підготовки, безпосереднього учинення й приховування шахрайства в інтернет-комерції з аналізом раніше досліджуваних способів та врахуванням злочинних дій шахраїв під час пандемії Covid-2019 та умов воєнного стану;

– сукупність криміналістично вагомих відомостей щодо правил побудови та перевірки версій, зокрема, під час розслідування шахрайства в інтернет-комерції;

– організаційно-тактичні рекомендації щодо проведення пред'явлення для впізнання у кримінальних провадженнях щодо шахрайства в інтернет-комерції;

– сукупність засобів організаційно-тактичного забезпечення проведення процесуальних дій, спрямованих на отримання інформації з матеріальних джерел під час розслідування шахрайства в інтернет-комерції (обшук, тимчасовий доступ до речей та документів, огляд тощо);

– наукові підходи щодо використання міжнародного досвіду щодо діяльності з питань подолання протидії шахрайству в інтернет-комерції;

дістали подальшого розвитку:

– наукові підходи щодо розуміння предмету шахрайського посягання в інтернет-комерції (майно, гроші, цінні папери, послуги – працевлаштування, страхування, перевезення, придбання квитків на залізничний чи авіатранспорт);

– сукупність криміналістичних даних, що характеризують потерпілого та особу, що вчиняє шахрайства в інтернет-комерції;

– положення щодо оцінки первинної інформації на початковому етапі розслідування шахрайства в інтернет-комерції;

– комплекс обставин, що підлягають з'ясуванню при розслідуванні шахрайства, пов'язаного з інтернет-комерцією;

– особливості тактики проведення окремих НСРД (встановлення місцезнаходження радіообладнання (радіоелектронного засобу), зняття інформації з електронних комунікаційних мереж та електронних інформаційних систем тощо);

– наукові положення щодо стану дослідження проблемних питань розслідування шахрайства, пов'язаного з інтернет-комерцією**;**

– наукові підходи до визначення слідової картини та обстановки учинення шахрайства в інтернет-комерції;

– форми використання спеціальних знань під час розслідування шахрайства в інтернет-комерції в межах проведення тактичних операцій;

– тактичні особливості проведення окремих СРД для вилучення інформації з особистісних джерел (допит підозрюваного, потерпілого та свідка);

– рекомендації щодо змін до КПК України стосовно обов'язку виявляти причини й умови, що сприяли учиненню шахрайств в інтернет-комерції уповноваженими службовими особами, які їх розслідують.

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

– *законотворчій діяльності* – для удосконалення чинного законодавства у сфері профілактики й запобігання протиправним діям у мережі Інтернет, а також шахрайствам в інтернет-комерції із внесенням пропозицій до чинного КПК України;

– *науковій діяльності* – для подальшого удосконалення наукових положень щодо методики розслідування кримінальних правопорушень окремих категорій (акти впровадження Дніпропетровського державного університету внутрішніх справ від 29.11.2022 р., ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом» від 24.11.2022 р.);

– *освітньому процесі* – при викладанні навчальних дисциплін «Методика розслідування окремих видів кримінальних правопорушень», «Методика розслідування кримінальних проступків», «Криміналістика», «Кримінальний процес», «Оперативно-розшукова діяльність», а також під час підготовки наукових, а також навчально-методичних видань (акти впровадження Національної академії внутрішніх справ від 29.10.2022 р., Харківського національного університету внутрішніх справ від 14.11.2022 р., Дніпропетровського державного університету внутрішніх справ від 30.11.2022 р.);

– *правозастосовній діяльності* – для вдосконалення діяльності правоохоронних органів МВС України (акти впровадження органів досудового розслідування ГУНП в Дніпропетровській області від 03.01.2023 р.), а також при проведенні практичних занять.

Апробація результатів дисертації. Основні теоретичні узагальнення та наукові положення дисертації оприлюднено на науково-практичних конференціях і семінарах, зокрема: «Актуальні проблеми розслідування кримінальних правопорушень у сфері громадської безпеки та громадського порядку» (м. Дніпро, 2017 р.), «Актуальні питання теорії та практики криміналістичної науки» (м. Дніпро, 2018 р.), «Актуальні проблеми експертного забезпечення досудового розслідування» (м. Дніпро, 2019 р.), «Актуальні проблеми експертного забезпечення досудового розслідування» (м. Дніпро, 2020 р.).

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

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, трьох розділів, що містять вісім підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 250 сторінок, із яких 195 сторінок основного тексту. Список використаних джерел налічує 232 найменування на 26-и сторінках, 4 додатки викладено на 29-и сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** обґрунтовано вибір теми дослідження, висвітлено ступінь вивчення проблеми, зв’язок роботи з науковими програмами, планами, темами, визначено мету, завдання, об’єкт і предмет дослідження, охарактеризовано методи, теоретичне й емпіричне підґрунтя дослідження, сформульовано наукову новизну одержаних результатів і наукові положення, які виносяться на захист, підкреслено наукове й практичне значення одержаних результатів, подано відомості про наукові публікації, структуру та обсяг дисертації.

Розділ 1 «Теоретичні основи розслідування шахрайства в інтернет-комерції» складається з двох підрозділів, які характеризують актуальність проблематики, поняття, сутність та структуру криміналістичної характеристики протиправного діяння, а також складові її структурні елементи.

У *підрозділі 1.1 «Стан наукових досліджень проблем протидії кібер-шахрайствам та правові передумови виникнення інтернет-комерції»* наголошено, що протиправні дії, що вчиняються у кіберпросторі, за різних часів були об’єктом пильної уваги вчених різних галузей знань. Одні вчені приділяли увагу питанням законодавчого регулювання правовідносин, що регулюють правові й інформаційні відносини у мережі інтернет, інші – зосереджували увагу на протидії таким кримінальним правопорушенням, а також питанням кримінально-правової кваліфікації та юридичній відповідальності за вчинення злочинних дій у кіберпросторі. Низку праць присвячено й методиці розслідування шахрайств, учинених у кіберпросторі. Натомість, значна кількість питань з розслідування шахрайств в інтернет-комерції залишається не дослідженою. Окрім того, у жодній з наукових робіт докладно не розглянуто питання щодо особливостей правового режиму здійснення комерційних операцій в мережі інтернет та його впливу на формування криміналістичної характеристики комерційного інтернет-шахрайства. Організація і тактика документування злочинної діяльності, пов’язаної з комерцією в інтернет-просторі, потребує також доопрацювання і

висвітлення у новому вимірі. Недостатньо з'ясовано й питання щодо особливостей організації і тактики проведення НСРД, а також здійснення тактичних операцій у провадженнях щодо шахрайств, пов'язаних з інтернет-комерцією. Залишаються недослідженими й заходи криміналістичної профілактики шахрайств, що потребує ґрунтовного вивчення, вдосконалення та подальшого розвитку вказаних аспектів.

У *підрозділі 1.2 «Концептуальні основи щодо формування криміналістичної характеристики шахрайства в інтернет-комерції»* на основі наукових розробок учених (А. Волобуєва, А. Мізерак, Т. Романенко, О. Самойленко, С. Самойлова, Р. Степанюка, С. Чучко, С. Шапочки та ін.) здійснено криміналістичний аналіз шахрайства в інтернет-комерції та визначено місце кожного елемента криміналістичної характеристики такого кримінального правопорушення. Наголошено, що теоретичні положення і практичні рекомендації з розслідування шахрайства можуть бути більш аргументованими у разі врахування особливостей правового режиму, що регулює відносини між різноманітними суб'єктами, які беруть участь в укладанні дистанційних угод; характеристики цих суб'єктів; предмета злочинного посягання; обстановки й умов, в яких вчиняється шахрайство; способу шахрайських дій. Особливе криміналістичне значення має слідова інформація про злочинну подію.

З'ясовано обстановку шахрайств з урахуванням просторово-часових характеристик, а також умов складної взаємодії комплексу чинників економічного, політичного та соціального характеру. Зазначено, що місцем учинення шахрайства у широкому розумінні є інтернет-простір, який утворюється завдяки електронним пристроям, підключеним до глобальної мережі інтернет. У вузькому значенні місцем шахрайства є місцезнаходження електронного технічного засобу (IP-адреса), підключеного до мережі інтернет, а також місце проведення розрахункових операцій (банк, банкомат). Час учинення шахрайств в інтернет-комерції характеризується досить тривалою подією у часі.

Предметом шахрайських дій виступає як майно – речі, гроші, цінні папери (92 %), так і послуги – страхування, працевлаштування, перевезення, придбання квитків на залізничний чи авіатранспорт (8 %). Натомість, внаслідок пандемії Covid-2019 у провадженнях щодо шахрайств в інтернет-комерції в якості предмету посягання стали фігурувати ліки від цієї хвороби, апарати штучного дихання, маски, а під час воєнного стану – речі, необхідні для несення служби у зонах бойових дій (воєнний одяг, бронежилети, військове обладнання, генератори тощо).

Визначено основні дії, до яких вдаються шахраї при підготовці й вчиненні шахрайства в інтернет-комерції, а саме: розробка дизайну сайта, верстання його web-сторінок і його програмування; розміщення інформації у соціальних мережах; наповнення сторінок інтернет-магазину фотографіями і іншими характеристиками товарів і послуг; підтримання рекламування товарів та послуг з метою зацікавлення населення; втягнення у процес дистанційної

комерції потенційних потерпілих; використання платіжних інструментів для переказу коштів або оплати товарів і послуг; заволодіння товарами, послугами чи грошима без виконання умов договору, укладеного в дистанційному форматі.

Виокремлено способи приховування шахрайства в інтернет-комерції, у тому числі в умовах воєнного стану. Виявлено специфічний механізм слідоутворення. Особливу увагу приділено інформаційним (віртуальним) слідам, що можуть бути виявлені під час вивчення комп'ютерного обладнання, а також містяться в мережі інтернет (web-сторінки, сайти, електронне листування, особисті профілі).

Сформовано типовий портрет особи шахрая з визначенням соціально-демографічних, біологічних і морально-психологічних ознак. Надано класифікацію осіб, які прямо або опосередковано можуть мати відношення до шахрайства в інтернет-комерції, зокрема: фізична особа, що пропонувала товар, у тому числі не існуючий; юридична особа, дані про яку розміщені в Єдиному державному реєстрі юридичних осіб, що пропонувала товар, у тому числі не існуючий; банківський працівник; посередники-провайдери, або оператори в системі мережі інтернет та інші суб'єкти, що надають різноманітні види послуг; покупець та ін.

Особливу увагу приділено характеристиці особи потерпілого та рівню її віктимної поведінки. Віктимність проявляється у довірливості по відношенню до суб'єктів, які пропонують товари та послуги у дистанційному форматі.

Розділ 2 «Організація розслідування шахрайства в інтернет-комерції» складається з трьох підрозділів, у яких висвітлено особливості початкового етапу розслідування шахрайства в інтернет-комерції, а також проблемні питання організації і планування розслідування кримінальних правопорушень.

У *підрозділі 2.1 «Оцінка первинної інформації на початку кримінального провадження»* визначено характерні підстави для початку кримінального провадження та проблемні питання, які виникають на цьому етапі.

Наголошено на необхідності збільшення терміну 24 години, протягом якого слідчий повинен встановити приводи і підстави для відкриття кримінального провадження щодо шахрайських дій в інтернет-комерції. У такі стислі строки досить складно прийняти об'єктивне рішення, адже така категорія шахрайств нерідко знаходиться на межі з цивільно-правовими відносинами і, без проведення ряду заходів, дуже складно у стислі терміни визначити склад шахрайства. Без встановлення умислу вже на початку розслідування ймовірним може бути у подальшому закриття провадження (у зв'язку з відсутністю складу злочину або встановленням неможливості виконати цивільно-правові зобов'язання у зв'язку з форсмажорними обставинами). Окреслено основні напрями взаємодії слідчого з працівниками Департаменту кіберполіції та іншими підрозділами Національної поліції, а також представниками служби безпеки Банку (щодо незаконних транзакцій) при оцінці первинної інформації, що надійшла з відповідних джерел.

У *підрозділі 2.2 «Організація та планування розслідування шахрайства в інтернет-комерції та коло обставин, що підлягають встановленню»* зазначено, що ефективність вирішення тактичних завдань залежить від правильної організації та планування процесу розслідування, що включає комплекс необхідних заходів, які забезпечують діяльність органів досудового розслідування з виявлення, розслідування та попередження шахрайств на різних етапах розслідування.

Зосереджено увагу на необхідності визначення тактичних завдань та обранні шляхів їх реалізації в рамках організації та планування розслідування шахрайства в інтернет-комерції. Основним тактичним завданням є встановлення точок доступу (IP-адреси), з яких здійснювалося спілкування між покупцем та продавцем, а також встановлення кола осіб, які користуються певним терміналом та їх приналежності до вчинення протиправних дій, пов'язаних з інтернет-комерцією. Висвітлюється питання щодо отримання інформації у соціальних мережах, мобільних додатках, державних реєстрах, що підтверджує причетність певних осіб до інтернет-шахрайства. Наведено офіційні правила здійснення інтернет-торгівлі та особливості виявлення фактів укладання дистанційних угод всупереч закону.

Запропоновано перелік загальних і приватних версій та коло обставин, що підлягають встановленню у даній категорії кримінальних проваджень.

З'ясовано, що однією з умов вчасного запобігання шахрайським проявам, швидкого розкриття й розслідування шахрайств в інтернет-комерції є правильна організація взаємодії відповідних органів. Визначено напрями взаємодії органів Національної поліції з постачальниками електронних комунікаційних послуг, операторами послуг платіжної інфраструктури, адміністраторами, що присвоюють мережеві ідентифікатори, та іншими суб'єктами, які забезпечують передачу й зберігання інформації з використанням інформаційно-комунікаційних систем, а також банківськими представництвами. Серед правоохоронних органів, котрі взаємодіють з органами досудового розслідування та прямо або опосередковано здійснюють виявлення кіберзлочинів, є підрозділи Департаменту кіберполіції, оперативні підрозділи карного розшуку та Департаменту захисту економіки тощо.

Зазначено, що у виявленні та розслідуванні кібершахрайств, вчинених в установах виконання покарань, важливою є комплексна співпраця працівників поліції з оперативними співробітниками СІЗО та працівниками Департаменту з питань виконання кримінальних покарань Мін'юсту. Визначено особливості організації взаємодії між вказаними суб'єктами під час розслідування шахрайств.

У процесі організації розслідування шахрайства в інтернет-комерції важливу роль займає міжнародне співробітництво з компетентними органами інших держав у вигляді надання запитів, звернень щодо необхідності проведення окремих процесуальних дій, вручення документів, видачі осіб, які вчинили протиправні дії, тимчасової передачі осіб, перейняття кримінального переслідування та ін.

У *підрозділі 2.3 «Типові слідчі ситуації, що виникають під час розслідування шахрайства в інтернет-комерції»* здійснено аналіз наукових розробок вчених стосовно поняття, сутності та видів слідчих ситуацій. Сформульовано типові слідчі ситуації розслідування шахрайства в інтернет-комерції та визначено алгоритми дій правоохоронних органів відповідно до кожної з них. Так, *у першій ситуації* (наявна інформація про шахрая і механізм шахрайства в цілому) передбачається проведення комплексу заходів, спрямованих на встановлення усіх обставин справи і доведення вини особи, яку підозрюють у шахрайстві, зокрема: допит потерпілого щодо обставин здійснення правочину у дистанційній формі та умов, що висувалися продавцем і покупцем; встановлення умов створення сайту, на якому викладалися пропозиції щодо купівлі-продажу товарів (послуг); отримання інформації від інтернет-провайдерів і операторів телекомунікаційного зв'язку; допит підозрюваного щодо обставин ошукування громадян, легітимності існування його діяльності; отримання даних, що характеризуютьх підозрюваного; пред'явлення підозрюваного для впізнання потерпілому (за умов спілкування у відеорежимі); огляд засобів комп'ютерної техніки, проведення обшуку у підозрюваного; призначення комп'ютерно-технічної та інших видів експертиз. *У другій ситуації*, коли наявна інформація про обставини шахрайства, але дані про шахрая невідомі, натомість, є вірогідність їх встановлення, окрім вказаних вище заходів, усі зусилля слідчого повинні бути спрямовані на отримання інформації щодо місцезнаходження шахрая. *У третій ситуації* (є інформація про обставини шахрайства, але особу шахрая не встановлено) необхідно проводити комплекс розшукових заходів, спрямованих на встановлення IP-адреси та осіб, які мали доступ до комп'ютерного обладнання, з якого здійснювалось управління web-сайтом та наповнення web-сайту забороненим контентом. Усі зусилля слід спрямувати на дослідження: операційної системи та оперативної пам'яті; вивчення змісту файлів; вивчення змісту web-браузерів; вивчення змісту електронної пошти; вивчення змісту смс-повідомлень, журналу вхідних і вихідних дзвінків на мобільному пристрої потерпілого та ін. Вказано типові джерела доказів у кримінальних провадженнях щодо шахрайства, що враховуються при визначенні слідчих ситуацій та напрямів подальшого розслідування.

Розділ 3 «Організаційно-тактичне забезпечення розслідування шахрайства в інтернет-комерції» складається з трьох підрозділів, у яких охарактеризовано особливості проведення тактичних операцій та окремих СРД і процесуальних дій, а також профілактична діяльність уповноважених осіб у кримінальних провадженнях за фактами шахрайства в інтернет-комерції.

У *підрозділі 3.1 «Організаційно-тактичні особливості проведення окремих слідчих (розшукових) та процесуальних дій»* з'ясовано, що до найбільш поширених процесуальних дій при розслідуванні шахрайства можна віднести: допит – 100 %, проведення експертизи – 100 %, отримання зразків для експертного дослідження – 91 %, огляд – 92 %, обшук – 56 %, допит в

режимі відеоконференції – 23 %, впізнання речей – 11 % та особи в режимі відеоконференції – 13 %, за фотографією – 8 %, слідчий експеримент – 5 %. Специфіка процесуальних дій, спрямованих на одержання інформації з матеріальних джерел (огляд, обшук, тимчасовий доступ до речей і документів) зумовлена тим, що у ході розслідування шахрайства виникає необхідність у виявленні, фіксації та вилученні низки матеріальних об'єктів, що мають доказове значення. До того ж, механізм шахрайських дій пов'язаний з використанням низки електронних носіїв, які відображають інформацію про здійснений правочин, та здійсненням ряду операцій, які відбуваються через електронні та телекомунікаційні мережі. З одного боку, одержана інформація може сприяти встановленню певних фактів щодо здійснення правочину, з іншого – паперові та електронні документи, а також комп'ютерна техніка можуть виступати речовими доказами у кримінальному провадженні.

Наведено перелік об'єктів, що підлягають вилученню під час обшуку чи тимчасового доступу до речей та документів: комп'ютерна техніка і програмне забезпечення (67 %), технічні засоби телекомунікації (91 %), розрахункові документи (43 %) та ін. Визначено організаційно-тактичні особливості вилучення та огляду таких носіїв комп'ютерної інформації. Розглянуто тактичні прийоми, у тому числі спрямованих на запобігання пошкодженню та знищенню інформації, яка знаходиться на матеріальних носіях комп'ютера та у «хмарних» сховищах.

Доведено, що слідчий нерідко стикається зі складнощами технічного та програмного характеру, що потребують втручання обізнаних осіб (програміст, системний інженер). Окреслено форми участі даних осіб під час проведення обшуку, огляду і тимчасового доступу до речей та документів. Запропоновано алгоритм дій під час огляду локального комп'ютерного засобу. Узагальнено не типові ситуації (складнощі), що можуть виникати під час проведення процесуальних дій, та надано рекомендації щодо їх усунення.

Висвітлено підготовчі заходи до проведення допиту підозрюваного, потерпілого та свідка. Сформовано перелік обставин, що підлягають встановленню під час допиту потерпілого, зокрема: за допомогою яких засобів дистанційного зв'язку потерпілий дізнався про товар або послугу (телекомунікаційні мережі, телебачення, мережа інтернет); чи було приділено увагу вивченню репутації продавця; чи було накладено електронний підпис для закріплення угоди; що саме рекламувалося, основні характеристики продукції, чи були фотознімки товару; якими були умови продажу (оплата, доставка); яким чином відбувався зв'язок з метою обговорення предмету договору (телефонний чи відеозв'язок, смс-спілкування); чи запам'ятав потерпілий зовнішність особи, яка виявилася шахраєм (під час відеозв'язку); чи робив потерпілий скріни екрану монітора (інтернет-магазину), спілкування з шахраєм; яким чином відбувалася автентифікація та авторизація користувача; що було підтвердженням електронного правочину (чи були вказані умови і порядок обміну чи повернення товару або відмови від виконання роботи чи надання послуги; чи вказані дані на продавця; чи вказані

гарантійні зобов'язання та інформація про інші послуги, пов'язані з утриманням чи ремонтом товару або з виконанням роботи чи наданням послуги; чи є інформація про розірвання договору; яким чином здійснювалася оплата потерпілим за товар або послугу; чи відповідають банківські реквізити, які надали потерпілому, тим, які розміщено на офіційному сайті; яким чином потерпілий зрозумів, що умови комерційного договору з продажу товарів (послуг) в онлайн-режимі не виконані; чи висувалися потерпілим претензії і як реагували на ці претензії шахраї; чи було прохання відправки товару накладним платежем; скільки пройшло часу з моменту протиправних дій до звернення громадян до правоохоронних органів чи направлення звернення на електронну скриньку Сервісної служби кіберполіції.

Зосереджено увагу на предметі допиту підозрюваних та осіб, які виступали свідками шахрайських дій. Розкрито особливості одночасного допиту двох або більше раніше допитаних осіб, а також пред'явлення для впізнання речей та особи за фотознімками, голосом, в режимі відеоконференції.

Значну увагу приділено НСРД, які мають найбільшу специфіку у кримінальних провадженнях щодо шахрайств в інтернет-комерції, зокрема: зняття інформації з електронних комунікаційних мереж (76 %), зняття інформації з електронних інформаційних систем (75 %), встановлення місцезнаходження радіообладнання, радіоелектронного засобу (91 %) та ін. Поширеність саме таких НСРД пов'язана з тим, що спілкування між шахраєм і потерпілим, особливо під час підготовки до вчинення шахрайських дій, здебільшого відбувається через транспортні телекомунікаційні мережі та через мережу інтернет (смс-повідомлення, відеозв'язок, листування через електронну адресу тощо).

У *підрозділі 3.2 «Криміналістична профілактика у кримінальних провадженнях за фактами шахрайства в інтернет-комерції»* наголошено, що ефективна протидія шахрайським проявам в інтернет-комерції вимагає від правоохоронних органів не тільки збирання доказової інформації, але й забезпечення певної профілактичної функції.

Виокремлено причини й умови, що сприяють учиненню шахрайств, зокрема: надмірна довірливість й безпечність громадян; халатне відношення до вивчення інформації, що міститься в електронній формі щодо умов купівлі-продажу товарів і послуг; зниження рівня життя населення та надання громадянами переваги укладанню дистанційного варіанта угод щодо купівлі-продажу товарів і послуг; розповсюдженість недостовірних пропозицій у ЗМІ та мережі інтернет; недосконала законодавча база щодо обмеження реклами, яка містить підозрілий контент, а також визначення підстав для блокування відповідних інтернет-ресурсів; професійно-моральна деформація суб'єктів підприємницької діяльності, що задіяні в інтернет-торгівлі; складність доведення факту вчинення обману в мережі інтернет та неоднозначність правових позицій суду щодо шахрайств; недоліки в діяльності контролюючих і правоохоронних органів, які своєчасно не виявляють шахрайства в мережі інтернет; наявність

законодавчих колізій щодо здійснення комерційних інтернет-угод. Запропоновано заходи профілактики, що можуть здійснюватися працівниками правоохоронних органів для попередження шахрайств в інтернет-комерції.

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. Значну увагу приділено профілактичним заходам технічного характеру, що здебільшого поєднуються з організаційними і правовими чинниками. Досліджено модель виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу. Розглянуто міжнародний досвід запобігання комерційним інтернет-шахрайствам, у тому числі й профілактичні заходи, що проводяться Європолом.

У *підрозділі 3.3 «Застосування тактичних операцій під час розслідування шахрайства в інтернет-комерції»* на підставі аналізу наукових праць учених (С. Кузьменка, О. Пчеліної, Д. Птушкіна, В. Шевчука) сформовано типові тактичні операції, що проводяться при розслідуванні шахрайства в інтернет-комерції, зокрема: «Фальшивий сайт», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному просторі», «Встановлення умислу», «Організація затримання шахрая, який діяв в мережі інтернет» та ін.

У межах наведених тактичних операцій розглянуто систему виявлення шахрайських операцій шляхом перевірки за різними фільтрами; специфіку аналізу бази даних проведених транзакцій; можливість встановлення місцезнаходження точки доступу до інтернету та провайдера, який сприяв доступу до мережі інтернет, особливості доступу до інформації, що міститься у поштовій скринці тощо. Визначено комплекс дій, що входять до змісту тактичних операцій у кримінальних провадженнях з розслідування шахрайств в інтернет-комерції.

Наголошено на ролі Департаменту кіберполіції, що відіграє важливу роль у реалізації низки тактичних операцій і надає істотну допомогу органам досудового розслідування у виявленні та доведенні фактів шахрайства у мережі інтернет.

Визначено перелік тактичних помилок й прорахунків, що допускаються слідчими під час проведення вказаних тактичних операцій.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що виявляється в розробленні теоретичних і практичних засад методики розслідування шахрайства в інтернет-комерції, а також формулювання науково обґрунтованих пропозицій і практичних рекомендацій щодо їх розвитку й удосконалення. Найсуттєвішими результатами дослідження є такі:

1. Визначено стан наукового дослідження питань розслідування

шахрайства в інтернет-комерції. Більшість наукових робіт, що присвячені питанням протидії злочинності у кіберпросторі, стосуються адміністративно-правових, цивільно-правових та кримінологічних аспектів. Втім, наукові розробки щодо методики розслідування шахрайств, учинених у кіберпросторі, містять значну кількість проблемних питань, пов'язаних зі специфікою організації та планування розслідування шахрайств, тактики проведення процесуальних дій, а також питань, пов'язаних із криміналістичною профілактикою шахрайств в інтернет-комерції. Доведено, що виникає необхідність розробки й впровадження у правозастосовну діяльність методики розслідування шахрайства в інтернет-комерції.

2. Узагальнено сучасні наукові підходи до розуміння криміналістичної характеристики шахрайства в інтернет-комерції та підкреслено наявність вагомих кореляційних зв'язків між усіма її елементами. Розслідування шахрайства в інтернет-комерції характеризуються складним механізмом та специфічною технологізацією таких кримінальних правопорушень. Система криміналістичної характеристики шахрайства в інтернет-комерції складається з таких елементів: спосіб учинення шахрайства, слідова картина, особа шахрая, особа потерпілого, місце, час і обстановка в розрізі законодавчого регулювання комерційних правовідносин у мережі інтернет, предмет злочинного посягання.

Способи шахрайства в інтернет-комерції проявляються у системі взаємопов'язаних дій з підготовки, безпосереднього вчинення й приховування кримінального правопорушення. Цей факт можна пояснити складним механізмом здійснення правочинів у дистанційному варіанті. Протиправні дії можуть початися з розміщення оголошення про продаж певних товарів і 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, протиправні дії можуть припинятися на певному етапі.

Серед способів приховування шахрайства в інтернет-комерції виявлено такі: виготовлення і використання фіктивних документів при реєстрації на сайті – 22 %, маскування шахрайських дій під легальні цивільно-правові угоди – 24 %, знищення електронних документів, що використовувалися при здійсненні електронних правочинів – 45 %, знищення персональної інформації, що надавалася провайдеру для реєстрації – 38 %, підкуп свідків – 34 %, маскування зовнішності під час онлайн-спілкування з потенціальною жертвою – 17 %, використання чужих платіжних карток для здійснення грошових переказів – 66 % та ін.

Шахрайство в інтернет-комерції характеризується специфікою слідів, що можуть залишатися на таких носіях: пам'яті телефону – 78 %, сім-картці – 48 %, комп'ютері – 81 %, сервері мобільного оператора – 18 % або інтернет-провайдера – 17 %, флешці чи зовнішньому вінчестері – 38 %, пам'яті

електронного журналу банкомату (терміналу) – 67%, історії платіжних переказів через банківську систему – 78 %, квитанціях і роздруківках про електронні банківські платежі – 51 %, банківських картках – 37 %, пам'яті системи відеоспостереження (зал інтернет-кафе, фойє банку, місце біля банкомату) – 31 %, слідах папілярних ліній на засобах комп'ютерної техніки, клавіатурі терміналу – 38 % та ін.

Специфікою обстановки вчинення шахрайств в інтернет-комерції є часткова втрата ознаки чіткої територіальності та розпливчастість часових і просторових меж через віртуальний характер правочинів, а також уникнення безпосереднього фізичного контакту між потерпілим та шахраєм.

З'ясовано, що предметом посягань у кримінальних провадженнях щодо шахрайств в інтернет-комерції переважно є: гроші (47 %), різноманітні товари побутового призначення (13 %), предмети, які мають стратегічне призначення (бронежилети, каски, військове обладнання) (12 %), генератори (3 %), медикаменти (4 %), певні цінності (9 %), послуги (8 %) та ін.

Виокремлено криміналістично вагомі ознаки особи шахрая, а також складено його типовий портрет. Відзначено консолідацію кібершахраїв у групи, з подальшим їх укрупненням до злочинних угруповань, що діють на транснаціональному рівні. Потерпілими від шахрайства можуть стати будь-які фізичні та юридичні особи, підприємці, інші споживачі товарів та послуг. У 88 % випадків від дій шахраїв страждає особа, яка виступає набувачем товарів та послуг (покупець). Проте, іноді потерпілим може стати не тільки покупець, а й продавець.

3. Визначено специфіку початкового етапу розслідування шахрайства в інтернет-комерції, яка полягає у тому, що основним джерелом інформації про таке кримінальне правопорушення є матеріали Департаменту кіберполіції Національної поліції (64 %). Безпосереднє звернення громадян із заявою та повідомленням до органів Національної поліції складає 26 %. Джерелом інформації про шахрайства може бути й інформація, отримана від служби безпеки Банку про незаконні транзакції (13 %). Реалізація такої інформації повинна здійснюватися тільки у взаємодії з Департаментом кіберполіції та підрозділами Національної поліції.

На початку розслідування найбільші складнощі виникають саме у процесі встановлення територіальної юрисдикції, у межах якої вчинено шахрайство, тому основним завданням перевірки заяв і повідомлень про шахрайські дії, а також оцінки матеріалів самостійного виявлення посадовою особою правоохоронних і контролюючих державних органів щодо фактів учинення чи підготовки до шахрайств, є з'ясування наявності достатніх приводів і підстав для відкриття кримінального провадження. Не менш важливим завданням є також встановлення попередньої правової кваліфікації, а також вибір процесуальних заходів, найбільш доцільних для прийняття об'єктивного рішення.

4. Розглянуто основні елементи організації й планування розслідування шахрайства в інтернет-комерції та визначено коло обставин, що підлягають встановленню. При розслідуванні шахрайств виникають різного роду організаційні питання, пов'язані з висуненням версій, встановленням обставин, що підлягають доказуванню, окресленням тактичних завдань, визначенням строків та переліку осіб, яких необхідно задіяти для виконання тих чи інших заходів. Водночас, реалізація цих напрямків є неможливою без відповідного планування, особливо у багатоепізодних кримінальних провадженнях. Правильно організоване планування сприяє всебічності, повноті та цілеспрямованості розслідування, з дотриманням визначених законом процесуальних строків.

Виокремлено обставини, що підлягають встановленню, зокрема: джерело надходження інформації про подію шахрайства; наявність факту кримінального правопорушення (чи дійсно дії, пов'язані з торгівлею в мережі інтернет, є злочинними, чи мав місце цивільно-правовий делікт); у чому полягали підготовчі дії, дії з безпосереднього вчинення та приховування шахрайства, яка їх тривалість, де вони відбувалися; кількість епізодів; час і місце вчинення шахрайських дій; обставини, що характеризують особу потерпілого і шахрая, їх кількість та характер участі кожного у вчиненні шахрайства; обставини, що свідчать про вчинення шахрайства організованою групою; обставини, що підтверджують вину кожного з шахраїв або виключають кримінальну відповідальність; обставини, які впливають на ступінь тяжкості кримінального правопорушення, обтяжують чи пом'якшують покарання кожного співучасника; обставини, що підтверджують вид і розмір завданої шкоди; наявність злочинних зв'язків шахраїв з представниками влади та особами, які супроводжують дистанційні правочини щодо купівлі-продажу товарів і послуг через мережу інтернет. Серед окремих обставин, що підлягають встановленню, можна виокремити наступні: приналежність і характеристика сайту; визначення провайдера, який надавав послугу хостингу; визначення банку, через який проводилися транзакції; обставини, що доводять намір не виконувати умови, оговорені на момент укладання правочину у дистанційному форматі; абонентська інформація про особу та її ідентифікація; встановлення права продавця на здійснення дистанційного правочину; встановлення IP-адреси, з якої здійснювався доступ, необхідний для укладання угоди через мережу інтернет та ін.

Встановлення низки обставин, що мають значення для кримінального провадження, є неможливим без належної взаємодії уповноважених осіб правоохоронних органів між собою та з державними і приватними структурами, які мають відношення до супроводження комерційних правочинів в мережі інтернет (постачальники послуг проміжного характеру в інформаційній сфері, органи державної влади та органи місцевого самоврядування в частині виконання ними функцій держави або місцевого

самоврядування). Встановлено особливості взаємодії слідчого з працівниками карного розшуку та кіберполіції, що полягає у повному супроводі розслідування шахрайства в інтернет-комерції, зокрема: обміні інформацією, виконанні доручень, оперативному супроводі при проведенні СРД, НСРД та застосуванні заходів забезпечення кримінального провадження, а також наданні слідчому матеріалів, зібраних під час ОРД, для вирішення питання щодо відкриття кримінального провадження за новими фактами.

5. Виокремлено типові слідчі ситуації, що складаються при розслідуванні шахрайства в інтернет-комерції: наявна інформація про особу шахрая та механізм шахрайства в цілому – 57 %; наявна інформація про обставини шахрайства, але дані про шахрая невідомі, натомість, є вірогідність їх встановлення – 13 %; є інформація про обставини шахрайства, але особа шахрая невідома – 30 %. Наведено рекомендований перелік заходів для кожної слідчої ситуації.

6. З'ясовано організаційно-тактичні особливості проведення окремих СРД, НСРД та процесуальних дій. Виокремлено об'єкти вилучення у провадженнях щодо шахрайства, пов'язаного з інтернет-комерцією, зокрема: мобільні телефони (91 %); флеш-носії, диски та інші електронні носії інформації (91 %); аудіо-, відеозаписи (61 %); комп'ютерна техніка й програмне забезпечення (67 %); записні книжки, рукописні тексти, електронні записники (14 %); попередні договори купівлі-продажу між покупцем і продавцем – договір-завдаток, розписки (57 %); документи, що посвідчують особу (22 %); печатки й штампи, кліше підписів (21 %); бланки, які необхідні для укладання угод цивільно-правового характеру (16 %); ілюстровані брошури, буклети, каталоги (52 %); бланки залізничних і авіаквитків, туристичних полісів (12 %); документи, що підтверджують виконання договірних зобов'язань (12 %); документи, що підтверджують оплату послуг (розрахунковий документ) (43 %); договори між організаціями і приватними підприємцями, які беруть участь у комерційних операціях (41 %); документи, що посвідчують законність діяльності суб'єкта підприємницької діяльності (44 %); акти підключення до інтернету (54 %); акти виконаних робіт щодо обслуговування інтернету (45 %); засоби маскування, що застосовувалися при онлайн-спілкуванні (8 %) та ін. Вказані об'єкти можна вилучити шляхом обшуку чи тимчасового доступу до речей і документів у разі, якщо йдеться про добровільну видачу речей та документів, що знаходяться у володінні певної особи. До таких осіб можна віднести: представників банківської установи, інтернет-провайдерів, власників комп'ютерних клубів та інтернет-кафе та ін.

Наголошено, що у 56 % випадків під час розслідування шахрайств виникає необхідність саме примусового вилучення, тобто, шляхом обшуку. Проведення обшуку потребує ретельної підготовки і розробки тактики дій, а також залучення фахівців із комп'ютерної техніки і програмного забезпечення (програміст, системний інженер). Дані особи надають консультації щодо

правильного увімкнення технічних пристроїв, пошуку файлів, доступу до хмарних сховищ та операційної системи (78 %); здійснюють допомогу у правильному вилученні комп'ютерної техніки та інформації, що знаходиться на жорстких, віртуальних дисках (81 %); здійснюють допомогу в огляді функціональної частини комп'ютера і зовнішніх носіїв даних, а також технічної документації (93 %); допомагають подолати систему захисту комп'ютерної інформації та провести аутентифікацію доступу до комп'ютера чи телефону конкретного користувача (62 %) та ін.

Запропоновано підготовчі заходи до проведення допиту підозрюваного, потерпілого й свідка. Окрім загальновизнаних елементів підготовки (вивчення особи допитуваного, обрання місця і часу допиту, підготовка засобів фіксації допиту), слідчий повинен опрацювати й законодавство, що регулює торгівельні правовідносини в режимі онлайн із використанням електронних засобів зв'язку. Серед питань, що стосуються здійснення інтернет-комерції в онлайн-режимі, необхідно опрацювати наступні: загальний принцип регулювання договорів, що укладаються електронним шляхом; порядок надання електронним договорам юридичної сили; вимоги щодо забезпечення ідентифікації особи, яка підписала документ, і гарантії незмінності документа, що скріплений електронним цифровим підписом; способи встановлення автентичності в онлайн-режимі. Запропоновано розширений перелік обставин, що підлягають встановленню під час допиту різної категорії осіб. Встановлено коло осіб, які підлягають допиту як свідки: працівники, які супроводжують комерційні угоди в онлайн-режимі; представники юридичної особи, яка використовувалася під час шахрайських дій; спеціалісти, які мають професійний досвід у галузі інформатики та комп'ютерної техніки, програмування, у тому числі особи, які приймали участь у якості спеціалістів під час СРД; особи, які знаходилися у приміщенні інтернет-кафе, банку; банківські працівники; родичі та знайомі потерпілого; родичі та знайомі підозрюваних та ін.

Розроблено найбільш ефективні тактичні прийоми, що впливають на ситуацію допиту як в умовах безконфліктності, так і в умовах конфліктності. Розкрито тактику проведення одночасного допиту двох або більше раніше допитаних осіб. Встановлено, що пред'явлення для впізнання проводиться рідко (8 %), адже спілкування між шахраєм і потерпілим здебільшого здійснюється через смс-повідомлення або за допомогою телекомунікаційних пристроїв. Необхідність у пред'явленні для впізнання може виникнути у разі, якщо контакт відбувався через відеозв'язок і потерпілий заявляє, що запам'ятав зовнішність шахрая і зможе його впізнати. За таких обставин доцільно обрати об'єктами пред'явлення для впізнання або живих осіб, або осіб, зображених на фотокартках.

Запропоновано перелік основних НСРД під час розслідування шахрайства, зокрема: зняття інформації з електронних комунікаційних мереж

та електронних інформаційних систем; установлення місцезнаходження радіообладнання (радіоелектронного засобу) та ін. За допомогою вказаних НСРД можна отримати інформацію, що міститься в електронних інформаційних системах, здійснити фіксацію телефонних розмов, іншої інформації та сигналів, які мають значення для встановлення обставин вчинення шахрайства в інтернет-комерції, запеленгувати місцезнаходження кінцевого обладнання мереж телекомунікацій та ін.

7. Визначено особливості профілактичної діяльності уповноважених осіб у кримінальних провадженнях за фактами шахрайства в інтернет-комерції. Серед основних профілактичних заходів є виявлення причин і умов, що сприяють учиненню шахрайств, а також застосування заходів щодо їх усунення та перешкоджання. Профілактика поєднує низку заходів правового, соціального, технічного, організаційного та інформаційного характеру, зокрема: розміщення оголошень у ЗМІ щодо способів комерційних інтернет-шахрайств і заходів їх запобігання; виявлення ознак кіберзагроз в транзакціях користувачів мобільного та інтернет-банкінгу; відслідковування операцій, що потенційно можуть бути шахрайськими з урахуванням кількості карток клієнта, його місцезнаходженням та місцем здійснення операції, місцезнаходженням і адресою доставки; використання новітніх електронних систем і досягнень штучного інтелекту щодо запобігання електронного комерційного шахрайства; актуалізація законодавчих актів, що регулюють інтернет-відносини; підсилення відповідальності за вчинення шахрайств у мережі інтернет; посилення відповідальності адміністраторів баз даних та інших осіб, які забезпечують функціонування мережі інтернет, електронних вузлів і пристроїв; підсилення міжнародного співробітництва у боротьбі з комерційним кібершахрайством; створення Єдиної інформаційної системи, яка поєднуватиме різноманітні інформаційні ресурси, платформи та бази даних про шахраїв, які вчиняють комерційні інтернет-шахрайства; залучення громадськості з профілактики шахрайства у сфері електронної торгівлі та ін.

8. Сформовано типові тактичні операції, спрямовані на вирішення завдань розслідування шахрайства в інтернет-комерції. Виходячи з окреслених завдань розслідування, запропоновано такі типові тактичні операції: «Фальшивий сайт», «Незаконна транзакція», «Встановлення IP-адреси», «Ідентифікація особи у віртуальному просторі», «Встановлення умислу», «Організація затримання шахрая, який діяв в мережі інтернет». Висвітлено організаційно-тактичні особливості проведення процесуальних дій, НСРД, організаційних і розшукових заходів у рамках тактичних операцій та окреслено роль використання спеціальних знань.

Для кожної з тактичних операцій розроблено оптимальний комплекс дій.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Рейнгольд А.В. Слідчі (розшукові) та інші процесуальні дії, спрямовані на вилучення матеріальних джерел при розслідуванні шахрайств в інтернет-комерції. *Юридична наука*. 2019. № 5. Том 2. С. 87–92.
2. Рейнгольд А.В. Концептуальні підходи до побудови криміналістичної характеристики шахрайства в інтернет-комерції. *Юридична наука*. 2019. № 6. Том 2. С. 73–77.
3. Рейнгольд А.В. Оцінка первинної інформації на початку розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 1. Том 2. С. 114–118.
4. Рейнгольд А.В. Типові слідчі ситуації під час розслідування шахрайства в інтернет-комерції. *Юридична наука*. 2020. № 2. Том 2. С. 129–133.
5. Рейнгольд А.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.
6. Рейнгольд А.В. Стан розробленості проблеми боротьби із шахрайством в інтернет-комерції. *KELM*. 2022. № 7. С. 112–117 (Республіка Польща).

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Рейнгольд А.В. Наукові дискусії щодо обставин, які підлягають встановленню під час розслідування шахрайства в інтернет-комерції. *Актуальні проблеми розслідування кримінальних правопорушень у сфері громадської безпеки та громадського порядку :* матер. наук.-практ. семінару (м. Дніпро, 30 трав. 2017 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2017. С. 219–222.
8. 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.
9. Рейнгольд А.В. Заходи запобігання шахрайству в інтернет-комерції: теоретико-прикладні проблеми. *Актуальні проблеми експертного забезпечення досудового розслідування :* матер. наук.-практ. семінару (м. Дніпро, 24 трав. 2019 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. С. 252–256.

10. Рейнгольд А.В. Наукові підходи щодо організації та планування розслідування шахрайства в інтернет-комерції. *Актуальні проблеми експертного забезпечення досудового розслідування :* матер. наук.-практ. семінару (м. Дніпро, 29 трав. 2020 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2020. С. 380–382.

АНОТАЦІЯ

Рейнгольд А. В. Основи методики розслідування шахрайства в інтернет-комерції. – *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, 2023.

У дисертації на монографічному рівні досліджено теоретичні та практичні засади розслідування шахрайства в інтернет-комерції. На основі системного аналізу розкрито інформативне наповнення криміналістичної характеристики шахрайства, у якій послідовно охарактеризовано такі елементи: спосіб шахрайства, предмет злочинного посягання, слідова картина, особа шахрая і потерпілого, місце, час і обстановка з позицій законодавчого регулювання комерційних правовідносин у мережі інтернет. Окреслено кореляційні зв’язки між зазначеними елементами.

Визначено типові способи шахрайства в інтернет-комерції, що переважно мають повноструктурний склад, адже наявний складний механізм здійснення правочинів у дистанційному варіанті. Розкрито слідову картину та обстановку. Визначено вузлові ділянки, де можуть бути зосереджені сліди шахрайських дій. Виділено віктимологічні групи потерпілих. Встановлено криміналістично значущі типологічні ознаки особи шахрая, запропоновано його ймовірний «портрет».

Визначено особливості організації й планування розслідування шахрайства, систематизовано типові слідчі ситуації та з’ясовано коло обставин, що підлягають встановленню. Наголошено на особливостях взаємодії слідчого з працівниками карного розшуку та кіберполіції. З’ясовано специфіку огляду, обшуку і тимчасового доступу до речей та документів. Серед процесуальних дій потрібно виділити обшук, який є не тільки осередком доказового матеріалу, але й служить суттєвим джерелом інформації про обставини шахрайства та осіб, що його здійснили. Розкрито тактику допиту підозрюваного, потерпілого та свідка. Запропоновано перелік основних НСРД. Сформовано типові тактичні операції, спрямовані на вирішення завдань розслідування шахрайства в інтернет-комерції. Розглянуто міжнародний досвід запобігання шахрайствам і охарактеризовано профілактичну діяльність уповноважених осіб щодо виявлення та усунення причин й умов учинення шахрайських дій. Виділено

заходи щодо їх профілактики.

Ключові слова: *шахрайство, інтернет-комерція, шахрай, досудове розслідування, методика, взаємодія, криміналістична характеристика, інтернет-провайдер, слідча (розшукова) дія, тактична операція, віртуальний простір.*

SUMMARY

Reinhold A. V. Basics of fraud investigation methods in Internet 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, 2023.

The dissertation at the monographic level explores the theoretical and practical foundations of fraud investigation in Internet commerce. On the basis of a systematic analysis, the informative content of the forensic characteristics of fraud was revealed, in which the following elements were consistently characterized: the method of fraud, the object of the criminal offense, the trail picture, the identity of the fraudster and the victim, the place, time and situation in terms of the legislative regulation of commercial relations on the Internet. The correlations between the specified elements are outlined.

Typical methods of fraud in Internet commerce are defined. It has been found that when fraud is committed, the full-structured composition of the method is mostly used, because there is a complex mechanism for carrying out transactions in a remote version. The situation and trace pattern are characterized. Nodal areas where traces of fraudulent activities may be concentrated have been identified. Forensically significant typological features of the fraudster's personality were established, and his probable «portrait» was proposed. Victimological groups of the victims have been identified.

The peculiarities of the organization and planning of the fraud investigation are determined, typical investigative situations are systematized, and the circumstances to be established are clarified. The peculiarities of the interaction of the investigator with criminal investigation and cyber police officers are emphasized.

The specifics of inspection, search and temporary access to things and documents have been clarified. Among the procedural actions, it is necessary to single out a search, which is not only a source of evidential material, but also serves as a significant source of information about the circumstances of the fraud and the persons who committed it. The interrogation tactics of the suspect, the victim and the witness were disclosed. A list of the main NSRD is proposed.

Keywords: *fraud, Internet commerce, fraudster, cyber fraudsters, pretrial investigation, technique, interaction, forensic characteristics, Internet provider, investigative (search) action, tactical operation, IP address, virtual space.*